Faculteit Rechtsgeleerdheid
Universiteit Gent
Academiejaar 2016-2017

THE EU-U.S. PRI(VA)CY SHIELD: ENSURING THE CONTINUATION OF DATA FLOWS INSTEAD OF REBUILDING TRUST?

Europe tangled up in its own data protection requirements?

Masterproef van de opleiding
'Master in de rechten'

Ingediend door

Judith Vermeulen

01202363

Promotor: Prof. Dr. Yves Haeck
Commissaris: Andy Van Pachtenbeke

TABLE OF CONTENTS

PREFACE 7
GENERAL INTRODUCTION 9
A. Research questions and structure 9
B. Basic concepts 10
1. Right to privacy and right to data protection 10
2. Processing of personal data for commercial purposes 11
3. Mass surveillance and difference between content data and metadata 12
CHAPTER 1. ADEQUACY EX DIRECTIVE 95/46/EC AS A NECESSARY CONDITION FOR THE TRANSFER OF PERSONAL DATA FROM THE UNION TO A THIRD COUNTRY 13
A. Introduction 13
B. Directive 95/46/EC: purpose, scope and relevance for the EU-U.S. Privacy Shield 14
C. Notion of 'adequacy' 15
D. Assessment of 'adequacy' 17
1. Adequacy decision by the European Commission 17
2. Adequacy assessment by the controller, the national data protection authority or any other body established to fulfil this task 18
E. Transfer of personal data to countries not ensuring an adequate level of data protection 19
1. Specific exceptions 19
2. Adducement of adequate safeguards 20
F. Conclusion 23
CHAPTER 2. SUBSTANTIVE EU DATA PROTECTION STANDARDS AND PERMISSIBILITY OF DEROGATIONS 25
A. Introduction 25
B. Substantive EU data protection standards 25
1. Content principles 27
a. Purpose limitation 28
b. Proportionality 29
c. Data quality 29

d. Data retention limitation principle 29
e. Transparency 30
f. Data security and confidentiality of processing 30
g. Rights of access, rectification and opposition 32
h. Restrictions on onward transfers – adequacy requirement 32
i. Additional principles which apply to specific types of processing 33
(1) Sensitive data 33
(2) Direct marketing 33
(3) Automated individual decision 33
2. Procedural/enforcement mechanisms 34
a. Good compliance 34
b. Support and help to individual data subjects 36
c. Appropriate redress 36
C. Permissibility of derogations 37
1. Case law of the Court of Justice of the European Union 39
a. Digital Rights Ireland judgment 39
(1) Facts of the case and background of the Data Retention Directive 39
(2) Ruling of the Court 41
(a) Interference with the right to privacy (article 7 Charter) and to data protection (article 8 Charter) 41
(b) Justification of the interference in the light of article 52, §1 Charter 42
(i) Respect for the essence of the rights and objectives of general interest 43
(ii) Proportionality 43
b. Tele2 Sverige judgment 46
(1) Relevance of article 15, §1 of Directive 2002/58/EC and facts of the case 46
(2) Ruling of the Court 48
c. Schrems judgment 50
(1) Facts of the case 50
(2) Ruling of the Court 52

(a) Powers of the national supervisory authorities 52
(b) Validity of Decision 2000/520/EC 53
d. Conclusion 56
2. Case law of the European Court of Human Rights 56
a. Zakharov v. Russia 57
(1) Facts of the case 58
(2) Ruling of the Court 58
b. Szabó and Vissy v. Hungary 62
(1) Facts of the case 62
(2) Ruling of the Court 62
c. Conclusion 64
D. Main findings and conclusive remarks 65
CHAPTER 3. ADEQUACY OF THE U.S. DATA PROTECTION REGIME AS COMPLEMENTED BY THE EU-U.S. PRIVACY SHIELD IN THE LIGHT OF THE SUBSTANTIVE EU DATA PROTECTION STANDARDS AND THE EU REQUIREMENTS IN CASE OF DEROGATIONS TO THE BENEFIT OF GOVERNMENT AUTHORITIES 69
A. Introduction 69
B. Structure of the adequacy decision and functioning of the EU-U.S. Privacy Shield 71
C. Adequacy assessment of the substantive data protection requirements to which U.S. self-certified companies are ought to adhere 74
1. Content principles 75
a. Notice 76
b. Choice 76
c. Accountability for Onward Transfer 77
d. Security 78
e. Data integrity and purpose limitation 78
f. Access 79
g. Lack of a data retention limitation principle 80
h. Automated individual decision 80
2. Procedural/enforcement mechanisms 80

a. Procedural/enforcement mechanisms 81
b. Fulfilment of the EU requirements 83
D. Adequacy assessment of the U.S. privacy and data protection policy in case of collection and further processing of personal data transferred under the EU-U.S. Privacy Shield by U.S. public authorities 85
1. Limitations and safeguards regarding the collection and further processing of personal data in the interests of national security 87
a. Strict necessity 87
b. Oversight 93
c. Redress: Privacy Shield Ombudsperson 96
2. Limitations and safeguards regarding the collection and further processing of personal data for law enforcement and public interest purposes 97
3. Lack of purpose limitation 100
4. Conclusion 101
E. Conclusion: a 'Pricy' Shield 101
CHAPTER 4. EU POLICY REGARDING BULK COLLECTION OF PERSONAL DATA AFTER TELE2 SVERIGE AND FEASIBILITY OF (STANDARD) CONTRACTUALS CLAUSES AND BINDING CORPORATE RULES AFTER SCHREMS: EUROPE TANGLED UP IN ITS OWN DATA PROTECTION REQUIREMENTS? 103
A. Air Passenger Name Record Data (PNR) – Agreements and Directive 103
1. Air Passenger Name Record Data (PNR) 104
2. PNR Agreements 105
3. PNR Directive 108
4. Conclusion 109
B. EU-U.S. Terrorist Finance Tracking Programme (TFTP) Agreement 109
1. Terrorist Finance Tracking Programme (TFTP): functioning and SWIFT 110
2. EU-U.S. Agreement 111
3. Conclusion 113
C. (Standard) contractual clauses and binding corporate rules 114
D. Conclusion 115
MAIN FINDINGS 117

BIBLIOGRAPHY 121
ANNEX: NEDERLANDSTALIGE SAMENVATTING 135

PREFACE

I would like to thank my promotor, Prof. Dr. Yves Haeck, for having given me the opportunity to write this thesis, to get more acquainted with data protection legislation, and to develop this topic freely.

I also want to make a special reference to my mom, because I'm finishing this thesis on mother's Day.

GENERAL INTRODUCTION

A. Research questions and structure

1. On 6 October 2015, the Court of Justice of the European Union, in the *Schrems* case, invalidated the European Commission's Safe Harbour adequacy decision, which facilitated the flow of commercial data from the European Union to the United States. Bearing in mind Edward Snowden's disclosures concerning the mass surveillance programmes run by the U.S. government, the Court considered that the decision did not sufficiently demonstrate that the United States in fact ensured an adequate level of data protection. As a result, such data transfers could no longer be based on that decision. Alternative tools, such as (standard) contractual clauses ((S)CCs) and binding corporate rules (BCRs), had to be used instead. On 12 July 2016, however, the Commission adopted a new decision regarding 'the adequacy of the protection provided by the EU-U.S. Privacy Shield'.

2. Hence, the main research question of this thesis will be whether the United States, by reason of its domestic law or of the international commitments it has entered into, and in particular by reason of the EU-U.S. Privacy Shield, in fact does ensure an adequate level of data protection in the light of the EU data protection requirements, and, accordingly, whether the Commission's Privacy Shield adequacy decision can be considered valid. Whereas the Court, in *Schrems*, did not examine the adequacy of the Safe Harbour Privacy Principles as such and confined its analysis to an assessment of the mass surveillance programmes in relation to the fundamental rights of EU data subjects, the current assessment will envisage both the principles the recipient companies have to adhere to (*i.e.* the EU-U.S. Privacy Shield Framework Principles, which replace the Safe Harbour Principles) as well as the safeguards and limitations meant to ensure that interferences (i.e. the surveillance measures) by the U.S. government authorities with the privacy and data protection rights of EU data subjects are justifiable.

In order to be able to answer this question, first, the rationale and the significance of the notion of 'adequacy' will be examined, and, thereinafter, the EU data protection requirements will be set out and analysed. As regards these requirements, the recent case law of the Court of Justice of the European Union and the European Court of Human Rights will be of significant importance.

3. In a second instance, and in order to put the first question into perspective, the repercussion of the said case law in relation to a number of other EU instruments will also be addressed, be it in a less extensive manner.

4. Accordingly, the structure of this thesis will be as follows: firstly, the 'adequacy' requirement ex Directive 95/46/EC will be addressed (Chapter 1); secondly, the substantive EU data protection requirements and permissibility of derogations thereto will be examined (Chapter 2); thirdly, the U.S data protection regime as complemented by the EU-U.S. Privacy Shield will be analysed in the light of the

findings in Chapter 1 and 2 (Chapter 3); and lastly, the repercussions of the recent case law of the Court of Justice of the European Union in relation to other EU instruments will be assessed (Chapter 4).

B. Basic concepts

1. Right to privacy and right to data protection

5. Since the coming into force of the Lisbon Treaty in 2009, the EU has in place a legally binding document pertaining to fundamental rights: the Charter on Fundamental Rights of the European Union.[1] The provisions of the Charter are addressed to the institutions, bodies, offices and agencies of the Union and to the Member States when they are implementing Union law.[2] The Charter not only includes a right to privacy (and family life) (article 7), but also sets out a distinct right to data protection (article 8).[3] In other authoritative human rights documents, such as the European Convention on Human Rights, for the most part, the protection of personal data is treated as an extension of the right to privacy, making the EU Charter unique in that respect.[4] The inclusion of a separate right to data protection has to do with the fact that EU Member States have previously engaged in the protection of personal data via the adoption of legally binding instruments specifically related to data protection.[5]

Article 7 of the EU Charter provides that:

> *"[e]veryone has the right to respect for his or her private and family life, home and communications".*

Article 8 reads as follows:

> *"1. Everyone has the right to the protection of personal data concerning him or her.*

---

[1] Charter of Fundamental Rights of the European Union [2007] OJ C 326/391 ['Charter of Fundamental Rights of the European Union']; European Union Agency for Fundamental Rights (FRA), Council of Europe and Registry of the European Court of Human Rights, *Handbook on European data protection law* (Publications Office of the European Union 2014), 20 ['Handbook on European data protection law']; 'EU Charter of Fundamental Rights' (Website Commission) <http://ec.europa.eu/justice/fundamental-rights/charter/index_en.htm> accessed 5 May 2017.

[2] Charter of Fundamental Rights of the European Union, art 51(1).

[3] 'Information society, privacy and data protection' (Website European Union Agency for Fundamental Rights, (FRA)) <http://fra.europa.eu/en/theme/information-society-privacy-and-data-protection> accessed 5 May 2017 [FRA, 'Information society, privacy and data protection'].

[4] FRA, 'Information society, privacy and data protection'; Convention for the Protection of Human Rights and Fundamental Freedoms [1950] ETS No. 5 ['ECHR'].

[5] FRA, 'Information society, privacy and data protection'; Handbook on European data protection law, 15; Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L281/31 ['Directive 95/46/EC']; Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data [1981] ETS No.108 ['CoE Convention 108']; Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authorities and transborder data flows [2001] ETS No. 181 ['Additional Protocol to CoE Convention 108'].

2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.

3. Compliance with these rules shall be subject to control by an independent authority."

6. As stated above, the European Convention on Human Rights, be it via the right to respect for private and family life as embodied in article 8 ECHR, also plays an important role when it comes to the protection of personal data.[6]

Article 8, §1 ECHR stipulates that:

"[e]veryone has the right to respect for his private and family life, his home and his correspondence".

2. Processing of personal data for commercial purposes

7. Under EU law 'personal data' is defined as:

"any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity".[7]

Examples of personal data are: a name, phone number, birth date, home and email address, credit card number, national insurance or employee number, login name, gender and marital status.[8]

8. By 'processing of personal data' is meant:

"any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction".[9]

---

[6] Handbook on European data protection law, 15.
[7] Directive 95/46/EC, art 2(a).
[8] Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council of the adequacy of the protection provided by the EU-U.S. Privacy Shield [2016] OJ L207/1, 8 and 52 ['Privacy Shield Decision']; Directorate-General for Justice and Consumers (Commission), *Guide to the EU-U.S. Privacy Shield* (Publications Office of the European Union 2016), 7 ['Guide to the EU-U.S. Privacy Shield'].
[9] Directive 95/46/EC, art 2(b).

9. The Privacy Shield adequacy decision was adopted in order to facilitate commercial data flows, *i.e.* transfers of data from one company to another, from the Union to the United States.[10] In that regard, the Commission stated that *"[t]ransfers of personal data are an important and necessary part of the trans-atlantic relationship, especially in today's global digital economy"*[11] and *"for new growing digital businesses, such as social media or cloud computing, […] large amounts of data [are] going from the EU to the U.S."*.[12]

3. Mass surveillance and difference between content data and metadata

10. A government is conducting 'mass' or 'bulk' surveillance when it is processing personal data about anyone – suspect or not.[13] In June 2013, Edward Snowden, a former U.S. Intelligence Community officer, revealed that the U.S. National Security Agency (NSA) had set up numerous programmes that operated in such a way.[14] The first Snowden documents disclosed that the NSA collected the call detail records of millions of US customers of Verizon, which is a large telecom provider in America.[15] Those records included information such as the originating and terminating number, the duration of each call, trunk identifiers, etc.[16] This kind of information is so called 'metadata', which is 'data about data'.[17] Not the actual 'content' of the communications itself is acquired, but rather the information that a system uses to operate or data that is a by-product thereof.[18] Nonetheless, a lot of conclusions can be drawn from metadata: where you went, who you called, how long you called, what you purchased, and so on.[19] However, the day after these first revelations, Snowden leaked files which indicated that the U.S. government, via programmes such as PRISM, also gathered a lot of 'content' data of individuals, meaning actual conversations, as it for example had obtained direct access to the servers of giant U.S. internet companies, such as Google, Facebook and Apple.[20]

---

[10] Guide to the EU-U.S. Privacy Shield, 7.
[11] Ibid.
[12] Commission, 'Communication from the Commission to the European Parliament and the Council on Rebuilding Trust in EU-US Data Flows' COM (2013) 846 final, point 1 ['COM (2013) 846 final'].
[13] Bruce Schneier, *Data and Goliath – The Hidden Battles to Collect Your Data and Control Your World* (W. W. Norton & Company Ltd, first edition 2015) 26-27 ['Bruce Schneier, *Data and Goliath – The Hidden Battles to Collect Your Data and Control Your World*'].
[14] <https://edwardsnowden.com/> (Website Edward Snowden) accessed 6 May 2017.
[15] Glenn Greenwald, 'NSA collecting phone records of millions of Verizon customers daily' *The Guardian* (6 June 2013) <https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order> accessed May 2017.
[16] Ibid.
[17] Bruce Schneier, *Data and Goliath – The Hidden Battles to Collect Your Data and Control Your World*, 17.
[18] Ibid.
[19] Bruce Schneier, *Data and Goliath – The Hidden Battles to Collect Your Data and Control Your World*, 21.
[20] Glenn Greenwald and Ewen MacAskill, 'NSA Prism program taps in to user data of Apple, Google and others' *The Guardian* (6 June 2013) < https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data> accessed May 2017; Bruce Schneier, *Data and Goliath – The Hidden Battles to Collect Your Data and Control Your World*, 21.

CHAPTER 1. ADEQUACY EX DIRECTIVE 95/46/EC AS A NECESSARY CONDITION FOR THE TRANSFER OF PERSONAL DATA FROM THE UNION TO A THIRD COUNTRY

A. Introduction

11. In order to transfer personal data, which has been gathered within the European Union, to a third country, European Union law requires that this country ensures an adequate level of data protection. This requirement is a core element of European data protection law since it is laid down in numerous legal instruments adopted by the EU that deal with personal data in some way or another.[21] In this Chapter, however, the meaning of the adequacy requirement is analysed only within the context of Directive 95/46/EC given the relevance of this directive with regard to the EU-U.S. Privacy Shield.

The notion of 'adequacy' is, however, not strictly defined. As a consequence the actual assessment of the adequateness of the data protection regime of a third country is not a straightforward task. Therefore, a careful analysis of this requirement is needed. In any event, the transfer of personal data from the EU to the third country in question is permitted when the outcome of the examination is positive.[22] In the reverse case, the transfer of personal data to the this particular country should in principle be prohibited.[23] However, under certain conditions Directive 95/46/EC allows the transfer of personal data to third countries which do not ensure an adequate level of data protection.[24]

12. On 24 May 2016 Regulation 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) [hereinafter: 'GDPR'] entered into force. However, as this regulation will only apply from 25 May 2018 and the provisions regarding the adequacy requirement laid down in it correspond with the ones laid down in Directive 95/46/EC, only those of the latter will be further examined in this Chapter.

---

[21] E.g.: Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters [2008] OJ L350/60, art 13(1)(d) ['Council Framework Decision 2008/977/JHA']; Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data [2001] OJ L8/1, art 9(1) ['Regulation 45/2001']; Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L119/1, art 45 ['GDPR']; Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA [2016] OJ L119/89, arts 35(1)(d) and 36 ['Directive 2016/680']; Additional Protocol to CoE Convention 108', art 2(2).

[22] Directive 95/46/EC, art 25(1) and recital 56.

[23] Directive 95/46/EC, recital 57.

[24] Directive 95/46/EC, art 26.

13. The structure of this Chapter will be as follows: firstly, the scope and purpose of Directive 95/46/EC will be discussed (B); secondly, the notion of 'adequacy' will be examined (C); thirdly, the levels at which an assessment of 'adequacy' can be done will be addressed (D); fourthly, the exceptions to the adequacy requirement will be analysed (E); and finally, there will be a conclusion summing up the main findings in this Chapter (F).

B. Directive 95/46/EC: purpose, scope and relevance for the EU-U.S. Privacy Shield

14. Directive 95/46/EC was adopted to achieve, through the approximation of national laws on data protection, two closely interlinked objectives: removing the obstacles to flows of personal data within the unified market[25] by ensuring, in all Member States, an equivalently high level of protection of the rights and freedoms of individuals, and in particular the right to privacy, with regard to the processing of such data.[26] Before, differences in the levels of protection afforded in the Member States prevented the transmission of personal data from the territory of one Member State to that of another. Given the importance of such data flows with regard to a number of economic activities at Union level, these differences were considered to form an impediment to the functioning of the internal market.[27] By harmonizing national laws, the transfer of data to other Member States became possible while still protecting personal data.

The same reasoning is applied when personal data is transferred from the EU to a third country: only when this country ensures an adequate level of data protection, there can be a free flow of personal data. In the absence of this requirement, the high standard of European data protection would soon be rendered meaningless, considering the ease with which personal data can move around in international networks nowadays.[28] On top of that, the EU data protection rules could easily be circumvented by transfers of personal data from the European Union to third countries for the purpose of being processed.[29] Hence, the free flow of personal data can, in principle, only be allowed if the European data protection standards are upheld once such data has been transferred. As the EU-U.S. Privacy Shield Decision enables the transfer of personal data from the EU to the U.S., it thus must be proven that the data transferred on the basis of this shield are granted an adequate level of data protection in the U.S (see *infra*).

---

[25] Which comprises also three EEA member countries (Norway, Liechtenstein and Iceland).
[26] Directive 95/46/EC, recitals 7-10; Peter Hustinx, 'EU Data Protection Law: The Review of Directive 95/46/EC and Proposed General Data Protection Regulation' [2014], 9 <https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2014/14-09-15_Article_EUI_EN.pdf> accessed March 2017 ['Peter Hustinx, 'EU Data Protection Law: The Review of Directive 95/46/EC and Proposed General Data Protection Regulation'].
[27] Ibid.
[28] Case C-362/14 *Maximilian Schrems v Data Protection Commissioner* [2015] ECLI:EU:C:2015:650, para 2 ['Schrems']; 'Data transfers outside of the EU' (Website Commission) <http://ec.europa.eu/justice/data-protection/international-transfers/index_en.htm> accessed 18 March 2017.
[29] *Schrems*, para 73.

Directive 95/46/EC applies to the private (commercial) as well as to the public sector and lays down the general legal framework concerning the processing of personal data in the course of an activity which falls within Union law and which is not explicitly excluded from its scope, such as processing operations concerning public security, defence, State security and the activities of the State in areas of criminal law.[30] As the EU-U.S. Privacy Shield is negotiated in order to facilitate transfers of personal data between EU and U.S. companies, it concerns data flows which fall within the scope of directive 95/46/EC.

15. In sum, transfers of personal data for commercial reasons from the EU to the U.S. may only be allowed when the transferred data are guaranteed a level of data protection in the U.S which can be considered adequate in the light of the EU data protection standards as envisaged in Directive 95/46/EC.

C. Notion of 'adequacy'

16. In Directive 95/46/EC, the adequacy requirement is laid down in article 25, §1. It stipulates, more specifically, that:

> *"The Member States shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if, without prejudice to compliance with the national provisions adopted pursuant to the other provisions of the Directive, the third country in question ensures an adequate level of protection".*

Moreover, recital 57 of this directive states that the transfer of personal data which does not ensure an adequate level of protection must be prohibited.

The directive does not define the concept of adequacy as such. However, it does determine, in article 25, §2, that the level of protection afforded by a third country should be assessed in the light of *all the circumstances* surrounding a data transfer operation or set of data transfer operations.[31] These include in particular the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law, both general and sectoral, in force in the third country in question and the professional rules and security measures which are complied with in that country.[32] The European Data Protection Officer (EDPS) observes in that regard that the assessment of adequacy thus requires an evaluation of the intended processing activity itself and of the legal regime, or measures applicable to the recipient.[33]

---

[30] Directive 95/46/EC, art 3(2).
[31] Directive 95/46/EC, art 25(2).
[32] Ibid.
[33] European Data Protection Supervisor, 'The transfer of personal data to third countries and international organisations by EU institutions and bodies' [2014] Position paper, 10 <https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Papers/14-07-14_transfer_third_countries_EN.pdf> accessed 18 March 2017 ['EDPS Position paper data transfers by EU institutions and bodies'].

The Working Party on the Protection of Individuals with regard to the Processing of Personal Data[34] [hereinafter: (Article 29) Working Party] further concretised this requirement by outlining a framework for how the adequacy of protection should be assessed in a particular case.[35] It considers that the data protection regime of a third country should at least comply with a set of *'core' data protection principles* in order to be deemed adequate.[36] These principles consist of both data protection 'content' standards and 'procedural/enforcement' requirements.[37] Data protection rules indeed only contribute to the protection of individuals if there are sufficient means in place for ensuring their effective application.[38] This same functional approach to apply the concept of adequacy is also used by the EDPS.[39] In fact, the assessment of adequacy comes down to an evaluation of the risks posed by the potential transfer of personal data to the fundamental rights and freedoms of individuals and in particular their right to privacy.[40] The use of a basic list of minimum requirements can in that regard serve as a starting point for the analysis of the level of data protection in a certain country.[41] None of these requirements, neither those regarding the 'content' nor the 'procedural/enforcement' ones, may of course be undermined by too broadly formulated exceptions. Article 13 of Directive 95/46/EC states that the Member States may adopt legislative measures to restrict the scope of certain obligations and rights provided for in the directive when such a restriction constitutes a necessary measure to safeguard, amongst others, national security, defence, public security and the prevention, investigation detection and prosecution of criminal offences. However, the Court of Justice of the European Union and the European Court of Human Rights both ruled on several occasions that such legislation must be limited to what is 'strictly necessary'.[42] The lack of (sufficient) limitations in that regard may also prove the inadequacy of the data protection regime of a country.[43] The actual substance of the basic data protection principles as well as the case-law of the CJEU and the ECtHR regarding the said exceptions will be discussed in Chapter 2.

---

[34] The Working Party on the Protection of Individuals with regard to the Processing of Personal Data is established by article 29 of directive 95/46/EC and its tasks are laid down in article 30 of that directive.
[35] Working Party on the Protection of Individuals with regard to the Processing of Personal Data, 'Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive' [1998] Working Document WP12, 3 <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/1998/wp12_en.pdf> accessed 18 March 2017 ['Working Party 29 WP12'].
[36] Working Party 29 WP12, 5
[37] Ibid.
[38] Ibid.
[39] EDPS Position paper data transfers by EU institutions and bodies, 10.
[40] Ibid.
[41] Ibid.
[42] Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, The Commissioner of the Garda Síochána, Ireland and the Attorney General, and Kärntner Landesregierung, Michael Seitlinger, Christof Tschohl and Others* [2014] ECLI:EU:C:2014:238, para 52 ['*Digital Rights Ireland*']; *Schrems*, para 92; Joined Cases C-203/15 and C-698/15 *Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others* [2016] ECLI:EU:C:2016:970, para 96 ['*Tele2 Sverige AB*'].
[43] *Schrems*, paras 79-98.

17. The EDPS also stated that an adequate system does not necessarily require the existence of legal rules and procedures, but can also be established by other 'measures', such as codes of conduct, internal rules, security controls and audit mechanisms.[44]

18. In the *Schrems* case of 6 October 2015 the Grand Chamber of the Court of Justice of the European Union recently confirmed that the examination (*in casu* by the Commission) of the level of protection afforded by a third country must include an assessment of the content of the applicable rules in that country resulting from its domestic law or international commitments it has entered into as well as the practice designed to ensure compliance with those rules, since, as noted above, all circumstances have to be taken into account.[45] Furthermore, the Court explicated that the adequacy requirement does not require a third country to ensure an identical level of protection of fundamental rights and freedoms, but rather a level of protection that is *essentially equivalent* to that guaranteed within the European Union by virtue of Directive 95/46/EC read in the light of the Charter.[46] The latter is now also expressly stated in recital 104 of the General Data Protection Regulation.

D. Assessment of 'adequacy'

19. As stated above, Directive 95/46/EC requires the Member States to adopt provisions at national level which provide that the transfer of personal data to a third country is only allowed when that country ensures an adequate level of data protection.[47] This means that the adequacy of the data protection regime of a third country has to be established before the transfer of data can take place. The question then arises as to who should assess whether a certain country assures an adequate level of protection. As will be explained below, this assessment can be carried out at different levels and hence results in different legal effects.[48]

1. Adequacy decision by the European Commission

20. Article 25, §6 of directive 95/46/EC provides that:

> *"The Commission may find (…) that a third country ensures an adequate level of protection within in the meaning of §2 of this Article, by reason of its domestic law or of the international commitments it has entered into (…) for the protection of private lives and basic freedoms and rights of individuals".*

[44] EDPS Position paper data transfers by EU institutions and bodies, 12.
[45] *Schrems*, para 75.
[46] *Schrems*, para 73.
[47] Directive 95/46/EC, art 25(1).
[48] EDPS Position paper data transfers by EU institutions and bodies, 12.

An adequacy decision by the European Commission pursuant to this article is binding upon all Member States and enables the free flow of data from the EU to a particular third state within the context of activities which fall within the scope of directive 95/46/EC.[49] For the controller who wishes to transfer data to a third country, such a decision is of great importance as no additional measures will have to be taken in relation to the data transfer in order to be in compliance with the national provisions adopted pursuant to article 25, §1 of directive 95/46/EC (see nos. 27-30).[50] Accordingly, an adequacy finding by the Commission helps to oversee certain data flows to the third country in question.[51]

With respect to the United States, the European Commission adopted the Commission implementing decision (EU) 2016/1250 pursuant to Directive 95/46/EC of the European Parliament and the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield on 12 July 2016 in this regard. According to article 1, §1 of this decision, the United States ensures an adequate level of protection for personal data transferred from the Union to organisations in the United States under the EU-U.S. Privacy Shield for the purposes of article 25, §2 of Directive 95/46/EC. This claim will be examined and assessed in Chapter 3.

21. The Commission may, however, also find, as stipulated in article 25, §4, that a third country does not, either in general or sectoral, ensure an adequate level of protection. In that case, the Member States are obliged to take the necessary measures in order to prevent any transfer of data of the same type to the third country in question.[52] However, under certain conditions Directive 95/46/EC allows the transfer of personal data to third countries even when the level of data protection in this country is considered inadequate (*see infra*).[53]

2. Adequacy assessment by the controller, the national data protection authority or any other body established to fulfil this task

22. In the absence of a decision *ex* article 25, §6 by the European Commission, a case-by-case approach whereby the assessment of adequacy in relation to individual transfers or individual categories of transfers is required.[54] How these cases are dealt with depends on the way the individual Member States have transposed article 25 into national law[55]: there might be given a specific role to the national supervisory authority in this regard; some other body might have been established specifically to fulfil this task; or

[49] EDPS Position paper data transfers by EU institutions and bodies, 12-13; the effect of such a decision extends to three EEA member countries (Norway, Liechtenstein and Iceland).
[50] EDPS Position paper data transfers by EU institutions and bodies, 12.
[51] *Schrems*, para 69.
[52] Directive 95/46/EC, art 25(4).
[53] Directive 95/46/EC, art 26.
[54] Working Party 29 WP 12, 26.
[55] Working Party 29 WP 12, 27.

the controller might even be responsible himself to conduct the assessment.[56] However, having in mind the large number of transfers of personal data departing from the European Union every day and the abundance of actors involved in these transfers, it will not be practicable to examine all these cases one by one.[57] For a controller in particular, it might not always be doable to carry out an entire assessment of adequacy with regard to a third country.[58] In such cases, it is often more feasible for the controller to assume the inadequacy of the data protection regime of a particular country and adduce adequate safeguards with respect to protection of the rights of individuals whose data will be transferred and as regards the exercise of these rights (see nos. 27-30).[59]

E. Transfer of personal data to countries not ensuring an adequate level of data protection

23. As stated above, there are cases where there is no adequate level of data protection in a third country, or where there has not yet been made an adequacy assessment, or where such an assessment is simply inconvenient.[60] Recital 57 of Directive 95/46/EC stipulates that the transfer of personal data to a third country must be prohibited in those cases. On the other hand, it is stated in recital 58 that provisions should be made for exemptions from this prohibition in certain circumstances. Accordingly, article 26 sets out the conditions under which derogations to the adequacy requirement can be allowed. These derogations can be subdivided into two categories: the first type of derogations is laid down in article 26, §1 and involves an exhaustive list of specific exceptions. In this case, no additional measures are required upon transfer; the second is mentioned in article 26, §2 and concerns all other transfers of personal to third countries which do not ensure an adequate level of data protection. These transfers may only be conducted where the controller adduces adequate safeguards.[61]

1. Specific exceptions

24. In article 26, §1 is stipulated that, by way of derogation from Article 25 and save where otherwise provided by domestic law governing particular cases, Member States shall provide that a transfer or a set of transfers of personal data to a third country that does not ensure an adequate level of protection within the meaning of Article 25 (2) may take place on specific conditions. These include, amongst others, situations where the data subject has unambiguously given his/her consent, or where the transfer is necessary for the performance of a contract concluded with or in the interest of the data subject, or where the transfer is necessary or legally required on important public interest grounds.[62]

---

[56] Working Party 29 WP12, 27.
[57] Working Party 29 WP12, 26.
[58] EDPS Position paper data transfers by EU institutions and bodies, 13.
[59] Directive 95/46/EC, art 26(2); EDPS Position paper data transfers by EU institutions and bodies, 13.
[60] EDPS Position paper data transfers by EU institutions and bodies, 18.
[61] Mutatis mutandis: EDPS Position paper data transfers by EU institutions and bodies, 14.
[62] Directive 95/46/EC, art 26(1)(a)-(d).

25. The The Article 29 Working Party observed that, in spite of the fact that this provision might seem ambiguous in the light of the basic principle of adequacy, there are good reasons which justify the said exceptions. More specifically, it points at the fact that the expansion of international trade sometimes requires flexibility of international data transfers. Furthermore, the Working Party considers that the specific exceptions listed in article 26, §1 concern situations in which an exemption from the adequacy requirement can be considered 'appropriate'. This because it involves *"cases where risks to the data subject are relatively small or where other interests (public interests of those of the data subject himself) override the data subject's right to privacy".* Moreover, they must be interpreted in a restrictive way since they constitute exemptions form a general principle.[63] Article 29 Working Party noted, however, that, in practice, controllers tend to make use of these exceptions as a first option, even in circumstances where this would be inappropriate. Therefore, the Working Party examined the specific exemptions one by one in order to determine their scope and meaning in a uniform and strict manner so as to avoid any future misuse.[64] It goes, however, beyond the extent of this thesis to address all specific derogations in detail.

26. In any event, when a transfer or a set of transfers of personal data to a third country can be based on one of the conditions laid down in article 26, §1, the controller does not have to adduce additional safeguards with respect to the protection of these data upon transfer.[65]

2. Adducement of adequate safeguards

27. On the contrary, in article 26, §2 is stated that:

> *"Without prejudice to paragraph 1, a Member State may authorize a transfer or a set of transfers of personal data to a third country which does not ensure an adequate level of protection within the meaning of Article 25, §2, where the controller adduces adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals and as regards the exercise of corresponding rights; such safeguards may in particular result from appropriate contractual clauses".*

It thus concerns cases where a third country does not ensure an adequate level of data protection and which do not fall within one of the exceptions laid down in article 26, §1. As the notion of 'adequacy', the concept of 'adequate safeguards' is, not defined in Directive 95/46/EC. According to the EDPS, 'adequate safeguards' should be understood as *"data protection guarantees which are created for the*

---

[63] Working Party of on the Protection of Individuals with regard to the Processing of Personal Data, 'A common interpretation of Article 26 (1) of Directive 95/46/EC of 24 October 1995' [2005] Working Document WP114, 7 <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2005/wp114_en.pdf> accessed 18 March 2017 ['Working Party 29 WP114'].
[64] Working Party 29 WP114, 7.
[65] EDPS Position paper data transfers by EU institutions and bodies, 14.

specific situation, and which do not already exist in the recipient's legal system".[66] As stated in article 26, §2, these safeguard may in particular result from contractual clauses. Another typical example in that regard are binding corporate rules.[67] These instruments are used to remedy the inadequacy of the level of data protection in the data's country of destination.[68]

28. For a contractual provision to be considered 'adequate', it must offer sufficient compensation for the lack of adequate data protection principles in the recipient third country and must thus include the essential elements of protection which are absent in a specific case.[69] The contractual solution must result in an obligation on the recipient to ensure that the 'core' data protection rules are complied with when the transferred data is processed in a third country concerned.[70] As mentioned before, these 'core' principles will be discussed in Chapter 2.

Consequently, any set of contractual clauses has to be very detailed and properly adapted to the data transfer in question.[71] Moreover, article 26, §2 stipulates that such transfers require authorization by the Member States. Clearly, the use of contracts to remedy the lack of adequate data protection in a certain third country will often be complex and difficult.[72] Making use of standard contractual clauses (SCCs) may offer a solution in that respect. At Member State level, the national data protection authorities may be given the responsibility to provide guidance in that regard.[73] At Union level, the Commission has expressly been granted the power to decide that certain standard contractual clauses offer sufficient safeguards as required by article 26, §2.[74] In that case, the Member States have to take the necessary measures to comply with the Commission's decision.[75] The effect of such a decision is that by incorporating the standard contractual clauses into a contract, personal data may be transferred from the EU to a third country which does not ensure an adequate level of data protection.[76] So far, the European Commission has issued three sets of standard contractual clauses: two for transfers from data controllers to data controllers established outside the EU and one set for the transfer from data controllers to data processors established outside the EU.[77]

---

[66] EDPS Position paper data transfers by EU institutions and bodies, 18.
[67] Ibid.
[68] Ibid.
[69] Working Party 29 WP12, 16.
[70] Working Party 29 WP12, 17.
[71] Working Party 29 WP12, 22.
[72] Working Party 29 WP12, 28.
[73] Ibid.
[74] Directive 95/46/EC, art 26(4).
[75] Ibid.
[76] Commission, 'Frequently Asked Questions relating to transfers of personal data from the EU to third countries' [2009], 23 <http://ec.europa.eu/justice/data-protection/international-transfers/files/international_transfers_faq.pdf> accessed 18 March 2017.
[77] 'Model Contracts for the transfer of personal data to third countries' (Website Commission) <http://ec.europa.eu/justice/data-protection/international-transfers/transfer/index_en.htm> accessed 18 March 2017.

29. Article 26, §2 can also be implemented in practice through the adoption of binding corporate rules (BCRs). Binding corporate rules are internal rules drawn up by multinational groups of companies which define their global policy regarding the protection of personal data and which are specifically directed at entities of these groups located in countries not ensuring an adequate level of data protection.[78] That way, a corporate group is able to transfer personal data internally while still providing adequate protection in the light of the European standards concerning the processing of such data, regardless of the location of their entities.[79] The Article 29 Working Party has set out the criteria which binding corporate rules should meet.[80]

As is the case with regard to contractual provisions, article 26, §2 requires the authorisation of transfers of personal data allegedly justified on the basis of the adoption of BCRs by the Member State from whose territory such data are leaving the EU. Consequently, national data protection authorities may also be given an important role in approving BCRs.[81] As corporate groups might as well be interested in submitting draft binding corporate rules for the approval of several data protection authorities, the Article 29 Working Party drew up a coordinated procedure in that regard.[82] This procedure makes it possible for multinationals to submit their draft BCRs to only one lead authority, which then will take the necessary steps to obtain the approval of all data protection authorities concerned.[83]

30. In sum, when personal data have to be transferred to third countries which do not ensure an adequate level of data protection for purposes which do not fall within the scope of article 26, §1 of Directive 95/46/EC, the data controller can adduce adequate safeguards in order to make such transfers permissible after all.

---

[78] 'Binding Corporate Rules' (Website Commission) <http://ec.europa.eu/justice/data-protection/article-29/bcr/index_en.htm> accessed 18 March 2017.
[79] Ibid.
[80] 'BCR Procedure' (Website Commission) <http://ec.europa.eu/justice/data-protection/international-transfers/binding-corporate-rules/procedure/index_en.htm> accessed 18 March 2017.
[81] Working Party on the Protection of Individuals with regard to the Processing of Personal Data, 'Transfers of personal data to third countries: Applying Article 26 (2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers' [2003] Working document WP74, 5 <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2003/wp74_en.pdf> accessed 18 March 2017 ['Working Party 29 WP74'].
[82] Working Party on the Protection of Individuals with regard to the Processing of Personal Data, 'Setting Forth a Co-Operation Procedure for Issuing Common Opinions on Adequate Safeguards Resulting From "Binding Corporate Rules"' [2005] Working document WP107 <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2005/wp107_en.pdf> accessed 18 March 2017 ['Working Party 29 WP107'].
[83] 'BCR Procedure' (Website Commission) <http://ec.europa.eu/justice/data-protection/international-transfers/binding-corporate-rules/procedure/index_en.htm> accessed 18 March 2017.

F. Conclusion

31. The adequacy requirement aims at maintaining a high level of data protection whenever personal data is transferred to a country outside of the EU and is consequently one of the essential elements of European data protection law. Despite the fact that the notion of 'adequacy' is not defined in Directive 95/46/EC, it is clear that in order to conclude that the data protection framework in place in a third country can be considered 'adequate', at least the 'core' principles of EU data protection law should be complied with in this particular country. Moreover, the protection provided by these principles should not be undermined by the provision, in favour of the government, of very broad derogations thereto. Accordingly, the Court of Justice of the European Union interprets the term 'adequate' as meaning 'essentially equivalent', rather than 'identical'. The European Commission is entitled, on the basis of article 25, §6 of Directive 95/46/EC, to establish that the data protection regime in a third country, by reason of its domestic law or of the international commitments it has entered into, can indeed be considered 'adequate'.

In certain circumstances, however, Directive 95/46/EC foresees in specific exceptions to the adequacy requirement. Despite the fact that their use may prove to be very convenient in some instances, they should in any event be interpreted in a strict manner in order to avoid any potential abuse. Furthermore, the directive provides the possibility for data controllers who wish to transfer their data to countries which do not ensure an adequate level of data protection, to adduce adequate safeguards to remedy the said lack of adequacy. Two typical examples in that regard are (standard) contractual clauses (SCC) and binding corporate rules (BCRs).

In sum, protection of personal data should not end at the European borders.

CHAPTER 2. SUBSTANTIVE EU DATA PROTECTION STANDARDS AND PERMISSIBILITY OF DEROGATIONS

A. Introduction

32. As explained in Chapter 1, the adequacy requirement is an important principle of EU data protection law. Only when a third country is considered to have a system in place which protects personal data in an adequate manner, a transfer of personal data to that country is permissible.

33. The adequacy of a data protection regime is assessed by means of a comparison between the substantive EU data protection standards and those in place in a third country. However, as stated in Chapter 1 (see no. 16) and as is apparent from the case-law of the Court of Justice, the adequacy of a data protection regime equally depends on the formulation of the possible derogations to the substantive data protection standards. This because such exceptions are to be regarded as an interference with the right to privacy and the right to data protection and consequently must prove to be justified (see no. 74-82). In its case law, the Court of Justice accordingly also clarified the conditions which have to be fulfilled in order to make such exceptions permissible. In this respect, the jurisprudence of the European Court of Human Rights can also not be disregarded.

34. The structure of this Chapter will be as follows: firstly, the substantive EU data protection standards will be discussed (B); then, the permissibility of derogations with regard to these standards will be examined (C); and finally, there will be a conclusion summing up the main findings in this Chapter (D).

B. Substantive EU data protection standards

35. Already in 1997, the Article 29 Working Party compilated a set of *'core' principles* of EU data protection law in order to facilitate the assessment of the adequacy of the data protection regime in place in a third country.[84] This basic list of principles consists of 'content' standards as well as 'procedural/enforcement' requirements.[85] The latter were included by the Working Party as it considered that data protection rules only contribute to the protection of individuals if they are followed in practice.[86]

36. This list was drawn up using the provisions laid down in Directive 95/46/EC as a starting point, and bearing in mind those set out in other international data protection texts, such as the Council of Europe Convention 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data of 28 January 1981 of the Council of Europe [hereinafter: Convention 108], the 1980 OECD

---

[84] Working Party on the Protection of Individuals with regard to the Processing of Personal Data, 'First orientations on Transfers of Personal Data to Third Countries – Possible Ways Forward in Assessing Adequacy' [1997] Discussion Document WP4, 5-7 <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/1997/wp4_en.pdf> accessed 28 March 2017 ['Working Party 29 WP4'].
[85] Working Party 29 WP4, 5-7.
[86] Working Party 29 WP4, 5.

Guidelines on the Protection of Privacy and Transborder Flows of Personal Data and the UN Guidelines for the Regulation of Computerized Personal Data Files of 1990.[87]

37. Convention 108 deserves particular attention as it was the first internationally binding instrument on the matter.[88] Already in the beginning of the 1980s, the necessity to reconcile the fundamental values of the respect for privacy and the free flow of information between the territories and the peoples of the Contracting Parties was recognised in the convention.[89] In that sense, and since the principles set out in Directive 95/46/EC further substantiate and amplify those contained in Convention 108[90], this convention should be seen as the predecessor of Directive 95/46/EC. It is interesting to note, however, that the scope of application of Convention 108 differs somewhat from the one of Directive 95/46/EC. In principle, Convention 108 applies to automated personal data files and automatic processing of personal data both in the public and private sectors.[91] However, the convention allows the Parties to exclude certain categories of personal data under particular conditions.[92] Directive 95/46/EC on the other hand, applies to all types of processing, whether it is automatic or not, but excludes processing of personal data in the course of certain activities (see no. 14).[93]

38. In any event, the provisions set out in Directive 95/46/EC rely on the ones established in Convention 108 and in that way the Council of Europe data protection principles have been introduced at European level. Today, these principles form a well-established part of EU data protection law in general. For example, when the EU legislator observed that, due to the developments in the telecommunications sector, specific requirements concerning protection of personal data and privacy where needed in that sector, Directive 97/66/EC was adopted and later, as an update, Directive 2002/58/EC.[94] These directives simply translate the principles set out in Directive 95/46/EC into specific rules for the said sector and, accordingly, this directive should thus be regarded as the *lex generalis* for what concerns EU data protections law.[95] For what follows, it suffices however to refer to the list of basic requirements as

[87] Working Party 29 WP4, 5.
[88] Peter Hustinx, 'EU Data Protection Law: The Review of Directive 95/46/EC and Proposed General Data Protection Regulation', 4.
[89] CoE Convention 108, preamble.
[90] Directive 95/46/EC, recital 11.
[91] CoE Convention 108, art 3(1).
[92] CoE Convention 108, art 3(2).
[93] Directive 95/46/EC, art 3.
[94] Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector [1997] OJ L024/1, recital 3; Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) [2002] OJ L201/37, recital 4 ['Directive 2002/58/EC (e-Privacy Directive)'].
[95] Directive 2002/58/EC (e-Privacy Directive), recital 4.

compiled by the Article 29 Working Party[96] and to the corresponding articles encompassing these principles as laid down in Directive 95/46/EC.

39. In Directive 95/46/EC, a distinction is made between the different actors that can somehow be involved in the processing of personal data.[97] Depending on their capacity, these actors will be responsible to a greater or a lesser extent for compliance with the data protection rules as laid down in the directive.[98] This division of responsibilities is also determining to the way in which data subjects can exercise their rights.[99] The most important concepts in that regard are that of the data 'controller' and that of the data 'processor'.[100] A controller is *"the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing"*.[101] A processor on the other hand is *"a natural or legal person , public authority, agency or any other body which processes personal data on behalf of the processor"*.[102] The controller has been allocated the greatest responsibility: the controller is responsible for compliance with articles 6, §1, 10-12, 14, 15-21 and 23.[103] The processor has been allocated responsibility in articles 16-17.[104] The precise obligations laid down in these different articles will be discussed hereinafter.

1. Content principles

40. Data protection rules are established to protect the individuals whose data are being processed.[105] According to the Article 29 Working Party, this protection is typically achieved through a combination of rights for the data subject and obligations on those processing data, or those exercising control over such processing.[106] These rights and obligations can be regarded as the 'content' principles of data protection law. The Working Party first identified generic 'content' principles, which apply to all types of processing. In a second instance, it also listed 3 additional principles which apply to only specific types of processing.[107]

---

[96] Working Party 29 WP4, 6-7.
[97] Directive 95/46/EC, art 2(d)-(g).
[98] Working Party on the Protection of Individuals with regard to the Processing of Personal Data, 'Opinion 1/2010 on the concepts of "controller" and "processor" [2010] Opinion WP169, 2 <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_en.pdf> accessed 26 April 2017 ['Working Party 29 WP169'].
[99] Ibid.
[100] The concepts of 'third party' and 'recipient, encompassed respectively in point (f) and (g) of article 2 of Directive 95/46/EC, will not be discussed in the context of this thesis.
[101] Directive 95/46/EC, art 2(d).
[102] Directive 95/46/EC, art 2(e).
[103] Working Party 29 WP169, 4-5.
[104] Working Party 29 WP169, 5.
[105] Working Party 29 WP4, 5.
[106] Ibid.
[107] Working Party 29 WP4, 6-7.

a. Purpose limitation

41. The first principle that has been identified by the Working Party is the principle of 'purpose limitation'.[108] The purpose limitation principle should be regarded as a cornerstone of data protection and is an essential first step for applying other data quality requirements.[109] Article 6, §1, b of Directive 95/46/EC stipulates more specifically that *"personal data must be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes (...)"*. This principle thus has two components.[110]

The first one entails in essence that the controller must carefully assess what purpose or purposes the personal data will be used for[111], that these purposes should be 'in accordance with the law' in the broadest sense of the word, and in particular in accordance with article 7 of Directive 95/46/EC, which lays down the criteria for making data processing legitimate,[112] and that these purposes must be clearly revealed, explained or expressed in some intelligible form.[113]

At the same time, the second component recognizes that data which have already been collected, may also prove to be useful for other purposes, which were not previously specified and which could not have been expected at the time of initial sharing of personal data.[114] From the wording of article 6, §1, b of Directive 95/46/EC it must be concluded that a certain degree of additional use should be regarded permissible as long as this added use is not considered to be 'incompatible' with the initial purpose of collection.[115] This assessment is not always easy to make and will often imply a multi-criteria evaluation. Therefore, the Article 29 Working Party has set out a non-exhaustive list of key factors in this regard.[116] These relate to the relationship between the purposes for which the data have been collected and the purposes of further collection, to the context in which the data have been collected, the reasonable expectations of the data subjects as to their future use, to the nature of the data, the impact of the further processing on the data subjects, and to the safeguards applied by the controllers to ensure fair processing and to prevent any undue impact on the data subjects.[117] These factors will, however, not further be discussed in the context of this thesis.

---

[108] Working Party 29 WP4, 6.
[109] Working Party on the Protection of Individuals with regard to the Processing of Personal Data, 'Opinion 03/2013 on purpose limitation' [2013] Opinion WP203, 4 <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf> accessed 29 March 2017 ['Working Party 29 WP203'].
[110] Working Party 29 WP203, 4.
[111] Working Party 29 WP203, 15.
[112] Working Party 29 WP203, 19-20.
[113] Working Party 29 WP203, 17.
[114] Working Party 29 WP203, 4.
[115] Working Party 29 WP203, 5.
[116] Working Party 29 WP203, 23-27.
[117] Ibid.

b. Proportionality

42. The second principle is laid down in article 6, §1, c of Directive 95/46/EC, which states that *"personal data must be adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed".* This is the principle of 'proportionality'.[118] Specification of the purpose is thus a prerequisite for the application of the proportionality test.[119]

This means that the categories of data chosen for processing must be necessary in order to achieve the explicated purpose or purposes of the processing operations. Hence, a controller should only collect data which can be considered directly relevant for the pursued purposes.[120]

c. Data quality

43. The data quality principle[121], as a third standard, is laid down in article 6, §1, d of Directive 95/46/EC and entails that the data must be *"accurate and where necessary, kept up to date"*. Furthermore, it is stated that *"every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified".*[122]

A data controller thus may not use personal information without ensuring with reasonable certainty that the data are accurate and up to date.[123] Moreover, and as is the case with the principle of 'proportionality', compliance with this obligation also requires the application of the principle of 'purpose limitation' in advance.[124] Depending on the purpose of the processing, updating stored data might either be an absolute necessity or even be legally prohibited.[125]

d. Data retention limitation principle

44. The 'data retention limitation' principle, as a fourth principle, though not expressly mentioned by Article 29 Working Party, is encompassed in article 6, §1, e of Directive 95/46/EC. According to this principle *"personal data must be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they were further processed"*.[126] On the other hand, Member States are obliged, under this principle, to lay down

[118] Working Party 29 WP4, 6.
[119] Working Party 29 WP203, 4.
[120] Handbook on European data protection law, 70.
[121] Working Party 29 WP4, 6.
[122] Directive 95/46/EC, art 6(1)(d).
[123] Handbook on European data protection law, 71.
[124] Working Party 29 WP203, 4.
[125] Handbook on European data protection law, 72.
[126] Directive 95/46/EC, art 6(1)(e).

"appropriate safeguards for personal data stored for longer periods for "historical, statistical or scientific use"".[127]

e. Transparency

45. The fifth principle relates to the information which the controller or his representative must provide to a data subject. Article 29 Working Party refers to this obligation as the 'transparency' principle.[128] Article 10 and 11 of Directive 95/46/EC stipulate the types of information which should be made available. Article 10 relates to the information that should be provided in cases of collection of data directly from the data subject, while article 11 specifies the information that should be provided, at the time of undertaking the recording of personal data or if a disclosure to a third party is envisaged, no later than the time when the data are first disclosed, where the data have not been obtained from the data subject. In both cases, the controller or his representative must acquaint the data subject with at least the identity of the controller or his representative, with the purposes of the processing for which the data are intended, or with any further information insofar that is considered necessary to safeguard fair processing having regard to the specific circumstances in which the data are collected, such as the recipients or categories of recipients, the existence of the right of access to and the right to rectify the data concerning him, and in case of article 11, also the categories of data concerned.[129]

46. Article 21 of Directive 95/46/EC also requires the Member States to take measures to ensure that certain information relating to processing operations are publicized or, depending on the circumstances, at least made available upon request of the data subject.[130]

f. Data security and confidentiality of processing

47. The sixth principle regards the security of processing of personal data.[131] In that respect, the first paragraph of article 17 of Directive 95/46/EC states that *"the controller must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing".* The second clause of this paragraph determines that such measures have to ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected and this

---

[127] Ibid.
[128] Working Party 29 WP4, 6.
[129] Directive 95/46/EC, arts 10-11; Article 11(2) of Directive 95/46/EC stipulates that information does not have to be provided where, in particular for processing for statistical purposes or for the purposes of historical or scientific research this would prove to be impossible or would involve a disproportionate effect or if recording or disclosure is expressly laid down by law. In that case, however, the Member States shall provide appropriate safeguards.
[130] Directive 95/46/EC, art 21(2)(3) and 19(1)(a)-(e).
[131] Working Party 29 WP4, 6.

bearing in mind the state of the art and the cost of their implementation. A processor, carrying out the processing on behalf of the controller, must also have sufficient guarantees in place in this respect.[132]

Since security measures protecting personal data cannot be defined generically for all processing operations of personal data, there is a need for a specific framework to assess the risks posed by the processing of personal data in order to define the necessary measures in this regard.[133] According to the EDPS, such a framework is referred to as 'Information Security Risk Management (ISRM) process'.[134] In essence, the ISRM is a tool to identify and evaluate risks related to the processing of personal data in order to facilitate the determination and the adoption of appropriate security measures.[135] This tool can also be used to manage the security of information in general, rather than merely in the context of securing personal data.[136] The details of the ISRM process will however not be discussed in the context of this thesis.

Article 17 of Directive 95/46/EC explicitly mentions risks to confidentiality ('unauthorised disclosure or access'), integrity ('unlawful', 'accidental', or 'alteration') and availability ('accidental or unlawful destruction or accidental loss'), however indicates that other risks also have to be taken into account ('all other unlawful forms of processing').[137] The ones explicitly mentioned consequently do not constitute an exhaustive list.[138] At the same time, however, these listed risks do not necessarily occur with regard to all processing operations concerning personal data.[139] Accordingly, a specific framework, such as the ISRM is essential.[140]

48. The secure processing of data is further safeguarded by article 16 of Directive 95/46/EC on the 'confidentiality of processing'.[141] According to this article, *"any person acting under the authority of the controller or of the processor, including the processor himself, who has access to personal data must not process them except on instructions from the controller, unless he is required to do so by law".*

Article 16 thus only concerns confidentiality within the context of a superior-subordinate relationship.[142] It requires subordinates to only use personal data entrusted to them in accordance with the instructions

---

[132] Directive 95/46/EC, art 17, (2)-(3).
[133] European Data Protection Supervisor, 'Guidance: Security Measures for Personal Data Processing, article 22 of Regulation 45/2001' [2016] Guidance document, 2 <https://edps.europa.eu/sites/edp/files/publication/16-03-21_guidance_isrm_en.pdf> accessed 30 March 2017 ['EDPS Guidance document on security measures for personal data processing'].
[134] EDPS Guidance document on security measures for personal data processing, 6.
[135] EDPS Guidance document on security measures for personal data processing, 6-8.
[136] EDPS Guidance document on security measures for personal data processing, 5.
[137] EDPS Guidance document on security measures for personal data processing, 9.
[138] Ibid.
[139] Ibid.
[140] Ibid.
[141] Working Party 29 WP4, 6; Handbook on European data protection law, 93.
[142] Handbook on European data protection law, 94.

given by their superior.[143] Non-compliance with this requirement is punishable under criminal law in many European countries.[144]

49. The carrying out of processing by way of a processor must be governed by a contract or a legal act binding the processor to the controller.[145] In particular, this contract must stipulate that the processor shall only act on instructions from the controller ('confidentiality of communications')[146] and that rules on data security as stipulated in article 17, §1 shall also be incumbent on the processor.[147] The obligation thus concerns the controller as well as the processor.

g. Rights of access, rectification and opposition

50. Seventhly, the Article 29 Working Party summed up a couple of rights that must be granted to the data subject.[148] The rights of access and rectification are included in article 12 of Directive 95/46/EC, while the data subject's right to oppose the processing of his data is laid down in article 14 of the directive. More specifically, article 12, (a) gives the data subject the right to obtain certain information concerning the processing, such as confirmation as to whether or not data relating to him are being processed, the purposes of the processing, and communication of the data undergoing processing. Article 12, (b) grants data subjects the right to obtain the rectification, erasure or blocking of processing of personal data, in particular where the concerned data are inaccurate or incomplete. Article 14 stipulates in what circumstances a data subject can object to the processing of its data. More specifically, it provides for the possibility of objection based on compelling legitimate grounds relating to the particular situation of the data subject[149] and where the controller anticipates the processing for purposes of direct marketing.

h. Restrictions on onward transfers – adequacy requirement

51. The last generic EU data protection 'content' principle that has been identified by Article 29 Working Party relates to the transfers of personal data from the destination third country to a second third country.[150] According to the Working Party, this second third country should also uphold adequate data protection standards.[151] In short, this means that the initial third country, to which personal data gathered within the EU is transferred, should also apply the adequacy requirement as laid down in article 25 of

[143] Ibid.
[144] Ibid.
[145] Directive 95/46/EC, art 17(3).
[146] Handbook on European data protection law, 94.
[147] Directive 95/46/EC, art 17(3).
[148] Working Party 29 WP4, 6.
[149] And this at least in the cases referred to in Article 7 (e) and (f) of Directive 95/46/EC.
[150] Working Party 29 WP4, 6.
[151] Ibid.

Directive 95/46/EC. Only in the situations stipulated in article 26, §1 exceptions to this requirement could be allowed.[152]

i. Additional principles which apply to specific types of processing

52. Lastly, the list of requirements also includes some additional principles which only apply to specific types of processing.[153]

(1) Sensitive data

53. The first additional principle concerns the processing of special categories of data, which can be regarded as 'sensitive'.[154] In this regard, article 8, §1 in principle prohibits *"the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership and the processing of data concerning health or sex life".* However, the second paragraph of this article nonetheless allows the processing where additional safeguards are put in place.[155] These include amongst others the situation where the data subject has explicitly given its consent or where the processing is necessary for the vital interests of the data subject.[156]

(2) Direct marketing

54. The second principle relates to the processing of personal data for the purpose of direct marketing and forms a part of a data subject's 'right to oppose' as discussed above (see no. 50).[157] More specifically, article 14, (b) requires the Member State to grant a data subject the right to object where its data is anticipated to be processed for the purposes of direct marketing.[158]

(3) Automated individual decision

55. The third principle regards decisions which are based on processing operations which are purely automated. Article 12, (c) of Directive 95/46/EC grants an individual the right to get acquainted with the logic involved in any automatic processing concerning him and in particular where a decision such as referred to in article 15, §1 the directive is taken based on such automated processing. Article 15, §1 requires the Member States to grant every person the right not to be subject to "*a decision which produces legal effects concerning him or significantly affects him and which is based solely on automated*

[152] Ibid.
[153] Working Party 29 WP4, 6-7.
[154] Working Party 29 WP4, 6.
[155] Ibid.
[156] Directive 95/46/EC, art 8(2)(a)-(b).
[157] Working Party 29 WP4, 7.
[158] Ibid.

processing of data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc". Paragraph 2 of that article sets out under which conditions a data subject nevertheless may be subjected to such a decision.

2. Procedural/enforcement mechanisms

56. As stated above, a third country does not only has to have 'content' principles in place but also needs to ensure that these principle are enforceable in practice. The Article 29 Working Party observed in that regard that there is a broad consensus among European countries regarding the fact that data protection principles should be embodied in law.[159] That way, non-compliance with these principles can be easily sanctioned and can give individuals a right to be compensated for damage where appropriate.[160] Moreover, Directive 95/46/EC foresees in the establishment, in each Member State, of independent 'supervisory authorities' with monitoring and complaint investigation powers.[161] This additional procedural mechanism initially did not form a part of the data protection rules set out by the Council of Europe, as it is not foreseen in Convention 108. However, in 2001 this mechanism has been included in the Additional Protocol to this convention.[162]

The Working Party also noted that those procedural mechanisms are not necessarily common in other parts of the world and can also not be regarded as inherently necessary for a data protection regime to be adequate. [163] Therefore, it decided to make reference to their underlying objectives rather than simply listing all European enforcement requirements in this regard.[164] For reasons of clarity, and since the measures set out in Directive 95/46/EC can still be seen as an example, the European standards in this regard have been included in this analysis nonetheless.

j. Good compliance

57. Firstly, the data protection system must deliver a good level of compliance with the 'content' rules.[165] The Working Party considers that this depends essentially on two closely linked factors: the degree of awareness among data controller of their obligations and among data subjects of their rights and the means of enforcing them, combined with the existence of effective sanctions which can successfully dissuade non-compliance with the data protection rules.[166] The effectiveness of such sanctions will be deemed demonstrated when the system in question provides for the direct verification of the rules by

[159] Working Party 29 WP4, 5 and 7.
[160] Working Party 29 WP4, 5.
[161] Ibid.
[162] Additional Protocol to CoE Convention 108, art 2(2).
[163] Working Party 29 WP4, 7.
[164] Ibid.
[165] Ibid.
[166] Ibid.

authorities, auditors, or independent data protection officials, however, this can also be achieved by way of different mechanisms.[167]

58. At EU level, the said awareness is for instance pursued by the obligation, laid down in article 27 of Directive 95/46/EC, for the Member States to encourage the drawing up of codes of conduct that are intended to contribute to the proper implementation of the data protection principles referred to above. Moreover, Article 20 of the directive requires the prior checking, by the national supervisory authorities (see *infra*), of processing operations likely to present specific risks to the right and freedoms of data subjects. By way of these measures, compliance with the data protection rules by data controllers is proactively stimulated.[168] As regards the implementation of the second factor, article 23 requires the imposition of liability on the controller[169] in case an individual has suffered damage as a result of non-compliance. Article 24 of Directive 95/46/EC requires the Member States to adopt suitable measures to ensure the full implementation of the provisions set out in the directive, and in particular to lay down the sanctions to be imposed in case of infringement of the provisions adopted pursuant to this directive. Furthermore, article 28 requires the establishment, in each Member State, of one or more public authorities responsible for monitoring the application within its territory of the provisions adopted at national level pursuant to the directive. The directive requires moreover that these 'supervisory authorities' shall be endowed with investigative powers, effective powers of intervention and the power to engage in legal proceedings,[170] which is in line with article 8, §3 of the EU Charter on Fundamental Rights in which is stated that *"compliance with [the rules on data protection] shall be subject to control by an independent authority"*. The supervisory authorities thus are competent to directly verify, on their own initiative or upon the receival of a complaint by individuals or an association representing that person (see no. 60)[171], compliance with the EU data protection rules, and to subsequently institute legal proceedings when they detect infringements. Article 22 of Directive 95/46/EC also requires the Member States to provide for the right to a judicial remedy for the individual himself for any breach of the rights guaranteed him by the national law applicable to the processing in question. The directive also requires controller or its

[167] Ibid.
[168] Working Party 29 WP169, 5.
[169] Working Party 29 WP169, 28: while Directive 95/46/EC imposes liability on the controller, it does not prevent national data protection laws from providing that, in addition, als the processor should be considered liable in certain cases.
[170] Directive 95/46/EC, art 28(3).
[171] Directive 95/46/EC, art 28(4).

representative to notify the supervisory authorities before carrying out any automatic processing activities and demands the publication of processing operations (see no. 46).[172] Accordingly, both the supervisory authorities and data subjects are able to identify these processes.[173]

k. Support and help to individual data subjects

59. The second objective of a data protection procedural system should be the provision of support and help to individual data subjects in the exercise of their rights.[174] As stated by the Working Party, *"the individual must be able to enforce his/her rights rapidly and effectively, and without prohibitive cost".*[175] To do so, *"there must be some sort of institutional mechanism allowing independent investigation of complaints"*.

60. Within the EU this requirement is met as article 28, §4 of Directive 95/46/EC states that each supervisory authority has the competence to hear claims lodged by any person or by an organisation representing that person, concerning the protection of his rights and freedoms in regard to the processing of personal data. Accordingly, EU law ensures the availability of an administrative remedy for the individual.[176] Article 22 of the Directive moreover grants a data subject a right to justice when the rights guaranteed him by the national law applicable to the processing have been breached and this without prejudice to an administrative solution such as the complaints procedure before the supervisory authority. Article 47 of the EU Charter on Fundamental Rights also states that *"everyone whose rights and freedoms guaranteed by the law of the Union are violated has the right to an effective remedy before a tribunal"* (see no. 114).

l. Appropriate redress

61. The third and last objective identified by the Article 29 Working Party relates to the redress options of an injured party where rules are not complied with.[177] More specifically, there should be a system of independent arbitration which allows the imposition of sanctions and the payment of compensation where this is appropriate.[178]

---

[172] Directive 95/46/EC, arts 18 and 21.
[173] Mutatis mutandis: Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council of the adequacy of the protection provided by the EU-U.S. Privacy Shield [2016] OJ L207/1, recital 31.
[174] Working Party 29 WP4, 7.
[175] Ibid.
[176] Directive 95/46/EC, art 22.
[177] Working Party 29 WP4, 7.
[178] Ibid.

62. As states above (see no. 58 and 60), Directive 95/46/EC obliges the Member States to ensure data subjects the right to a judicial remedy and to lay down the sanctions to be imposed in case of infringement.[179] The supervisory also have to competence to instigate legal proceedings.[180] This requirement is moreover further substantiated by article 23 of the directive on 'liability'.

C. Permissibility of derogations

63. In recent years, the Court of Justice of the European Union made clear that the adequateness of a data protection regime, both within and outside of the EU, depends not solely on the existence of substantive data protection principles, but also on the formulation, to the benefit of the government, of the possible derogations to these standards.

64. It must be noted in that regard, that EU data protection law provides the possibility to derogate from the data protection principles.[181] However, EU law also determines that any such restriction needs to be laid down in law and must prove to be a necessary measure to safeguard national security, defence, public security, the prevention, investigation, detection and prosecution of criminal offences, etc. (see no. 16).[182] Moreover, it became apparent from the *Digital Rights Ireland* case of 8 April 2014 and the *Tele2 Sverige* case of 21 December 2016 that such limitations must also respect the fundamental rights of EU citizens as laid down in the Charter of Fundamental Rights of the European Union, and more in particular in article 7 (right to privacy) and article 8 (the right to protection of personal data) thereof.[183] These fundamental rights constitute of course on its own important standards of data protection law and consequently always have to be born in mind when restrictions to the substantive data protection principles are laid down.[184] Accordingly, in those cases, the CJEU clarified the conditions under which such restrictions, which constitute an interference with the said rights, can be regarded as 'strictly necessary' in the sense of article 52, §1 of the Charter.[185] Article 52, §1 sets out the terms on which limitations of the rights encompassed in the Charter can take place.

65. In the *Schrems* case of 6 October 2015, the CJEU held that the data protection regime of a third country also has to comply with the EU standards with regard to limitations and exceptions in order to be deemed 'adequate' in the sense of article 25 of Directive 95/46/EC.[186] On that basis, the Court of

---

[179] Directive 95/46/EC, art 22 and 24.
[180] Directive 95/46/EC, art 28(3).
[181] Directive 95/46/EC, art 13; Directive 2002/58/EC (e-Privacy Directive), art 15(1).
[182] Ibid.
[183] *Digital Rights Ireland*, para 92; *Schrems*, paras 25 and 70.
[184] Peter Hustinx, 'EU Data Protection Law: The Review of Directive 95/46/EC and Proposed General Data Protection Regulation', 6.
[185] *Digital Rights Ireland*, para 31; *Tele2 Sverige AB*, para 81; with regard to the *Digital Rights Ireland* case: Directorate-General for Justice and Consumers (Commission), *2014 report on the application of the EU Charter of Fundamental Rights* (Publications Office of the European Union 2015) 7.
[186] *Schrems*, paras 96-98.

Justice, in that case, invalidated the previous adequacy decision[187] of the Commission concerning the data protection regime in the United States.[188] Accordingly, the Court did not even deem it necessary to examine the actual substantive data protection standards, *in casu* the Safe Harbour principles, in place in the United States.[189]

The Court of Justice of the European Union thus established that the 'adequacy' of a data protection regime of a third country, just as the 'adequacy' of the EU data protection system, depends equally on the substance of the standards and on the derogations and limitations of these standards given the fact that EU fundamental rights always have to be taken into account. That way, it confirmed that the level of data protection afforded by a third country has to be assessed in the light of all circumstances surrounding a data transfer (see no. 16).[190]

66. It is thus clear that an analysis of the case law of the Court of Justice with regard to the permissibility of exceptions to the substantive data protection standards is required in order to properly assess whether the level of data protection established in a third country can be considered adequate. In the *Schrems* case, the Court indeed referred to its judgment in *Digital Rights Ireland* to substantiate its assessment of the data protection regime in the U.S.[191] Accordingly, these two cases will be discussed below and this together with the Court's more recent judgment in the *Tele2 Sverige* case, in which it further developed the criteria it had established in the *Digital Rights Ireland* case (1).[192]

Two recent cases of the European Court of Human Rights, *Zakharov v. Russia* and V*issy and Szabó v. Hungary*, both dealing with the acceptability of secret surveillance by the government in the light of article 8 of the European Convention of Human Rights are also of particular importance in this context. The Court of Justice of the European Union moreover referred to both of these cases in certain of the decisive and innovating paragraphs in its *Tele2 Sverige* judgment.[193] Accordingly, these judgments of the Human Rights Court in Strasbourg will also be discussed (2).

---

[187] Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce [2000] OJ L215/7 ['Safe Harbour Decision'].
[188] Ibid.
[189] *Schrems*, para 98.
[190] Directive 95/46/EC, 25(2).
[191] *Schrems*, paras 78, 87 and 91-94.
[192] Orla Lynskey, 'Tele2 Sverige AB and Watson et al: continuity and radical change' (European Law Blog, 12 January 2017) <http://europeanlawblog.eu/2017/01/12/tele2-sverige-ab-and-watson-et-al-continuity-and-radical-change/> accessed 4 March 2017.
[193] *Zakharov v. Russia* ECHR 2015; *Szabó and Vissy v. Hungary* ECHR App no 37138/14 (ECtHR, 12 January 2016) ['*Szabó and Vissy v. Hungary* ECHR 2016'].

1. Case law of the Court of Justice of the European Union

67. Firstly, the case-law of the Court of Justice of the European Union in *Digital Rights Ireland, Tele2 Sverige* and *Schrems* will be analysed and discussed.

a. Digital Rights Ireland judgment

68. On the 8th of April 2014, the Grand Chamber of the Court of Justice of the European Union delivered a landmark judgment in the *Digital Rights Ireland* case.[194] In that case the Court declared the Data Retention Directive to be invalid as it considered that this directive entailed *"a wide-ranging and particularly serious interference with the fundamental rights to respect for private life and to the protection of personal data, without that interference being limited to what is strictly necessary".*[195] The Court ruled that the EU legislator consequently had exceeded the principle of 'proportionality' and this more specifically in light of article 7, 8 and 52, §1 of the Charter.[196] In doing so, the Court made clear that limitations are required in the phase of the 'collection' of personal data as well as in the phases of 'accessing' the gathered data or subsequent 'usage'[197], even when personal data is being processed in view of objectives of general interest such as the fight against serious crime.

(1) Facts of the case and background of the Data Retention Directive

69. Digital Rights Ireland Ltd, an Irish organization dedicated to defending Civil, Human and Legal Rights in the digital age[198], and the Austrian regional government of the Province of Carinthia, together with 11 128 other applicants, challenged national measures that respectively corresponded with the provisions of or were adopted pursuant to Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks

[194] Xavier Tracol, 'Legislative genesis and judicial death of a directive: The European Court of Justice invalidated the data retention directive (2006/24/EC) thereby creating a sustained period of legal uncertainty about the validity of national laws which enacted it' (2014) 30 Computer Law & Security Review 736, 737. ['Xavier Tracol, 'European Court of Justice invalidated the data retention directive: commentary'].
[195] Court of Justice of the European Union, 'The Court of Justice declares the Data Retention Directive to be invalid' (Press release, 8 April 2014), 1 <http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054en.pdf> accessed 3 April 2017.
[196] Xavier Tracol, 'European Court of Justice invalidated the data retention directive: commentary', 737.
[197] Gert Vermeulen, 'The Paper Shield: On the degree of protection of the EU-US privacy shield against unnecessary or disproportionate data collection by the US intelligence and law enforcement services' in Svantesson, Dan J.B. and Dariusz Kloza (eds), *Transatlantic Data Privacy Relationships as a Challenge for Democracy; European Integration and Democracy Series*, vol 4 (Intersentia 2017), 7 ['Gert Vermeulen, 'The Paper Shield' '].
[198] <https://www.digitalrights.ie/> (Website Digital Rights Ireland) accessed 4 April 2017.

and amending Directive 2002/58/EC [hereinafter: 'Directive 2006/24/EC' or 'Data Retention Directive'].[199] They challenged, respectively before the High Court of Ireland and the Austrian Constitutional Court, the legality of both these measures and Directive 2006/24/EC itself, and their compatibility with fundamental rights.[200] These Courts referred those cases to the Court of Justice for a preliminary ruling, essentially asking the CJEU whether the Data Retention Directive could be considered valid in the light of the EU 'proportionality' requirement, the Charter, and other EU legislation on data protection.[201]

70. The Data Retention Directive aimed at harmonising Member States' provisions adopted pursuant to article 15, §1 of Directive 2002/58/EC.[202] As mentioned above (see no. 38), Directive 2002/58/EC translates the principles set out in Directive 95/46/EC into specific rules for the telecommunications sector.[203] In particular, this directive provides for the confidentiality of communications and of traffic and location data (other than traffic data) as well as for the obligation to erase the data or make them anonymous where they are no longer needed for the purpose of the transmission of a communication, unless they are still necessary for billing purposes and this only for as long as necessary.[204] Article 15, §1 of Directive 2002/58/EC, which mirrors article 13 of Directive 95/46/EC, stipulates that Member States may adopt legislative measures to restrict the scope of certain rights and obligations provided for in that directive *"when such restriction constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system".* Moreover, that paragraph provides that *"to this end, Member States may, inter alia, adopt legislative measures providing for the retention of data for a limited period justified on the grounds laid down in this paragraph".* Consequently, several Member States had adopted legislation providing for the retention of traffic and location data of users by providers of publicly available electronic communications service or of public communications networks, in order to

---

[199] *Digital Rights Ireland*, paras 2-3; Marie-Pierre Granger and Kristina Irion, 'The Court of Justice and the Data Retention Directive in Digital Rights Ireland: Telling off the EU legislator and Teaching a Lesson in Privacy and Data Protection' (2014) 20 European Law Review 835, 839 ['Marie-Pierre Granger and Kristina Irion, 'The Court of Justice and the Data Retention Directive in Digital Rights Ireland'].
[200] *Digital Rights Ireland*, paras 17 and 19; Marie-Pierre Granger and Kristina Irion, 'The Court of Justice and the Data Retention Directive in Digital Rights Ireland, 839.
[201] *Digital Rights Ireland*, paras 18 and 20-21; Marie-Pierre Granger and Kristina Irion, 'The Court of Justice and the Data Retention Directive in Digital Rights Ireland, 839.
[202] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC [2006] OJ L 105/54, art 1 and recital 21 ['Data Retention Directive'].
[203] Directive 2002/58/EC (e-Privacy Directive), recital 4.
[204] *Digital Rights Ireland*, para 32.

ensure that the data are available for the purpose of the prevention, investigation, detection and prosecution of criminal offences.[205] These national provisions appeared to differ considerably from one another[206] and the EU legislator considered that these differences between national provisions presented an obstacle to the internal market. Consequently, it adopted Directive 2006/24/EC to harmonise the concerned provisions.[207] More specifically, article 3 of the directive laid down an obligation on the Member States to adopt measures to ensure that data specified in article 5 of the directive are retained by the said service providers to the extent that these providers gathered those data in the process of supplying the communications services concerned. Article 5 of the directive specified different types of traffic and location data, but did not refer to the content of the data concerned.[208] The retention thus involved so-called metadata (see no. 10).

(2) Ruling of the Court

71. The Court of Justice noted that recital 22 of the (former) Data Retention Directive stated that the directive sought to ensure full compliance with citizens' fundamental rights to respect for private life and communications and to the protection of their personal data, as enshrined in articles 7 and 8 of the Charter.[209] Simultaneously, the Court considered that the obligation, under article 3 of the Data Protection Directive, on the service providers to retain the data listed in article 5 raised questions relating to the fundamental rights laid down in the said articles of the Charter.[210] Those data, taken as a whole, indeed may have allowed very precise conclusions to be drawn concerning the private lives of persons whose data had been retained, such as their habits of everyday life, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them, even though the directive did not permit the retention of the content of communications.[211] Hence, the Court considered it appropriate to examine the validity of the directive in the light of articles 7 and 8 of the Charter.[212]

(a) Interference with the right to privacy (article 7 Charter) and to data protection (article 8 Charter)

72. The Court held that the obligation to retain and the possibility for the competent national authorities to subsequently access the data constitutes a derogation of the privacy standards laid down in Directive 2002/58/EC.[213] Since it does not matter whether the gathered data concern sensitive data or whether the

---

[205] Data Retention Directive, recital 5-6; Xavier Tracol, 'European Court of Justice invalidated the data retention directive: commentary', 737.
[206] Data Retention Directive, recital 6.
[207] Data Retention Directive, art 1 and recital 6.
[208] Data Retention Directive, art 1(2).
[209] *Digital Rights Ireland*, para 24.
[210] *Digital Rights Ireland*, para 25.
[211] *Digital Rights Ireland*, paras 27-28.
[212] *Digital Rights Ireland*, para 31.
[213] *Digital Rights Ireland*, para 32.

persons involved have been conceived in one way or another in order to establish the existence of an interference, the obligation to retain, by itself, is considered an interference with article 7 Charter.[214] The access of the authorities was moreover viewed as a further interference with these fundamental rights.[215] In addition, the Court found that the directive interfered with the article 8 of the Charter simply because *"it provides for the processing of personal data"*.[216] Furthermore, the Court noted, following the opinion of the Advocate General, that the interference was particularly serious, and, as the subscribers and users are not informed of the retention and subsequent use, these people might have gotten the feeling of being constantly surveyed.[217]

73. As stated above (see no. 8), both 'retention' or 'collection' and subsequent 'access' or 'use' are considered 'processing of personal data' under EU data protection law[218] and thus receive the protection applicable in the particular circumstances of the processing as set out in the directive. From the reasoning of the Court, as explained in the previous paragraph, it can be deducted that once derogations to the said protection are drawn up, these derogations constitute an interference with fundamental rights and should accordingly be justifiable in the sense of article 52, §1 of the Charter.[219]

(b) Justification of the interference in the light of article 52, §1 Charter

74. Article 52, §1 of the Charter determines that:

> *"Any limitation on the exercise of the rights and freedoms recognized by this Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognized by the Union or the need to protect rights and freedoms or others".*

The Court did not specifically mention the requirement regarding the 'legal basis' of the interference, presumably because this condition is evidently fulfilled. Accordingly, the Court went on to examine whether the interference respected the essence of the rights concerned, whether it satisfied an objective of general interest (i) and whether the interference could be considered to be proportionate (ii).

---

[214] *Digital Rights Ireland*, paras 33-34.
[215] *Digital Rights Ireland*, para 35.
[216] *Digital Rights Ireland*, para 63; Xavier Tracol, 'European Court of Justice invalidated the data retention directive: commentary', 743.
[217] *Digital Rights Ireland*, para 37.
[218] Directive 95/46/EC, art 2(b); Gert Vermeulen, 'The Paper Shield', 7.
[219] Peter Hustinx, 'EU Data Protection Law: The Review of Directive 95/46/EC and Proposed General Data Protection Regulation', 6.

(i) Respect for the essence of the rights and objectives of general interest

75. According to the Court, the essence of article 7 of the Charter had, despite the fact that the retention of data required by the Data Retention Directive constitutes a particularly serious interference, not been adversely affected as the directive does not require the acquisition of the content of electronic communications as such.[220] The essence of article 8 also was not considered to be impaired as article 7 of the directive provides that, without prejudice to the provisions adopted pursuant to directive 95/46/EC and directive 2002/58/EC, certain principles of data protection and data security must be respected by the concerned service providers.[221]

76. As regards the question of whether the interference satisfied an objective of general interest, the Court noted that, while Directive 2006/24/EC aimed at harmonizing the national provisions that had been adopted pursuant to article 15, §1, its material objective was to ensure that the data gathered by service providers were available to the competent national authorities for the purpose of the investigation, detection and prosecution of serious crime.[222] The Court also observed that the use of electronic communications became a valuable tool in the fight against serious crime[223] and even referred to article 6 of the Charter concerning the right to liberty and security in that regard.[224] Accordingly, it considered that the Data Retention Directive pursued an objective of general interest.[225]

(ii) Proportionality

77. In those circumstances, it was necessary for the Court to verify the 'proportionality' of the interference.[226] The principles of proportionality requires the acts of the EU institutions to be 'appropriate' for attaining the legitimate objectives pursued by the legislation at issue (1) and to not exceed the limits of what is necessary in order to achieve those objectives.[227] Moreover, the Court observed that the review in this regard should be strict given the importance of the protection of personal data in the light of the right to privacy and the extent and seriousness of the interference with that right caused by Directive 2006/24/EC.[228]

---

[220] *Digital Rights Ireland*, para 39.
[221] *Digital Rights Ireland*, para 40.
[222] *Digital Rights Ireland*, para 41.
[223] *Digital Rights Ireland*, para 43.
[224] *Digital Rights Ireland*, para 42.
[225] *Digital Rights Ireland*, para 44.
[226] *Digital Rights Ireland*, para 45.
[227] *Digital Rights Ireland*, para 46.
[228] *Digital Rights Ireland*, para 48.

Appropriateness

78. The Court considered that the retention of data required by the Data Retention Directive was indeed appropriate for attaining the objective pursued by that directive as, given the growing importance of means of electronic communications, the data retained allow the competent authorities to have additional opportunities to shed light on serious crime.[229] Consequently, they can be regarded to be a valuable tool for criminal investigations.[230]

Necessity

79. With regard to the 'necessity' of the measure, the Court recognised that the fight against serious crime is indeed of the utmost importance, however, it also pointed out that such an objective of general interest does not in itself justify a measure such as the one that was established by the Data Retention Directive.[231] Moreover, any limitations and derogations in relation to the right to private life and the right to data protection should be strictly necessary.[232]

Accordingly, EU legislation as such should lay down *"clear and precise rules governing the scope and application of the measure in question and imposing minimum safeguards so that the persons whose data have been retained have sufficient guarantees to effectively protect their personal data against the risk of abuse and against any unlawful access and use of that data".*[233]

80. As regards the rules governing the scope and application of the measure, the Court essentially identified three shortcomings in the Data Retention Directive:

The first one related to the fact that the retention was conducted in a generalised and indiscriminate manner.[234] The Court noted in particular that the directive applied to all persons and all means of electronic communication as well as all traffic data without any differentiation, limitation or exception being made in the light of the objective of fighting against serious crime.[235] Moreover, the directive did not require any relationship between the data whose retention is provided for and a threat to public security.[236] In particular, the measure was not restricted to retention in relation "*(i) to data pertaining to a particular time period and/or a particular geographical zone and/or to a circle of particular persons likely to be involved, in one way or another, in a serious crime, or (ii) to persons who could, for other*

[229] *Digital Rights Ireland*, para 49.
[230] Ibid.
[231] *Digital Rights Ireland*, para 51
[232] *Digital Rights Ireland*, para 52.
[233] *Digital Rights Ireland*, para 54.
[234] *Digital Rights Ireland*, para 57.
[235] *Digital Rights Ireland*, paras 57-58.
[236] *Digital Rights Ireland*, para 59.

reasons, contribute, by the retention of their data, to the prevention, detection or prosecution of serious offences".[237]

Secondly, the Court criticised the lack of any objective criterion by which to determine the limits of access of the competent authorities to the data and their subsequent use that could justify such a serious interference.[238] On the contrary, article 1, §1 of the directive merely stated that the data should be available for the purpose of the investigation, detection and prosecution of *serious crime* as defined by each Member State in its national law.[239] Furthermore, no substantive and procedural conditions, requiring that access and subsequent use of the data must be strictly restricted to the purpose of preventing and detecting precisely defined serious offences or of conducting criminal prosecutions relating thereto, and which had to be fulfilled in order to effectively gain access, had been determined in that regard.[240] The Data Retention Directive merely stated that it was up to the Member States to lay down such conditions.[241] More in particular, the Court noted that *"Directive 2006/24 [did] not lay down any objective criterion by which the number of persons authorised to access and subsequently use the data retained [was] limited to what [was] strictly necessary in the light of the objective pursued. […] the access by the competent national authorities to the data retained [was] not made dependent on a prior review carried out by a court or by an independent administrative body whose decision seeks to limit access to the data and their use to what is strictly necessary for the purpose of attaining the objective pursued and which intervenes following a reasoned request of those authorities submitted within the framework of procedures of prevention, detection or criminal prosecutions. Nor [did] it lay down a specific obligation on Member States designed to establish such limits".*[242]

The third shortcoming identified by of the Court concerned the data retention period. The directive simply required the data to be retained for at least 6 and for a maximum of 24 months without there being made a distinction between the categories of data and without there being determined an objective criteria justifying the length of the retention.[243]

Accordingly, the Court came to the conclusion that the Data Retention Directive did not lay down clear and precise rules governing its scope and application, while the interference it entailed was particularly serious and wide-ranging. Accordingly, the interference could not be regarded as limited to what is 'strictly necessary'.[244]

---

[237] Ibid.
[238] *Digital Rights Ireland*, para 60.
[239] Ibid.
[240] *Digital Rights Ireland*, para 61.
[241] Ibid.
[242] *Digital Rights Ireland*, para 62.
[243] *Digital Rights Ireland*, paras 63-64.
[244] *Digital Rights Ireland*, para 65.

81. As regards the requirement of clear and precise rules relating to the security and the protection of data retained by providers of publicly available electronic communications services or of public communications networks, the Court ruled that the Data Retention Directive did not contain sufficient safeguards against the risk of abuse and against any unlawful access and use of that data. In particular, the Court noted that article 7 of the directive on 'data protection and data security' did not lay down *"rules which are specific and adapted to (i) the vast quantity of data whose retention is required by that directive, (ii) the sensitive nature of that data and (iii) the risk of unlawful access to that data"*; nor had a specific obligation on Member States been laid down to establish such rules.[245] The directive also did not require that the data would be retained within the European Union and as a result the control by an independent authority of compliance with the requirements of protection and security, as explicitly required by article 8, §3 of the Charter, could not be ensured.[246] According to the Court, such a control, carried out on the basis of EU law, is an essential component of the protection of individuals with regard to the processing of personal data.[247]

82. Hence, the Court of Justice came to the conclusion that Directive 2006/24/EC did not comply with the principle of 'proportionality' in the light of articles 7, 8 and 52, §1 of the Charter and accordingly ruled that this directive was invalid.[248]

b. Tele2 Sverige judgment

83. On the 21st of December 2016, the Grand Chamber of the Court of Justice of the European Union, in another landmark judgment, clarified the application of the criteria concerning the 'proportionality requirement' it had laid down in the *Digital Rights Ireland* case. More specifically and most remarkably, the Court made clear that the *Digital Rights Ireland* judgment should be interpreted as meaning that the general and indiscriminate 'retention'/'collection' of data is to be condemned as a matter of principle.[249] The Court also further elucidated some of the other criteria, previously established in the *Digital Rights Ireland* case, that have to be fulfilled in order to comply with the principle of 'necessity'.[250]

(1) Relevance of article 15, §1 of Directive 2002/58/EC and facts of the case

84. It goes without saying that the *Digital Rights Ireland* judgment has had a big impact. In several Member States, national laws that enacted Directive 2006/24/EC have been challenged before national courts and have been declared invalid as a consequence of this judgment.[251] The European Commission,

---

[245] *Digital Rights Ireland*, para 66.
[246] *Digital Rights Ireland*, para 68.
[247] Ibid.
[248] *Digital Rights Ireland*, para 69 and 71.
[249] *Tele2 Sverige AB*, paras 46 and 112.
[250] *Tele2 Sverige AB*, paras 113-125.
[251] Xavier Tracol, 'European Court of Justice invalidated the data retention directive: commentary', 744.

for its part, stated that *"national legislation [adopted pursuant to the Data Retention Directive] needs to be amended only with regard to aspects that become contrary to EU law after a judgment by the European Court of justice. Furthermore, a finding of invalidity of the Directive does not cancel the ability for Member States under the e-Privacy Directive (2002/58/EC) to oblige retention of data".*[252] National law thus could remain valid and applicable.[253] More in particular, article 15, §1 of Directive 2002/58/EC would serve as the legal basis in that regard since it expressly states that *"Member States may, inter alia, adopt legislative measures providing for the retention of data for a limited period justified on the grounds laid down in this paragraph"*[254] and as the Data Retention Directive was precisely adopted to harmonise national law which had been adopted pursuant to this article (see no. 70).[255] Nonetheless, in the *Tele2 Sverige* case, the Court, before entering into the substantive part of its ruling, considered whether and to what extent national legislation on the retention of traffic and location data and access to that that by the national authorities, for the purpose of combatting crime, falls within the scope of Directive 2002/58/EC.[256] The Court was, however, of the opinion that it does fall within the scope of that directive and that such legislation must moreover comply with the Charter as the third sentence of article 15, §3 of the directive provides that *"[a]ll the measures referred to [in article 15, §1] shall be in accordance with the general principles of [European Union] law, including those referred to in article 6, §1 and §2 [EU], which include the general principles and fundamental rights now guaranteed by the Charter".*[257] Moreover and according to the previous case law of the Court of Justice in its *Fransson* and *Pleger* judgments, article 51, §1 of the Charter, stating that the Charter applies *"[…] to the Member States only when they are implementing Union law*", should be interpreted as being applicable to national legislation adopted as exceptions provided for by the Union law.[258] The Court could thus extent its case law in the *Digital Rights Ireland* case, with regard to the interpretation of articles 7, 8 and 52, §1 of the Charter, to article 15, §1 of directive 2002/58/EC and the national legislation now finding its legal basis in this article. Moreover, article 15, §1 itself requires that any derogation adopted pursuant to it is 'necessary, appropriate and proportionate' within a democratic society and in view of the objectives laid down in that provision.[259]

---

[252] Xavier Tracol, 'European Court of Justice invalidated the data retention directive: commentary', 744; Commission, 'Frequently Asked Questions: The Data Retention Directive' (Memo, 8 April 2014) <http://europa.eu/rapid/press-release_MEMO-14-269_en.htm> accessed 7 April 2017.
[253] Xavier Tracol, 'European Court of Justice invalidated the data retention directive: commentary', 744.
[254] LIBE (European Parliament), 'Questions relating to the judgment of the Court of Justice of 8 April 2014 in Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland* and *Seitlinger and other*s – Directive 2006/24/EC on data retention – Consequences of the judgment'(legal opinion) SJ-0890/14, 24 ['LIBE, 'Questions relating to the *Digital Rights Ireland* case' '].
[255] Data Retention Directive, art 1, §1 and recitals 4, 5, 6 and 12; *Tele2 Sverige AB*, paras 62-63.
[256] *Tele2 Sverige AB*, para 65.
[257] *Tele2 Sverige AB*, para 91.
[258] LIBE, 'Questions relating to the *Digital Rights Ireland* case', 23.
[259] *Tele2 Sverige AB*, para 95.

85. In *Tele2 Sverige*, the Court of Justice dealt with the questions of two referring national courts: those of the Administrative Court of Appeal of Stockholm (C-203/15) and those of the Court of Appeal of England & Wales (Civil Division) (C-689/15). The Swedish Court, with its first question, essentially asked the Court if article 15, §1 of Directive 2002/58/EC must be interpreted, bearing in mind the Court's case law in the *Digital Rights Ireland* case, as precluding national legislation providing for the general and indiscriminate retention of personal data or rather as requiring an assessment of all circumstances in order to determine the compatibility of national legislation with EU law.[260] In the same way, both the Swedish court and the UK court, with a next question, sought, in essence, to ascertain *"whether article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and Article 52(1) of the Charter, must be interpreted as precluding national legislation governing the protection and security of traffic and location data, and more particularly, the access of the competent national authorities to retained data, where that legislation does not restrict that access solely to the objective of fighting serious crime, where that access is not subject to prior review by a court or an independent administrative authority, and where there is no requirement that the data concerned should be retained within the European Union".*[261] According to the Court, this last question arises irrespective of whether retention is generalised or targeted.[262]

(2) Ruling of the Court

86. With regard to the first question, the Court started with reiterating its main findings in the *Digital Rights Ireland* case and stated consequently that national legislation such as that at issue in the main proceedings exceeds the limits of what is strictly necessary and cannot be considered as to be justified in a democratic society.[263] Thereinafter, the Court stated that *"article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, does not [however] prevent a Member State from adopting legislation permitting, as a preventive measure, the targeted retention of traffic and location data, for the purpose of fighting serious crime, provided that the retention of data is limited, with respect to the categories of data to be retained, the means of communication affected, the persons concerned and the retention period adopted, to what is strictly necessary".*[264] The substantive conditions to be laid down in law must be shown to be such as actually to circumscribe, in practice, the extent of the measure and, consequently, the public affected. In any event, the retention must *always* meet objective criteria that establish a connection between the data to be retained and the objective pursued.[265] Moreover, the legislation must require the existence of objective evidence which makes it possible to

[260] *Tele2 Sverige AB*, paras 46 and 62.
[261] *Tele2 Sverige AB*, para 114.
[262] *Tele2 Sverige AB*, para 113.
[263] *Tele2 Sverige AB*, para 107.
[264] *Tele2 Sverige AB*, para 108.
[265] *Tele2 Sverige AB*, para 110.

identify a public whose data is likely to reveal a link, at least an indirect one, with serious criminal offences, and to contribute in one way or another to fighting serious crime or to preventing a serious risk to the public security.[266] This can be achieved by using, for example, a geographical criterion.[267]

Accordingly, the Court ruled that *"article 15, §1 of Directive 2002/58/EC, read in the light of articles 7, 8 and 52, §1 of the Charter, [indeed] must be interpreted as precluding national legislation which, for the purpose of fighting crime, provides for the general and indiscriminate retention of all traffic and location data of all subscribers and registered users relating to all means of electronic communications".*[268]

87. With regard to the second question, the Court confirmed its previous case law regarding the conditions that have to be fulfilled before the competent national authorities can be granted access to data retained by the service providers.[269] The Court added moreover that general access to all retained data cannot be regarded as limited to what is strictly necessary. Instead, access can, as a general rule, be granted, in relation to the objective of fighting crime, only to "*the data of individuals suspected of planning, committing or having committed a serious crime or of being implicated in one way or another in such a crime",* however, in specific circumstances, exceptions can be allowed. [270] In that regard the Court referred to the case law of the ECtHR in its recent *Zakharov v. Russia* case, which will be discussed below (see nos. 99-103). The Court also reiterated that access to the data should be subject to prior and independent review, except in cases of validly established urgency, and thereto recalled the case law of the ECtHR in another recent case named *Vissy and Szabó v. Hungary* (see nos. 104-108).[271] The authorities should also notify the persons affected as soon as that notification is no longer liable to jeopardise the investigations in order to ensure that data subjects can exercise their right to a legal remedy, expressly provided for in article 15, §2 of Directive 2002/58/EC.[272] Lastly, the Court reiterated that the data should be retained within the European Union in order to ensure that review by the national supervisory authorities of compliance with the level of data protection guaranteed by EU law is possible, and more in particular to enable individuals to lodge a claim seeking the protection of their data with the national supervisory authority.[273] Of course, data that are transferred to a third country cannot be

[266] *Tele2 Sverige AB*, para 111.
[267] Ibid.
[268] *Tele2 Sverige AB*, para 112.
[269] *Tele2 Sverige AB*, paras 115-118.
[270] *Tele2 Sverige AB*, para 119.
[271] *Tele2 Sverige AB*, para 120.
[272] *Tele2 Sverige AB*, para 121.
[273] *Tele2 Sverige AB*, paras 122-123.

retained within the European Union, however, even when such transfers take place, the national supervisory authorities must be able to examine, when hearing a claim lodged by a person, whether these transfers of data comply with the requirements laid down by the directive.[274]

88. Consequently, the Court also answered the second question affirmatively.[275]

c. Schrems judgment

89. In the *Schrems* case, the Court of Justice found that the national supervisory authorities are allowed to examine the claim of a person in which he/she contends that the law and practices in force in a third country do not ensure an adequate level of data protection, where personal data is transferred to this country on the basis of an adequacy decision by the Commission.[276] Furthermore, the Court invalidated the Commission's adequacy decision 2000/520/EC in which the European Commission had declared that the implementation of the 'safe harbour' scheme ensured an adequate level of data protection in the United States.[277] More specifically, it ruled that *"the Commission did not state, in its Decision 2000/520, that the United States in fact 'ensures' an adequate level of protection by reason of it domestic law of its international commitments"*[278] and that *"the implementing powers granted by the EU legislature to the Commission in Article 25, §6 of Directive 95/46 does not confer upon it competence to restrict the national supervisory authorities' powers [as laid down in article 28 of directive 95/46]"*[279].

(1) Facts of the case

90. In this case, the Irish High Court made a request for a preliminary ruling in the proceedings between Maximilian Schrems, an Austrian national, and the Irish Data Protection Commissioner concerning the latter's refusal to investigate a complaint made by Mr Schrems regarding the fact that Facebook Ireland Ltd transferred the personal data of its users to the U.S. and kept it on its servers located there.[280]

Such transfers of personal data were made possible by the Commission's Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce [hereinafter: 'Safe Harbour Decision' or 'Decision 2000/520/EC'], which had been adopted on the basis of article 25, §6 of directive 95/46/EC, of 26 July 2000 (see no. 20). More in particular, the European Commission found in that decision that *"for the purposes of article*

---

[274] *Digital Rights Ireland*, para 57.
[275] *Tele2 Sverige AB*, para 125.
[276] *Schrems*, para 66.
[277] Xavier Tracol, '"Invalidator" strikes back: The harbour has never been safe' (2016) 32 Computer Law & Security Review 345, 346. ['Xavier Tracol, '"Invalidator" strikes back: The harbor has never been safe'].
[278] *Schrems*, para 97.
[279] *Schrems*, para 103.
[280] *Schrems*, para 2.

25, §2 of Directive 95/46/EC, for all the activities falling within the scope of that Directive, the 'Safe Harbor Privacy Principles' (...) implemented in accordance with the guidance provided by the frequently asked questions (hereinafter 'the FAQs') issued by the US Department of Commerce are considered to ensure an adequate level of protection for personal data transferred from the [Union] to organisations established in the United States".[281] This decision thus enabled data flows from the EU to the U.S. for commercial purposes when the receiving U.S. organisations self-certified their adherence to the Safe Harbour principles prior to reception of the data.[282]

However, Mr Schrems took the view that the law and practice in force in the United States did not ensure adequate protection of personal data held in its territory against the surveillance activities that were engaged in by the public authorities there.[283] More in particular, the National Security Agency (NSA), according to a top-secret document on the NSA PRISM programme, which allowed officials to collect material including search history, the content of emails, file transfers and live chats, appeared to have direct access to the servers of Google, Apple, Facebook and other U.S. internet giants.[284] As all the companies involved in the PRISM programme, which thus allowed mass collection of intelligence, were moreover Safe Harbour self-certified, the Safe Harbour scheme was one of the conduits through which the U.S. authorities were given large-scale access to data that had initially been processed in the EU.[285] The existence of these surveillance practices had of course been revealed by whistle-blower Edward Snowden, who is a former U.S. Intelligence Community officer.[286]

Mr Schrems accordingly made a complaint to the Irish Data Protection Commissioner by which he essentially requested the latter to exercise his statutory powers, as embodied in article 28 of directive 95/46/EC, by prohibiting Facebook Ireland Ltd from transferring his personal data to the United States.[287] The Commissioner, however, rejected the complaint, stating that there was no evidence that Mr Schrems' data had been accessed by the NSA and that any question relating to the adequacy of data protection in the U.S. had to be determined in the light of Decision 2000/520/EC in which the Commission had found that the U.S. indeed ensured an adequate level of data protection.[288] Consequently, Mr

---

[281] Safe Harbour Decision, art 1(1).
[282] Safe Harbour Decision, art 1(3).
[283] *Schrems*, para 28.
[284] Glenn Greenwald and Ewen MacAskill, 'NSA Prism program taps in to user data of Apple, Google and others' *The Guardian* (7 June 2013) <https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data> accessed 16 April 2017.
[285] *Schrems*, para 22; Commission, 'Communication from the Commission to the European Parliament and the Council on the Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Established in the EU' COM (2013) 847 final, point 7 ['COM (2013) 847 final'].
[286] <https://edwardsnowden.com/> (Website Edward Snowden) accessed 16 April 2017.
[287] *Schrems*, para 28.
[288] *Schrems*, para 29.

Schrems challenged the decision of the Irish Data Protection Commissioner before the Irish High Court.[289]

91. The High Court considered it necessary to stay the proceedings and to ask the Court of Justice whether and to what extent article 25, §6 of directive 95/46/EC, read in the light of article 7, 8 and 47 of the Charter, must be interpreted as meaning that a decision adopted pursuant to that provision prevents a national supervisory authority from being able to examine a claim such as the one at issue in the main proceedings.[290]

(2) Ruling of the Court

92. The Court started off by examining the extent of the powers of the national supervisory authorities, within the meaning of article 28 of Directive 95/46/EC, in circumstances where the Commission has adopted a decision pursuant to article 25, §6 of that directive.[291] In second instance, the Court actually assessed the validity of Decision 2000/520/EC.[292]

(a) Powers of the national supervisory authorities

93. The Court first recalled the importance of the Charter of Fundamental Rights of the European Union, and in particular of article 7 and 8 thereof, when assessing issues related to the processing of personal data.[293] Then it considered the powers available to the national supervisory authorities in respect of transfers of personal data to third countries.[294] It noted in that regard that both primary EU law, and more in particular article 8, §3 of the Charter and article 16, §2 TFEU, and secondary EU legislation, in particular article 28, §1 of directive 95/46/EC, require Member States to set up one or more public authorities responsible for monitoring, with complete independence, compliance with EU rules on the protection of individuals with regard to the processing of personal data, and that the establishment thereof constitutes an essential component of the protection of individuals with regard to the processing of personal data.[295] As mentioned before, these authorities have a wide range of powers for that purpose (see no. 58).[296] These powers however, as is apparent from article 28, §1 and §6, concern only the processing of personal data carried on the territory of their own Member State and not such processing operations conducted in a third country.[297] Nonetheless, the Court ruled that national supervisory authorities are competent to examine whether transfers from the EU to third countries of personal data are

[289] *Schrems*, para 30.
[290] *Schrems*, para 37.
[291] *Schrems*, paras 38-66
[292] *Schrems*, paras 67-106.
[293] *Schrems*, paras 38-39.
[294] *Schrems*, para 40.
[295] *Schrems*, paras 40-41.
[296] *Schrems*, para 43.
[297] *Schrems*, para 44.

in compliance the rules on 'adequacy', as laid down in directive 95/46/EC, considering that such transfers in itself should be considered as the 'processing of personal data' within the meaning of article 2, (b) of Directive 95/46/EC.[298] The Court further noted that the Commission may adopt an adequacy finding pursuant to article 25, §6 of Directive 95/46/EC, that such a decision is binding on the Member States[299] (see no. 20) and that consequently only the Court itself had the competence to invalidate such a finding.[300] However, the adoption of an adequacy decision cannot prevent individuals from lodging a claim with the national supervisory authorities (see nos. 58 and 60) concerning the protection of their rights and freedoms in regard to transfers of their data to third countries.[301] In that case, it is incumbent on the authorities to examine, with all due diligence, whether or not an adequacy finding of the Commission indeed complies with the requirements stemming from Directive 95/46/EC in that regard.[302] Where the supervisory authority disagrees with the claimant, the latter can, in accordance with the second subparagraph of article 28, §3 of Directive 95/46/EC and article 47 of the Charter, have access to judicial remedies enabling him to challenge such a decision adversely affecting him before the national courts.[303] In the opposite case, the supervisory authority itself can, having regard to the first subparagraph of article 28, §3 and article 8, §3 of the Charter, engage in legal proceedings.[304] Either way, the national court seized of the case shall have to stay proceedings and make a reference for a preliminary ruling for the purpose of examination of the decision's validity when it considers that there is at least doubt in that regard.[305] The Court consequently affirmatively replied to the question asked by the Irish High Court.[306]

(b) Validity of Decision 2000/520/EC

94. Considering its reasoning with regard to the powers of the national supervisory authorities and in order to give the referring court a full answer, the Court deemed it appropriate to effectively examine whether the Commission's Safe Harbour Decision complied with the requirements stemming from Directive 95/46/EC read in the light of the Charter.[307]

The Court first stated that a system of self-certification is not in itself contrary to the requirement laid down in article 25, §6 of Directive 95/46/EC that the country concerned must ensure an adequate level of protection 'by reason of its domestic law or … international commitments', but that its reliability, in

[298] *Schrems*, paras 45-47.
[299] *Schrems*, para 51.
[300] *Schrems*, paras 51-52.
[301] *Schrems*, paras 53-57.
[302] *Schrems*, para 63.
[303] *Schrems*, para 64.
[304] *Schrems*, para 65.
[305] *Schrems*, paras 64-65.
[306] *Schrems*, para 66.
[307] *Schrems*, para 67.

the light of that requirement, is founded essentially on the establishment of effective detection and supervision mechanisms which can ensure compliance with the rules.[308] Then, the Court noted that the safe harbour principles, which created the presumption of 'adequacy' in the U.S., as substantive data protection standards, were applicable solely to U.S. organisations that had self-certified their adherence to these principles, while United States public authorities were not required to comply with them.[309] Moreover, the Court observed that Decision 2002/520, and more specifically Annex I to that decision, on top of that provided that such self-certified organisations may be required by the US government to disregard the Safe Harbour privacy principles, and this without limitations, for reasons of 'national security, public interest or law enforcement'.[310]

Thereupon, the CJEU referred to its case-law in the *Digital Rights Ireland* case.[311] The Court stated more in particular that, given the general nature of these derogations, these exceptions to the Safe Harbour principles constitute an interference with the fundamental right to respect for private life as enshrined in article 7 of the Charter[312] and accordingly applied the conditions it had laid down in the *Digital Rights Ireland* case as regards the 'strict necessity' of derogations and limitations in relation to article 7 to the facts of the case (the Court thus did not assess the validity of Decision 2000/520/EC in the light of article 8 of the EU Charter on Fundamental Rights[313]).[314] The Court consequently stated that *"legislation is not limited to what is strictly necessary where it authorises, on a generalised basis, storage of all the personal data of all the persons whose data has been transferred from the European Union to the United States without any differentiation, limitation or exception being made in the light of the objective pursued and without an objective criterion being laid down by which to determine the limits of the access of the public authorities to the data, and of its subsequent use, for purposes which are specific, strictly restricted and capable of justifying the interference which both access to that data and its use entail".*[315] Moreover, it considered that *"in particular legislation permitting the public authorities to have access on a generalised basis to the content of electronic communications must be regarded as compromising the essence of the fundamental right to respect for private life, as guaranteed by article 7 of the Charter".*[316]

The Court added that the legislation in the United States also did not respect the essence of the fundamental right to effective judicial protection, as enshrined in article 47 of the Charter, as it did not provide

[308] *Schrems*, para 81.
[309] *Schrems*, para 82.
[310] *Schrems*, paras 84-86.
[311] *Schrems*, paras 78, 87 and 91-94.
[312] *Schrems*, para 87.
[313] Xavier Tracol, '"Invalidator" strikes back: The harbour has never been safe', 355.
[314] *Schrems*, paras 91-94.
[315] *Schrems*, para 93.
[316] *Schrems*, para 94.

for any possibility for an individual to pursue legal remedies in order to have access to personal data relating to him, or to obtain the rectification or erasure of such data.[317] Though it is true that neither Directive 95/46/EC, nor Directive 2002/58/EC prescribe an obligation for the EU Member States to provide the possibility for the individual to pursue these exact remedies in this context, as the processing of personal data by the government for purposes of national security and law enforcement are excluded from their scope, they are nevertheless required to do so on the basis of article 8, §2 of the Charter and article 8, (c) of Convention 108. While it is thus not entirely clear whether this requirement also stems from EU secondary law, it must be noted that for example the Belgian privacy legislation does provide this possibility.[318] The Court added that *"the first paragraph of Article 47 of the Charter requires everyone whose rights and freedoms guaranteed by the law of the European Union are violated to have the right to an effective remedy before a tribunal in compliance with the conditions laid down in that article"* and that *"the very existence of effective judicial review designed to ensure compliance with provisions of EU law is inherent in the existence of the rule of law"*.[319] The general requirement of article 47 of the Charter in that regard, unlike the specific requirement of the Court mentioned above, is of course complied with at EU level pursuant to article 15, §2 of directive 2002/58/EC and article 22 of directive 95/46/EC (see nos. 58 and 87).

The Court moreover found that Decision 2000/520/EC, and more in particular article 3 thereof, denied the national supervisory authorities the powers which they derive from article 28 of directive 95/46/EC, where a person, bringing a claim under that provision, alleges that an adequacy decision of the Commission is incompatible with the fundamental rights of individuals, and in particular their right to privacy.[320]

Having regard to the above mentioned considerations, the Court consequently invalidated the Commission's Safe Harbour Decision without even examining the content of the safe harbour principles themselves.[321]

95. As the judgment of the Court took effect retroactively, transfers of personal data which had been lawful before the judgment and which could not have been based on another legal basis (see nos. 27-30) had been illegal since the adoption of decision 2000/520/EC.[322] With this judgment, the Court moreover

[317] *Schrems*, para 95.
[318] Wet 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens (*BS* 18 March 1993, consolidated version *BS* 28 December 2015), art 13(1).
[319] Ibid.
[320] *Schrems*, para 102.
[321] *Schrems*, paras 97-98 and 104-106.
[322] Xavier Tracol, '"Invalidator" strikes back: The harbour has never been safe', 357.

created a legal vacuum with regard to future transfers of personal data from the EU to the U.S.[323] Accordingly, the Commission adopted a new adequacy decision encompassing the 'EU-U.S. Privacy Shield' on 12 July 2016. The adequacy of this new framework will, as stated in the general introduction, be assessed in Chapter 3.

d. Conclusion

96. In order to assess whether a third country ensures an adequate level of data protection, an evaluation of the extent to which can be derogated from the substantive data protection standards, next to a consideration of these standards *per se*, plays an important factor.

The Court stated that both EU legislation and national legislation adopted pursuant to EU legislation, by which such an exception is introduced, must encompass *"clear and precise rules governing the scope and application of the measure in question and imposing minimum safeguards so that the persons whose data have been retained have sufficient guarantees to effectively protect their personal data against the risk of abuse and against any unlawful access and use of that data".*[324] More in particular, the Court ruled in unmistakable terms that the mass collection of personal data (*in casu* by service providers) as well as mass access (*in casu* by competent national authorities for the purpose of the investigation, detection and prosecution of serious crime) to retained data cannot be justified in the light of the right to privacy and the right to protection of personal data respectively enshrined in article 7 and 8 of the Charter. The Court also emphasized that there should be objective criteria in place by which the length of the data retention measure can be justified, that there should be specific rules laid down with regard to the protection and security of the data, that Member States must fully ensure the control by way of independent oversight mechanisms of compliance with the level of data protection rules guaranteed by EU law and that an injured party should have the right to a judicial remedy.

Whereas after the *Digital Rights Ireland* case, it was for some not yet entirely clear that all of these criteria have to be fulfilled individually and independently of each other, the Court, in *Tele2 Sverige*, removed any ambiguity in that regard.

2. Case law of the European Court of Human Rights

97. When assessing the adequacy of a data protection regime, the European Convention on Human Rights [hereinafter: ECHR], which is of course, together with it protocols, interpreted and applied by the European Court of Human Rights[325], can evidently not be neglected. Unlike the Charter of Fundamental Rights of the European Union, which is addressed only to the institutions, bodies, offices and

[323] Xavier Tracol, '"Invalidator" strikes back: The harbour has never been safe', 358.
[324] *Digital Rights Ireland*, para 54.
[325] ECHR, art 32.

agencies of the Union and to the Member States when they are implementing Union law[326], this Convention grants individuals, groups of individuals and non-governmental organisations, the right to lodge a complaint to the European Court of Human Rights when they take the view that one of the Contracting Parties has violated one or more of their fundamental rights as set forth in the Convention or the Protocols thereto.[327] All EU Member States are a party to the convention, however, the EU itself is not. This means that individuals and undertakings cannot apply to the European Court of Human Rights for review of the acts of EU institutions.[328] However, the Treaty on European Union [hereinafter: TEU] now obliges the EU to accede to the convention. Accordingly the European Union is currently in the process thereto.[329] In any event, it is stated in article 6, §3 of the TEU that *"[f]undamental rights, as guaranteed by the European Convention on Human Rights and Fundamental Freedoms […] shall constitute general principles of the Union's law".* Accordingly, this convention, and more specifically article 8 concerning the right to privacy, is of particular importance in the present context.

98. The European Court of Human Rights recently also had to deal with cases concerning so called 'mass interception of personal data' in *Roman Zakharov v. Russia* and *Szabó and Vissy v. Hungary*. In both cases the Court came to the conclusion that the Member States in question had violated the applicants' right to privacy as embodied in article of the ECHR.

e. Zakharov v. Russia

99. On 4 December 2015, the European Court of Human Rights brought in a verdict in the *Roman Zakharov v. Russia* case. This judgment is one of the Court's most recent decisions concerning secret surveillance measures and came at a time where several human rights bodies started expressing concerns with regard to right to privacy of citizens in the digital age.[330] In particular, the Court found in this case that the Russian law did not meet the 'quality of law' requirement and was incapable of keeping the 'interference' to what is 'necessary in a democratic society' in the light of the right to privacy as laid down in article 8 of the European Convention on Human Rights.[331]

---

[326] Charter of Fundamental Rights of the European Union [2007] OJ C 326/391, art 51, §1.
[327] Convention for the Protection of Human Rights and Fundamental Freedoms [1950] ETS No. 5, art 34.
[328] 'Accession of the European Union' (Website ECHR) <http://www.echr.coe.int/Pages/home.aspx?p=basictexts/accessionEU&c> accessed 8 April 2017.
[329] 'Accession of the European Union' (Website ECHR) <http://www.echr.coe.int/Pages/home.aspx?p=basictexts/accessionEU&c> accessed 8 April 2017.
[330] Paul De Hert and Pedro Cristobal Bocos, 'Case of Roman Zakharov v. Russia: The Strasbourg follow up to the Luxembourg Court's Schrems judgment' (Strasbourg Observers, 23 December 2015) <https://strasbourgobservers.com/2015/12/23/case-of-roman-zakharov-v-russia-the-strasbourg-follow-up-to-the-luxembourg-courts-schrems-judgment/> accessed 6 April 2017.
[331] *Zakharov v. Russia* ECHR 2015, para 304.

(1) Facts of the case

100. Roman Zakharov, a Russian national, challenged the system of covert interception of mobile telephone communications in Russia in the light of his right to privacy as enshrined in article 8 of the European Convention on Human Rights.[332] The applicant complained in particular that mobile network operators in Russia were required by law to create databases, whereto the authorities had direct remote access, storing information about all subscribers and the services provided to them for three years[333], to install equipment enabling government authorities to perform operational-search activities[334], and that, without sufficient safeguards against abuse under Russian law, this permitted the authorities to have direct access to all mobile telephone communications and related communications ('meta') data and thus the interception of all communications.[335]

(2) Ruling of the Court

101. In an anonymous finding, the Court in Strasbourg ruled that there indeed had been a violation of article 8 of the European Convention on Human Rights.[336]

102. First, the Court admitted the case as it decided that the applicant could claim an interference with his right to privacy by the mere existence of the said legislation.[337] Hence, he did not have to demonstrate that the secret surveillance measures has in fact been applied to him.[338]

103. The Court then went on to assess whether the interference was in 'accordance with the law' and was 'necessary in a democratic society' in the interests of one or more of the 'legitimate aims' as required by article 8 of the Convention. The Court noted, however, that with regard to secret surveillance measures the lawfulness of the interference is closely related to the question of 'necessity' and considered it appropriate to jointly address the 'in accordance with the law' and 'necessity' requirement.[339] In order for the domestic law to be deemed 'foreseeable' (which is an aspect of 'in accordance with the law' requirement), the Court requires provisions to be sufficiently clear as to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to any such measures ('foreseeability requirement *sensu stricto*')[340] and developed minimum safeguards which have to be set out in the legislation concerned in order to avoid abuses of power

---

[332] *Zakharov v. Russia* ECHR 2015, paras 1 and 148; Press Unit of the European Court of Human Rights, 'Factsheet – Mass surveillance', 3 (Website ECHR, December 2016) <http://www.echr.coe.int/Documents/FS_Mass_surveillance_ENG.pdf > accessed 6 April 2017 ['Factsheet – Mass surveillance'].
[333] *Zakharov v. Russia* ECHR 2015, para 269.
[334] *Zakharov v. Russia* ECHR 2015, paras 115-122 and 269.
[335] *Zakharov v. Russia* ECHR 2015, para 10; Factsheet – Mass surveillance, 3.
[336] *Zakharov v. Russia* ECHR 2015, 81.
[337] *Zakharov v. Russia* ECHR 2015, para 171.
[338] *Zakharov v. Russia* ECHR 2015, para 170.
[339] *Zakharov v. Russia* ECHR 2015, para 236.
[340] *Zakharov v. Russia* ECHR 2015, para 229.

('rule of law' requirement)[341].[342] These safeguards relate to the nature of the offences which may give rise to an interception order, the definition of the categories of people liable to have their telephones tapped, the limit on the duration of telephone tapping, the procedure to be followed for examining, using and storing the data obtained, the precautions to be taken when communicating the data to other parties, and the circumstances in which recordings may or must be erased or destroyed.[343] Specifically with regard to the 'necessity' of the measures the Court noted that, while States enjoy a certain margin of appreciation in choosing the means for achieving the legitimate aim of national security, adequate and effective guarantees against abuse are nevertheless essential in view of the fact that a system of secret surveillance set up to protect national security may undermine or even destroy democracy, and this under the cloak of defending it.[344] The assessment of the 'necessity' of a measures depends on all the circumstances of the case, such as the nature, scope and duration of the possible measures, the grounds required for ordering them, the authorities competent for ordering them, the authorities competent to authorise, carry out and supervise them, the procedures for supervising the ordering and the implementation of the measures, and the kind of remedy provided by the national law.[345] The Court noted that review and supervision of secret surveillance measures may come into play at three stages: when the surveillance is first ordered, while it is being carried out, or after it has been terminated.[346] As regards the first two stages, the Court observed that, given the fact that the individual at that point in time cannot be notified of the surveillance, the procedures established should themselves provide adequate and equivalent guarantees safeguarding his or her rights.[347] Hence, the Court considers it desirable to entrust supervisory control to a judge as judicial control offers the best guarantees of independence, impartiality and a proper procedure.[348] As a rule, this authorisation should be acquired prior to surveillance takes place, however, the Court accepts that exceptions can be made in case of 'urgency'.[349] Accordingly, the Court noted with respect to the last stage, that the question of subsequent notification of surveillance measures is inextricably linked to the effectiveness of the remedies available, unless a person can suspect otherwise that he or she has been surveyed and accordingly seek to be remedied.[350]

The Court noted that it had not been disputed by the parties that the interceptions of mobile telecommunications had a basis in the domestic law and that these surveillance measures pursued the legitimate

---

[341] *Zakharov v. Russia* ECHR 2015, para 231.
[342] Yves Haeck and Clara Burbano Herrera, *Procederen voor het Europees Hof voor de Rechten van de Mens* (Tweede editie, Intersentia, 2011), 59-62.
[343] Ibid.
[344] *Zakharov v. Russia* ECHR 2015, para 232.
[345] Ibid.
[346] *Zakharov v. Russia* ECHR 2015, para 233.
[347] Ibid.
[348] Ibid.
[349] *Zakharov v. Russia* ECHR 2015, para 266.
[350] *Zakharov v. Russia* ECHR 2015, para 234.

aims of protecting national security and public safety, the prevention of crime and the protection of economic well-being of the country.[351] Moreover, it found that the legal provisions were sufficiently accessible to the public.[352]

Furthermore, the Court ruled that the Russian system passed the 'foreseeability' and the 'necessity' test with regard to a couple of aspects: the nature of the offences which gave rise to an interception was regarded to be sufficiently clear, however, the Court also noted that the Russian law at the same time allowed secret interception of communications in respect of a very wide range of criminal offences[353]; the Russian law also contained clear rules governing the storage, use and communications of intercepted data, making it possible to minimise the risk of unauthorised access or disclosure[354]; and the Court was also satisfied that any interception of telephone or other communications must be authorised by a Court[355].

The Court, however, also identified shortcomings in that regard in the following areas: the circumstances in which public authorities in Russia were authorized to make use of secret surveillance measures, specifically because the domestic law did not clearly define the categories of people liable to have their phones tapped for reasons of preventing and detecting criminal offences[356], and left the authorities an almost unlimited degree of discretion in determining which events or acts constitute a threat to Russia's national, military, economic or ecological security and whether such a threat is serious enough to justify secret surveillance[357]; the duration of such measures, and more specifically as to provisions concerning discontinuation; the procedures for authorising the interception, notably as the judicial scrutiny of the authorizing authority was regarded to be limited in scope since it was neither provided with sufficient information to assess whether there is a sufficient factual basis to reasonably suspect a particular person[358] (in this regard the CJEU in *Tele2 Sverige* referred to this case, see no. 87) nor instructed to verify the existence of a 'reasonable suspicion' against the 'person concerned' or to apply the 'necessity' and 'proportionality' test[359], and because the domestic law did not contain any requirements either with regard to the content of the request for interception or to the content of the interception authorisation, which sometimes resulted in authorisations which did not mention a specific person or telephone number to be tapped, but authorised interception of all telephone communications in the area where a criminal offence had been committed[360] (this specific identification is also required when the interception regards

[351] *Zakharov v. Russia* ECHR 2015, para 237.
[352] *Zakharov v. Russia* ECHR 2015, para 242.
[353] *Zakharov v. Russia* ECHR 2015, para 244.
[354] *Zakharov v. Russia* ECHR 2015, para 253.
[355] *Zakharov v. Russia* ECHR 2015, para 259.
[356] *Zakharov v. Russia* ECHR 2015, para 245.
[357] *Zakharov v. Russia* ECHR 2015, para 248.
[358] *Zakharov v. Russia* ECHR 2015, para 261.
[359] *Zakharov v. Russia* ECHR 2015, para 262.
[360] *Zakharov v. Russia* ECHR 2015, para 265.

premises[361]), and lastly because the authorities were not required under domestic law to show the judicial authorisation to the communications service providers before obtaining access to a person's communications while they had all the technical means to access the data anyway[362]; the storing and destroying the intercepted data, and notably the lack of requirement to destroy immediately any data that are not relevant to the purpose for which they have been obtained[363] and the lack of indication, when a person has been charged with a criminal offence, as to the circumstances in which intercept material may be stored after the end of the trial[364]; the supervision mechanisms of the interception[365], as the Court observed that the supervisory authorities cannot adequately control interceptions or even discover that interceptions were carried out without proper judicial authorisation as equipment installed by the communication service providers did not record or log information about interception, and as the authorities, supervising the implementation of the statutory requirements relating to the implementation of the surveillance measures, the storage, access to, use, processing, communication and destruction of intercept materials where the supervision actually would be carried out on the basis of proper judicial authorisations, were not judicial ones, did not prove to be sufficiently independent, were limited with regard to the scope of their supervision, did not have their activities subjected to public scrutiny etc.; and, after the Court noted that it may not be feasible in practice to require subsequent notification in all cases[366], the effectiveness of the remedies available to challenge the interception, as the Court noted that remedies were only available to persons who are in possession of information about the interception of their communications, which seemed practicably impossible since there was not a requirement in the Russian system to notify the subject of interception at any point nor was there an adequate possibility to request and obtain information about interceptions from the authorities[367], and as the Court was not convinced that the remedies to challenge the alleged insufficiency of safeguards against abuse in Russian law before the Russian courts, were effective[368].[369]

Therefore, the Court concluded that the domestic law did not contain adequate and effective safeguards and guarantees against arbitrariness and the risk of abuse which was particularly high in a system such as in Russia where the secret services and the police had direct access, by technical means, to *all* mobile

[361] *Zakharov v. Russia* ECHR 2015, para 264.
[362] *Zakharov v. Russia* ECHR 2015, para 270.
[363] *Zakharov v. Russia* ECHR 2015, para 255.
[364] *Zakharov v. Russia* ECHR 2015, para 256.
[365] *Zakharov v. Russia* ECHR 2015, paras 272-285.
[366] *Zakharov v. Russia* ECHR 2015, para 287.
[367] *Zakharov v. Russia* ECHR 2015, para 298.
[368] *Zakharov v. Russia* ECHR 2015, para 299.
[369] Factsheet – Mass surveillance, 3.

telephone communications, to meet the requirements of 'foreseeability' and 'necessity in a democratic society'.[370] Hence, it found that there had been a violation of article 8 of the European Convention.[371]

f. Szabó and Vissy v. Hungary

104. On 12 January 2016, the European Court of Human Rights again, this time in a Hungarian case, found a violation of article 8 of the Convention due to absence of sufficient guarantees against abuse in legislation on secret surveillance.[372] In the same way as in the *Zakharov* case, the Court came to that conclusion after jointly assessing the 'foreseeability' and the 'necessity in a democratic society' of the measures laid down in the concerned domestic provisions.[373]

(1) Facts of the case

105. This case originates in an application against Hungary lodged with the Court by two Hungarian nationals, Mr Máté Szabó and Ms Beatrix Vissy, on 13 May 2014.[374] The applicants complained in particular that they could potentially be subjected to unjustified and disproportionately intrusive measures within the framework of 'section 7/E (3) surveillance' of the Police Act, which lays down the competence of the TEK, an Anti-Terrorism Task Force established in 2011, with regard to secret surveillance for national security reasons.[375]

(2) Ruling of the Court

106. Also in this case, the Court unanimously found that there had been a violation of article 8 of the European Convention on Human Rights.[376]

107. First, the Court ruled that in the mere existence of the legislation itself there is, for all those to whom the legislation could be applied, a menace of surveillance involved, which necessarily influences the freedom of communications between users and accordingly constitutes an 'interference by a public authority' with the exercise of the applicants right to privacy.[377]

---

[370] *Zakharov v. Russia* ECHR 2015, paras 242 and 302-304.
[371] *Zakharov v. Russia* ECHR 2015, 81.
[372] European Court of Human Rights, 'Legal summary – Szabó and Vissy v. Hungary' (Hudoc, January 2016) <http://hudoc.echr.coe.int/eng#{"itemid":["002-10821"]}> accessed 6 April 2017.
[373] *Szabó and Vissy v. Hungary* ECHR 2016, paras 55, 58 and 89.
[374] *Szabó and Vissy v. Hungary* ECHR 2016, para 1.
[375] *Szabó and Vissy v. Hungary* ECHR 2016, paras 3 and 10.
[376] *Szabó and Vissy v. Hungary* ECHR 2016, 45.
[377] *Szabó and Vissy v. Hungary* ECHR 2016, para 53.

108. As regards the justification of the interference, the Court noted that the interference had a legal basis and that the accessibility of the relevant rules had not been called into question.[378] Moreover, the Court found that the measures in question pursued a legitimate aim.[379]

In order to examine whether the 'forseeability' requirement and the condition of 'necessity in a democratic society' the Court applied the same approach as in the *Zakharov v. Russia* case (see nos. 103) and thus examined these requirements jointly.[380]

In that regard, the Court observed more specifically that under 'section 7/E (3) surveillance', it was possible for virtually any person in Hungary to be subjected to secret surveillance.[381] In particular, the Court took the view that the notion of 'persons concerned identified … as a range of persons' might include any person and might be interpreted as paving the way for the unlimited surveillance of a large number of citizens.[382] According to the Court, the category is overly broad, as there is no requirement of any kind for the authorities to demonstrate the actual or presumed relation between persons or range of persons 'concerned' and the prevention of any terrorist threat.[383] Furthermore, the Court stated that *"it would defy the purpose of government efforts to keep terrorism at bay, thus restoring citizens' trust in their abilities to main public security, if the terrorist threat were paradoxically substituted for by a perceived threat of unfettered executive power intruding into citizens' private spheres by virtue of uncontrolled yet far-reaching surveillance techniques and prerogatives".*[384] Moreover, the Court found that the ordering of the surveillance completely took place within the realm of the executive[385] and that there was no legal safeguard requiring the TEK to produce a sufficient factual basis for the application of secret intelligence gathering measures which would enable the evaluation of necessity of the proposed measure and this on the basis of an individual suspicion regarding the target person.[386] The mere requirement for the authorities to give reasons for the request, arguing for the necessity of secret surveillance, thus was considered to fall short in this regard and could not be considered as demonstrating the 'strict necessity' of the measure.[387] The Court further explained, for the first time, that a surveillance measure must be *"strictly necessary, as a general consideration, for the safeguarding of the democratic institutions and, moreover, as a particular consideration, for the obtaining of vital intelligence in an*

[378] *Szabó and Vissy v. Hungary* ECHR 2016, para 61.
[379] *Szabó and Vissy v. Hungary* ECHR 2016, para 55.
[380] *Szabó and Vissy v. Hungary* ECHR 2016, paras 56-58.
[381] *Szabó and Vissy v. Hungary* ECHR 2016, para 66.
[382] *Szabó and Vissy v. Hungary* ECHR 2016, para 67.
[383] Ibid.
[384] *Szabó and Vissy v. Hungary* ECHR 2016, para 68.
[385] *Szabó and Vissy v. Hungary* ECHR 2016, para 75.
[386] *Szabó and Vissy v. Hungary* ECHR 2016, para 71.
[387] Ibid.

individual operation".[388] On top of that, the Court noted that there was also no control by a judge or an independent body over the issuing body's activity (in this regard the CJEU in *Tele2 Sverige* referred to this case, see no. 87).[389] Moreover, the complaint procedures did not seem to be of much relevance as citizens in the first place were not notified of the surveillance and the authority responsible for the investigation did not appear to be sufficiently independent either.[390]

Consequently, the Court concluded that the Hungarian legislation on 'section 7/E (3) surveillance' did not provide sufficiently precise, effective and comprehensive safeguards on the ordering, the execution and potential redressing of such measures.[391]

g. Conclusion

109. The European Court of Human Rights, in these two cases, thus made clear that collection of personal data cannot be conducted on mass scale, but should, instead, always be targeted. Surveillance measures can only be used when it is 'strictly necessary' in general as well as on an individual level. The domestic law must clearly define the categories of persons which might be subjected to a surveillance measure and when such measures are applied in practice. The authorities must prove that there is a 'real suspicion' on the part of the 'person concerned' which can justify the surveillance of a specific person or of a single set of premises.[392] Only data that will effectively be used by the authorities can be collected. However, there should also be clear rules governing the storage, use and communication of intercepted data in order to minimise the risk of unauthorized access or disclosure. Moreover, there should be adequate procedures in place for authorizing the specific surveillance measures in order to supervise the surveillance practices. Lastly, the Court requires the availability of effective remedies to challenge the interception.

Secret surveillance measures should in any event be surrounded by numerous conditions and the domestic law must in that regard contain adequate and effective safeguards and guarantees against arbitrariness and the risk of abuse.

---

[388] *Szabó and Vissy v. Hungary* ECHR 2016, para 73; Sarah St.Vincent, 'Did the European Court of Human Rights Just Outlaw "Massive Monitoring of Communications" in Europe?' (Center for Democracy & Technology (CDT), 13 January 2016) < https://cdt.org/blog/did-the-european-court-of-human-rights-just-outlaw-massive-monitoring-of-communications-in-europe/> accessed 9 April 2017.
[389] *Szabó and Vissy v. Hungary* ECHR 2016, 77.
[390] *Szabó and Vissy v. Hungary* ECHR 2016, 83.
[391] *Szabó and Vissy v. Hungary* ECHR 2016, para 89.
[392] Sarah St.Vincent, 'Did the European Court of Human Rights Just Outlaw "Massive Monitoring of Communications" in Europe?' (Center for Democracy & Technology (CDT), 13 January 2016) <https://cdt.org/blog/did-the-european-court-of-human-rights-just-outlaw-massive-monitoring-of-communications-in-europe/> accessed 9 April 2017.

D. Main findings and conclusive remarks

110. When personal data is transferred from the EU to a third country, the adequacy of the data protection regime of that country has to be established. In this Chapter, it became clear that an adequacy assessment requires not only an evaluation of the substantive data protection standards in place in a third country, but also an examination of the formulation and the implications of derogations provided with respect to the substantive standards.

111. As regards the substantive data protection standards, core 'content' principles as well as core 'procedural/enforcement' requirements have been identified.

The 'content' requirements concern the principles of 'purpose limitation', 'proportionality', 'data quality', 'transparency' and 'data security', the rights of 'access', 'rectification' and 'opposition', the 'restrictions on onward transfers' (adequacy requirement), and a number of 'additional principles' which apply to specific types of processing.

The 'procedural/enforcement' requirements demand mechanisms that ensure good compliance with the rules, that support and help individual data subjects and that guarantee an injured party (data subject) the right to redress where rules are not complied with.

112. As regards the derogations provided with respect to the substantive standards, both the Court of Justice and the European Court of Human Rights take the view that the collection, retention, access or use of personal data, regardless of whether it concerns 'content' or metadata, originally processed for other purposes, by or to the benefit of the government, constitute an interference with respectively articles 7 and 8 of the EU Charter on Fundamental Rights and article 8 of the European Convention on Human Rights. The CJEU stated that it does not matter whether the data are sensitive in their nature or whether the persons involved have been conceived in one way or another. The ECtHR ruled that such an interference derives from the mere existence of legislation allowing such surveillance practices.

As regards the justification of these measures, neither of the courts detected problems with respect to the 'legality' or the 'objective of general interest' requirements. On the other hand, the main issue in every case that has been discussed concerned the 'proportionality' and more in particular the 'strict necessity' of the interferences. According to the Court in Strasbourg, a surveillance measure must fulfil this requirement in general as well as on an individual level. Both courts moreover require the domestic law to be sufficiently clear and precise in that regard and to provide for minimum safeguards against abuse of powers. On that account, both courts ruled out the possibility for the government, as a matter of principle, to undertake surveillance in a general, indiscriminate and untargeted manner. From the Court of Justice's case law, and especially from its ruling in the *Tele2 Sverige* case, it became particularly clear that the mass 'collection'/'retention' of personal data in itself, even when there are sufficient

safeguards in place to limit the actual 'access' to and 'use' of the data by the competent authorities to what is 'strictly necessary', cannot be considered to be a justified interference with an individual's fundamental rights. Personal data may thus only be collected insofar intelligence or law enforcement authorities actually need the information in question. Preventively collecting personal data on mass scale in order to be able, in a later phase, to search the gathered info in a tailored manner, can thus not be regarded as 'strictly necessary' or 'proportionate'. The Court of Justice suggested the retention (*in casu* by the service providers) to be restricted to data pertaining to a particular time period and/or a particular geographical zone and/or a circle of particular persons likely to be involved, in one way or another, in serious crime, while the European Court of Human Rights, in *Zakharov v. Russia*, stated that surveillance measures should only be authorized when there is a 'sufficient factual basis to reasonably suspect a particular person'. Both courts also require the legislation to lay down objective criteria with regard to the duration of the surveillance measures and rules as regards the storage and deletion of data.

113. The Court of Justice of the European Union also paid particular attention to the measures that should be taken in view of the effective security and protection of collected data (*in casu* by the service providers). The European Court of Human Rights also took the view that there should be rules in place governing the storage, use and communication of intercepted data in order to minimise the risk of unauthorized access or disclosure. This is of course a very important aspect of the right to privacy and more in particular, at EU level, of the right to data protection. However, this aspect will not further be discussed in depth in the context of this thesis. Nonetheless, a third country should of course also have measures in place in this regard.

114. The Court of Justice as well as the European Court of Human Rights also require the installation of (an) independent supervisory mechanism(s), which monitor(s) the surveillance practices so as to ensure 'good compliance' with the rules, and the provision of a right for every person to a (judicial) remedy in case their rights have nevertheless been breached.

In order to assure 'good compliance' with the rules and more specifically to ensure that such interferences with the privacy rights of an individual is limited to what is 'strictly necessary', the CJEU requires the access by public authorities to personal data (*in casu* collected by electronic communications service providers) to be subjected to prior review, whereas the ECtHR demands surveillance measures to be authorised. The Court in Strasbourg has drawn up its conclusions in cases where prior authorisation to collect the data and the subsequent access to data would be difficult to distinguish.[393] On the contrary,

[393] Working Party on the Protection of Individuals with regard to the Processing of Personal Data, 'Working Document 01/2016 on the justification of interferences with the fundamental rights to privacy and data protection through surveillance measures when transferring personal data (European Essential Guarantees)' [2016] Working Document WP237, 10 <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2016/wp237_en.pdf> accessed 18 April 2017 ['Working Party 29 WP237'].

the facts in the cases dealt with by the CJEU did allow such a distinction. However, from the entirety of the jurisprudence of those courts in this regard, it is clear that prior authorisation or review is required from the moment intelligence or law enforcement authorities want to gain access to personal data, whether the phases of collection and access coincide, such as in the ECtHR cases, or whether there is a clear distinction between the phases of collection, by actors in the private sector, and access, by the authorities, such as in the cases before the CJEU. Such supervision, as a rule, is needed when the surveillance is first ordered, however, in urgent cases, it can be carried out while the surveillance is being conducted. According to the ECtHR, supervision in the course of the execution of the surveillance may also be required and this in order to reassure that the continuation of the measure is necessary. Both the CJEU and the ECtHR consider it desirable to entrust this supervision to a court. However, it may also be assigned to an administrative body, provided that its independence is assured.

Both courts also stressed that individuals should, of course, be provided with a right to a (judicial) remedy when they take the view that surveillance by the government has in some way or another violated their rights. At EU level, such a right is enshrined in article 22 of directive 95/46/EC, article 15, §2 of directive 2002/58/EC and in article 47 of the EU Charter. The Court of Justice put forward in the *Schrems* case that article 47 of the Charter also requires data subjects to have the right to request access to or the rectification or erasure of data that has been obtained by the government for reasons of national security or law enforcement. Moreover, despite the fact that in article 47 of the English language version of the Charter individuals are granted the right to an effective remedy before a 'tribunal', and thus not necessarily before a 'court', in other language versions of the Charter preference is given to the word 'court'.[394] Article 22 of directive 95/46/EC moreover stipulates that Member States may also provide for a right to an administrative remedy and this *inter alia* before the supervisory authorities referred to in article 28 of that directive, prior to referral a judicial authority. The provision of such an administrative remedy, however, does not seem to be obligatory. At the level of the Council of Europe, the right to an effective remedy is of course embodied in article 13 of the ECHR. This article only obliges the Member States ensure that *"everyone whose rights and freedoms (…) are violated shall have an effective remedy before a national authority".*[395] According to the case law of the ECtHR, this does not necessarily need to be a judicial authority.[396] The CJEU as well as the ECtHR also noted that individuals that have been the subject of a surveillance measures have to be notified thereof as soon as such a notification is no longer liable of jeopardising the pursued aim of the measure in question in order to ensure their right to an effective judicial remedy is not compromised, unless the concerned individuals can be informed of the surveillance in another way.

---

[394] Working Party 29 WP237, 11.
[395] Working Party 29 WP237, 11
[396] *Klass and others v Germany* (1978) Series A no 28, para 67; Working Party 29 WP237, 11.

115. In all 3 cases, and especially in *Schrems*, the Court of Justice also stressed the importance of the national supervisory authorities in view of the monitoring of compliance with the EU data protection principles and referred in that regard in particular to article 8, §3 of the EU Charter on Fundamental Rights.

116. The main findings in this Chapter with regard to the 'permissibility of exceptions' correspond, to a relatively great extent, with the conclusions of the Article 29 Working Party in its recently adopted 'Working Document 01/2016 on the justification of interferences with the fundamental rights to privacy and data protection through surveillance measures when transferring personal data (European Essential Guarantees)'[397], in which it identified four 'European Essential Guarantees', by way of analysing the case law of the Court of Justice and the European Court of Human Rights, which should be in place to make sure that interferences with the right to privacy and the right to data protection do not go beyond what is necessary in a democratic society.[398] The 'Guarantees' stipulate that processing should be based on clear, precise and accessible rules (1), the said interferences should be necessary and proportionate with regard to the legitimate objectives pursued (2), there should be an independent oversight mechanism in place (3) and there need to be effective remedies available to the individual (4).

117. In sum, the data protection regime in place in a third country must be compliant with EU primary and secondary law and the relevant judgments of both the European Court of Justice and the European Court of Human Rights in order to be deemed 'adequate' in the light of article 25 of Directive 95/46/EC.[399]

[397] Working Party 29 WP237.
[398] ECHR, art 13; Working Party 29 WP237, 6.
[399] European Parliament Resolution 2016/2727(RSP), 'Transatlantic data flows' (2016) <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+TA+P8-TA-2016-0233+0+DOC+PDF+V0//EN> accessed 25 April 2017 ['European Parliament Resolution 2016/2727(RSP)'].

CHAPTER 3. ADEQUACY OF THE U.S. DATA PROTECTION REGIME AS COMPLEMENTED BY THE EU-U.S. PRIVACY SHIELD IN THE LIGHT OF THE SUBSTANTIVE EU DATA PROTECTION STANDARDS AND THE EU REQUIREMENTS IN CASE OF DEROGATIONS TO THE BENEFIT OF GOVERNMENT AUTHORITIES

A. Introduction

118. In Chapter 1, it has been explained that according to EU law a transfer of personal data to a third country may only take place when that country ensures an adequate level of data protection. More in particular, its level of protection must prove to be 'essentially equivalent' to that guaranteed within the European Union. In Chapter 2, therefore, the principles and requirements that are indispensable in the EU in the context of data protection have been addressed. Accordingly, in order to assess whether the data protection regime of a third country meets the 'adequacy requirement', the concrete data protection rules in place in that country have to be weighed against those assured within the European borders.

119. In Chapter 1, it also has been put forward that the European Commission may find that a third country in fact ensures an adequate level of data protection and this by reason of its domestic law or of the international commitments it has entered into. The effect of such a decision is that personal data may be freely transferred from the EU to the third country in question without there being a need, for the controller, to adduce additional safeguards.

With respect to the United States, the Commission had, on 26 July 2000, adopted such an adequacy decision.[400] This decision enabled the free flow of data from companies established in the EU to U.S. based companies when the latter self-certified their adherence the Safe Harbour principles.[401] However, as explained in Chapter 2, the Court of Justice of the European Union invalidated this so-called 'Safe Harbour' Decision on 6 October 2015 in the *Schrems* case (see no. 94). This judgment was one of the logical consequences of the Snowden revelations, which unveiled the existence of mass surveillance programmes in the United States. The ruling indeed merely confirmed what, by that time, was clear to anybody: the harbour had never been safe.[402] Also the European Commission realised this as it, even prior to the ruling of the Court in *Schrems*, in its two communications to the European Parliament and the Council of 27 November 2013 concerning the impact of the said disclosures on EU-U.S. data flows,

---

[400] Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce [2000] OJ L215/7 ['Safe Harbour Decision'].

[401] Safe Harbour Decision, 10: organisations could also qualify for the safe harbour in different ways: for example, if an organization joined a self-regulatory privacy program that adheres to the Principles, it qualified for the safe harbour. Organisations could also qualify by developing their own self-regulatory privacy policies provided that they were conform with the Principles.

[402] Xavier Tracol, '"Invalidator" strikes back: The harbour has never been safe; Gert Vermeulen, 'The Paper Shield', 2.

stated that measures had to be taken in order to make the Safe Harbour safer.[403] Such measures, still according to the Commission, were necessary to "*rebuild trust in EU-U.S. data flows"*.[404] After *Schrems*, however, strengthening the Safe Harbour scheme, which in accordance with article 4 of the Commission's decision 2000/520/EC could indeed be 'adapted', could no longer suffice. While the Commission noted that data transfers from the European Union to the United States nevertheless remained possible using Standard Contractual Clauses or Binding Corporate Rules (see nos. 27-30), it, at the same time, declared that it was still committed to the goal of a renewed and sound framework for transatlantic transfers of personal data.[405] Accordingly, the Commission, on 12 July 2016, adopted a new adequacy decision, which, as previously mentioned, concerns more specifically the 'adequacy of the protection provided by the EU-U.S. Privacy Shield'.[406] This decision again enables data flows from the EU to the U.S. for commercial purposes. Whether the U.S. data protection regime as now, in the EU-U.S. relation, complemented by the EU-U.S. Privacy Shield can indeed be considered adequate in the light of the substantive EU data protection standards and the EU requirements in case of derogations thereto to the benefit of government authorities, will be discussed in this Chapter.

120. The European Data Protection Supervisor, on the basis of article 28, §2 and 41, §2 of Regulation 45/2001[407] and in line with Action 9 of the EDPS Strategy on 'facilitating responsible and informed policymaking', the Working Party on the Protection of Individuals with regard to the processing of personal data, on the basis of article 30, §1 of Directive 95/46/EC, and the European Parliament in a resolution on 'transatlantic data flows', have already given their opinion in that regard with respect to the Privacy Shield *draft* adequacy decision.[408] In a press release issued on the day of the adoption of the *final* adequacy decision, the European Commission accordingly stated that it had drawn on these opinions to include a number of additional clarifications and improvements in the Privacy Shield. It clarified

---

[403] COM (2013) 846 final, point 3; COM (2013) 847 final, point 8.
[404] COM (2013) 846 final, point 4.
[405] Commission, 'Communication from the Commission to the European Parliament and the Council on the Transfer of Personal Data from the EU to the United States of America under Directive 95/46/EC following the Judgment by the Court of Justice in Case C-362/14 (Schrems)' COM (2015) 566 final, point 1 ['COM (2015) 566 final'].
[406] Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council of the adequacy of the protection provided by the EU-U.S. Privacy Shield [2016] OJ L207/1 ['Privacy Shield Decision'].
[407] Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data [2001] OJ L8/1 ['Regulation 45/2001'].
[408] European Data Protection Supervisor, 'Opinion on the EU-U.S. Privacy Shield draft adequacy decision' [2016] Opinion 4/2016 <https://edps.europa.eu/sites/edp/files/publication/16-05-30_privacy_shield_en.pdf> accessed 25 April 2017 ['EDPS Opinion on the EU-U.S. Privacy Shield draft adequacy decision']; Working Party on the Protection of Individuals with regard to the Processing of Personal Data, 'Opinion 01/2016 on the EU-U.S. Privacy Shield draft adequacy decision' [2016] Opinion WP238 <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2016/wp238_en.pdf> accessed 25 April 2017 ['Working Party 29 WP238']; European Parliament Resolution 2016/2727(RSP).

that it had agreed with the U.S. on *"additional clarifications on bulk collection of data, strengthening the Ombudsperson mechanism, and more explicit obligations on companies as regards limits on retention and onward transfers".*[409] The European Parliament, moreover, recently adopted another resolution on 6 April 2017 this time specifically regarding the 'adequacy of the protection afforded by the EU-US Privacy Shield'.[410]

121. The structure of this Chapter will be as follows: firstly, the structure of the adequacy decision and the functioning of the EU-U.S. Privacy Shield will be discussed (B); secondly, the (in)adequacy of the substantive data protection requirements to which U.S. self-certified companies are ought to adhere to will be examined (C); thirdly, the (in)adequacy of the U.S. data protection policy in case of interferences with EU privacy and data protection rights by the U.S. authorities will be assessed (D); and finally, a conclusion will be formulated (E).

B. Structure of the adequacy decision and functioning of the EU-U.S. Privacy Shield

122. As regards the structure of the Privacy Shield adequacy decision, the large volume of this document compared to that of the former Safe Harbour Decision immediately attracts attention. While the latter consisted of 41 pages, the Privacy Shield Decision contains 112.

This can be explained by the extensive clarifications given in the recitals preceding the actual decision, which in itself only consists of 6 articles, and the big amount of annexes attached to it. In that regard, it is stipulated in article 1, §2 of the adequacy decision that *"the EU-U.S. Privacy Shield is constituted by the Principles issued by the U.S. Department of Commerce on 7 July 2016 as set out in Annex II and the official representations and commitments [by the U.S. administration] contained in the documents listed in Annexes I, III to VII"*. The principles and guarantees afforded by the Privacy Shield are set out in both the adequacy decision, namely in the recitals, and in its annexes, making the information difficult to find as well as inconsistent at times.[411] Accordingly, the decision will not be remembered for the accessible and clear manner in which it is drawn up.

123. As regards the functioning of the EU-U.S. Privacy Shield, article 1, §1 of the adequacy decision states that *"for the purposes of Article 25, §2 of Directive 95/46/EC, the United States ensures an adequate level of protection for personal data transferred from the Union to organisations in the United*

---

[409] Commission, 'European Commission launches EU-U.S. Privacy Shield: stronger protection for transatlantic data flows' (Press release, 12 July 2016) <http://europa.eu/rapid/press-release_IP-16-2461_en.htm> accessed 25 April 2017.
[410] European Parliament Resolution 2016/3018(RSP), 'Adequacy of the protection afforded by the EU-US privacy Shield' (2016) <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-%2F%2FEP%2F%2FNONSGML%20TA%20P8-TA-2017-0131%200%20DOC%20PDF%20V0%2F%2FEN> accessed 25 April 2017 ['European Parliament Resolution 2016/3018(RSP)'].
[411] Working Party 29 WP238, 2.

States under the EU-U.S. Privacy Shield". As this framework is based on several letters and unilateral statements from the U.S. administration, making up the Annexes to the adequacy decision and thus, as stipulated in the preceding paragraph, forming the actual EU-U.S. Privacy Shield, the 'adequacy' of the U.S. data protection regime essentially stems from the international commitments the U.S. has entered into rather than from its domestic law.[412] The U.S., by way of this framework, thus more or less created an *ad hoc* data protection regime implemented and applied in the U.S. to the extent necessary to ensure an 'adequate' level of protection for personal data transferred there from the EU.

The EU-U.S. Privacy Shield Decision in essence sets out two types of rules: those applicable to U.S. companies that wish to receive personal data originally processed within the European Union, and those applicable to the U.S. authorities when they collect the said data from the said companies in order to further process these data for government purposes.[413]

A U.S. organisation, in order to rely on the Privacy Shield adequacy decision to effectuate transfers of personal data from the EU, must self-certify its adherence to 'the Principles' to the Department of Commerce (or its designee).[414] These Principles, which consist of the actual 'Privacy Principles' (7) and the 'Supplemental Principles' (16), are issued by the said Department, though developed in consultation with the European Commission, and are set out in Annex II to the adequacy decision (see no. 122).[415] According to the U.S., the Principles are merely drawn up because the U.S. takes a different approach to privacy, namely a sectoral one that relies on a mix of legislation, regulations and self-regulation, and, by way of this framework, wants to offer organisations in the United States a reliable mechanism for personal data transfers from the EU to the U.S. while ensuring that EU data subjects continue to benefit from effective safeguards and protection as required by EU data protection law.[416] The Court of Justice of the European Union, in the *Schrems* case, stated that a system of self-certification is not in itself contrary to the requirement laid down in article 25, §6 of directive 95/46/EC that the country concerned must ensure an adequate level of protection 'by reason of its domestic law or … international commitments', but that its reliability, in the light of that requirement, is founded essentially on the establishment of effective detection and supervision mechanisms which can ensure compliance with the rules (see no. 94).[417] In that regard the Principles also set out an extensive arsenal of oversight, redress, complaint handling and enforcement mechanisms.[418] The way in which the 'adequacy requirement' with regard to

[412] Directive 95/46/EC, art 25(6).
[413] Privacy Shield Decision, recitals 14-63 and 64-135.
[414] Privacy Shield Decision, Annex II, I.
[415] Ibid.
[416] Ibid.
[417] *Schrems*, para 81.
[418] Privacy Shield Decision, recitals 30-64.

the U.S. organisations is dealt with, is thus no different from the manner in which this was handled under the Safe Harbour scheme.

The obligations, as described in the adequacy decision, upon the U.S. authorities, unlike the Principles and their subsequent enforcement, largely originate from U.S. domestic law adopted under the Obama administration following the Snowden disclosures.[419] The letters annexed to the decision mainly provide information as regards the application of the legislation as well as commitments in that regard. The lack of any findings in this regard in the Safe Harbour Decision, while it did on the other hand stipulate that adherence to the Safe Harbour principles could be limited for a number of vaguely formulated government purposes, and the revelations made by Edward Snowden with regard to the existence and extent of mass surveillance programmes in the U.S., had led the CJEU, in *Schrems*, to conclude that the Safe Harbour Decision did not demonstrate that the U.S. indeed ensures an adequate level of data protection (see no. 94).[420] The Privacy Shield Ombudsperson Mechanism on the other hand, which grants individual EU data subjects an additional redress avenue when they presume they have been the subject of unlawful (electronic) surveillance for national security purposes, has been created by the U.S. government in view of the Privacy Shield adequacy decision.[421] This mechanism must satisfy the demands of the Court of Justice, as stressed in the *Schrems* judgment, as regards the fundamental right to effective judicial protection as enshrined in article 47 of the Charter. More specifically, the Court ruled that legislation not providing for any possibility for an individual to pursue legal remedies in order to have access to personal data relating to him, or to obtain rectification or erasure of such data, does not respect the essence of the said right (see no. 94).[422]

124. As also required by the Court of Justice in *Schrems*, article 4, §1 of the Privacy Shield Decision stipulates that *"[t]he Commission will continuously monitor the functioning of the EU-U.S. Privacy Shield with a view to assessing whether the United States continues to ensure an adequate level of protection of personal data transferred thereunder from the Union to organisations in the United States".* This evaluation should moreover take place every year.[423] The EU Commissioner for Justice, Věra Jourová, during her visit to the U.S. in the beginning of May 2017, said that the first review of the Privacy Shield will take place in September 2017.[424]

---

419 <https://edwardsnowden.com/2014/01/17/presidential-policy-directive-ppd-28-concerning-signals-intelligence-activities/> (Website Edward Snowden) accessed 26 April 2017.
420 *Schrems*, paras 67-98.
421 Privacy Shield Decision, recitals 115-116.
422 *Schrems*, para 95; Privacy Shield Decision, recital 124.
423 Privacy Shield Decision, art 4(4).
424 'EU-US Privacy Shield review now promised for September' (Privacy Laws & Business, 5 May 2017) <http://www.privacylaws.com/int_enews_5_4_17> accessed 26 April 2017.

C. Adequacy assessment of the substantive data protection requirements to which U.S. self-certified companies are ought to adhere

125. As is the case in EU data protection law, the Privacy Shield adequacy decision sets out privacy and data protection 'content' principles as well as 'procedural/enforcement' mechanisms.[425] Accordingly, the substantive data protection principles will be assessed in two parts (1 and 2). According to Ken Hyatt, the Acting Under Secretary for International Trade from the U.S. Department of Commerce, in a letter to Věra Jourová that is annexed to the Privacy Shield Decision, stipulated that the Principles strengthens the protection of privacy, as compared to the protection provided under the Safe Harbour framework, in a number of ways: additional information must be provided to individuals under the 'Notice Principle', the rules regarding 'Onward Transfers' now require the conclusion of a contract, controller liability in case of transfers of personal data to a third party acting as an agent has been included, organisations may only process personal information that is relevant to the purpose of the processing, they must annually re-certify their adherence, independent recourse mechanisms must be provided to the individual at no cost, complaints and inquiries must be responded promptly to by organisations, and independent recourse mechanisms and organisations must publish reports it submitted to the Federal Trade Commission (FTC) if it becomes subject to an FTC or court order based on non-compliance.[426] Indeed, there was a need for improvements as the European Commission, in its two Safe Harbour communications of November 2013 (see no. 119), had identified structural shortcomings that, next to those in relation to the national security exception, related to the Safe Harbour Principles as well as to transparency and their enforcement.[427]

126. The Principles are applicable to both U.S. controllers and processors (agents) insofar the processing by these organisations does not fall within the scope of Union legislation[428] and where they are relevant *"unless otherwise stated"*[429].This means for example that when personal data is transferred from the Union to the United States merely for processing purposes, there is no need to repeat the obligation for EU controllers to enter in a contract with a U.S. processer, as EU controller are in any case, on the basis of article 17, §3 of Directive 95/46/EC required to do this, regardless of whether or not the processing operation is carried out inside or outside the EU.[430] Nevertheless, this is obligation is reiterated, in order to ensure that this obligation is also incumbent on a U.S. processor, in Supplemental Principle No. 10 on 'Obligatory Contracts for Onward Transfers', which moreover adds that the conclusion of a contract

[425] Privacy Shield Decision, recitals 16-18.
[426] Privacy Shield Decision, Annex I, 1-2.
[427] COM (2013) 846 final, 7; COM (2013) 847 final, 2-15.
[428] Privacy Shield Decision, recital 14-15.
[429] Privacy Shield Decision, Annex II, I, 7; European Parliament Resolution 2016/3018(RSP), point 15.
[430] Privacy Shield Decision, Supplemental Principle No. 10.

in those circumstances is required regardless of participation by the processor in the Privacy Shield.[431] The difference, however, with regard to the content of such a contract, as compared to the requirements under EU law in that regard (see no. 47), seems to be that the processor can also, when it self-certified, be required to assist the controller in responding to individuals exercising their rights *under the Principles*.[432] It cannot be explained, however, how a data subject whose data is being processed by a U.S. processor on behalf of an EU controller would exercise its right under the Principles. Rather, it would do this directly on the basis of the national provisions adopted pursuant to Directive 95/46/EC. It is also unclear why exactly this additional requirement has been included since no such provision exists under EU law. Moreover, the fact that Supplemental Principle No. 10 also implied that a U.S. processor, merely, for the purpose of processing, receiving personal data from an EU controller, can still self-certify to the Privacy Shield framework, raises additional questions. More specifically, it is not clear from the Privacy Shield adequacy decision to what extent the Principles apply to processors.[433] Contrary to EU law, where processors have been explicitly allocated responsibility with regard to 'data security' and the 'confidentiality of communications' (see nos. 47-48), processors, under the Privacy Shield scheme, seem to be responsible in the same way as controllers under the Privacy Shield, as every Principle in the adequacy decision generally addresses 'organisations [that are self-certified]'.[434] The same problem occurs with regard to U.S. processors receiving data from U.S. controllers. For instance, it is logical that Principle No. 4 on 'data security' applies to processors (the Principles do not include a principle on 'data security'), however, several other obligations included in the Principles are not suitable for data processors, as it is always the controller who determines the purposes and means of the processing of data.[435] For example, the processor will not be able to provide individuals with full 'Notice' (see nos. 128-129) because this organisation does not determine the purposes of the processing.[436] Moreover, U.S. processors should not have bear more responsibility than processors according to EU law.

1. Content principles

127. In this subsection it will be examined to what extent the 'content' principles, as they have been drawn up under EU law, are reflected in the Principles issued by the U.S. Department of Commerce. Only the Principles that correspond with the 'core' content principles at Union level will be assessed.

[431] Privacy Shield Decision, Supplemental Principle No. 10.
[432] Ibid.
[433] Working Party 29 WP238, 16; European Parliament Resolution 2016/3018(RSP), point 12 and 15.
[434] Working Party 29 WP238, 16.
[435] Ibid.
[436] Ibid.

a. Notice

128. The 'Notice' Principle sums up what a that self-certified organisations should inform an individual about.[437] To a large extent this list corresponds with what is required under the 'transparency' principle under EU law (see nos. 45-46). The organisations also have to communicate their participation in the Privacy Shield and need to acquaint data subjects with the procedural/enforcement mechanisms available by virtue of this framework. However, despite the fact that the companies have to inform individuals about their right to access their personal data, there is no prescription of a reference to their right to rectification.[438]

129. As regards the timing of provision of this information, the 'Notice' Principle states that it must be provided *"when individuals are first asked to provide personal information to the organisation or as soon thereafter as is practicable, but in any event before the organisation uses such information for a purpose other than that for which it was originally collected or processed by the transferring organisation or discloses it for the first time to a third party"*.[439] It is however unclear how a self-certified U.S. organisation receiving data from a European company would directly obtain personal data from an individual data subject.[440] Instead, U.S. organisations necessarily should be required to provide this information at the same point in time as is envisaged in article 11 of Directive 95/46/EC, being *"at the time of undertaking the recording of personal data or if a disclosure to a third party is envisaged"*.

b. Choice

130. Privacy Principle No. 2 on 'Choice' offers individuals a right to opt-out when their data is to be disclosed to a third party, though this is not in general requested by EU law, or to be used for a purpose that is materially different from the purpose(s) for which it was originally collected or subsequently authorized[441], though EU law does not prescribe such a right for either of these processing operations[442]. According to the Article 29 Working Party, no detail is provided about the manner and the moment this opt-out may be exercised while an individualised opportunity to exercise this right should be offered *before* the disclosure or re-use of personal information.[443] However, the use of the words 'to be' seems

[437] Privacy Shield Decision, Privacy Principle No. 1.
[438] Working Party 29 WP238, 19-20.
[439] Privacy Shield Decision, Privacy Principle No. 1.
[440] Working Party 29 WP238, 19; compare with article 10 of Directive 95/46/EC.
[441] Privacy Shield Decision, Privacy Principle No. 2.
[442] Article 14(1)(b) of Directive 95/46/EC does however grant individuals the right to be informed before personal data are disclosed for the first time to third parties or used on their behalf for purposes of direct marketing and to be expressly offered the right to object to such disclosures or uses.
[443] Working Party 29 WP238, 19.

to point out exactly that. Moreover, organisations must obtain the affirmative express consent (opt in) of individuals insofar 'sensitive data' are to be processed for either one of those purposes.[444]

Supplemental Principle No. 12 on 'Choice – Timing of Opt Out' on the other hand relates to the right to opt-out in case of processing of personal data for direct marketing purposes. It is stated that, as the 'Choice' Principle aims at ensuring that personal information is used and disclosed in ways that are consistent with the individual's expectations and choices, an individual should be able to exercise 'opt out' choice of having personal information used for direct marketing 'at any time' and 'subject to reasonable limits'.[445] In this case, the EU demand that a right to object should be available to the data subject when it is *anticipated* that its personal data will be used for such purposes seems to be met.

131. A greater concern, however, is the fact that the Privacy Shield Principles do not foresee in a more general right for a data subject to object 'at any time' on compelling legitimate grounds relating to his particular situation to the processing of data relating to him (see no. 50).[446]

c. Accountability for Onward Transfer

132. Under this Principle, self-certified organisations have to fulfil certain conditions in order to lawfully further transfer personal data they have received on the basis of the Privacy Shield. To transfer personal information to a third party controller, organisations must enter into a contract with this controller that amongst others provides that the transferred data may only be processed for limited and specified purposes and that the recipient will provide the same level of protection as the Principles.[447] As regards onward transfers to U.S. controllers it is, however, desirable that these companies would also be required to self-certify, as this would more effectively ensure the protection of personal data. Indeed, within the European Union all controllers are also required to comply with the same rules adopted by the government and this precisely to enable intra-community data flows while ensuring a high level of data protection (see no. 14).[448] With respect to onward transfers to non-U.S./non-EU controllers, the Article 29 Working Party considered that Privacy Shield organisations should, prior to transfer, be obliged to make an assessment of the adequacy of the overall privacy framework in place in the third country in which the third part controller is established as this country might have laws providing for public access to personal data for example for purposes of surveillance which might lead to unjustified interferences with the privacy and data protection.[449] This clearly is a very difficult exercise for individual organisations.

---

[444] Privacy Shield Decision, Privacy Principle No. 2.
[445] Privacy Shield Decision, Supplemental Principle No. 12.
[446] Directive 95/46/EC, art 14(1)(a); Working Party 29 WP238, 20; European Parliament Resolution 2016/3018(RSP), points H and 12; EDPS Opinion on the EU-U.S. Privacy Shield draft adequacy decision, 7.
[447] Privacy Shield Decision, Privacy Principle 3.
[448] Directive 95/46/EC, art 1.
[449] Working Party WP238, 21.

This problem would supposedly not occur with regard to onward transfers to U.S. controllers, whether or not these are self-certified, since the second part of the Privacy Shield specifically addresses this issue in relation to the United States and more in particular states that the U.S. does have sufficient safeguards in place in that regard (whether or not this is the case will be discussed in point D of this Chapter).

As regards onward transfers to third party processors (agents) the conclusion of such a contract is also required, however, it is not expressly stated, contrary to the EU requirements in that regard[450], that they shall only act on instructions from the controller.[451]

133. Moreover, from this Principle itself is not clear to what extent an organisation is liable when the said conditions are not fulfilled or when the third party does not comply with the contractual provisions. However, in Privacy Principle No. 7 on 'recourse, enforcement and liability' it is stipulated that *"in the context of an onward transfer, a Privacy Shield organisation has responsibility for the processing personal data it receives under the Privacy Shield and subsequently transfers to a third party agent"*.[452] No reference is made however to the liability of an organisation for onward transfers to third party controllers.

134. Additionally, it appears from recital 29 to the adequacy decision that these obligations are incumbent on Privacy Shield controllers and not on Privacy Shield processors. As the Principles simply refer to the 'organisation', this observation is not straightforward (see no. 126).

d. Security

135. On the matter of 'data security', the Principles are brief as it merely stated that *"organisations creating, maintaining, using or disseminating personal information must take reasonable and appropriate measures to protect it from loss, misuse and unauthorized access, disclosure, alteration and destruction, taking into due account the risks involved in the processing and the nature of personal data"*.[453] This seems sufficient in the light of EU data protection law, apart from the fact that it is not mentioned that organisations must also take into account the state of the art as regards security measures.[454]

e. Data integrity and purpose limitation

136. The 'Data integrity and purpose limitation' Principle does not expressly state that personal data should be processed for *"specified, explicit and legitimate purposes"*.[455] This is of course problematic

[450] Directive 95/46/EC, art 17(3).
[451] Privacy Shield Decision, Privacy Principle No. 3.
[452] Privacy Shield Decision, Privacy Principle No. 7.
[453] Privacy Shield Decision, Privacy Principle No. 4.
[454] Directive 95/46/EC, art 17(1).
[455] Privacy Shield Decision, Privacy Principle No. 5; Directive 95/46/EC, art 6(1)(b).

as the 'purpose limitation' principle is one of the cornerstones of EU data protection law since it requires the controller, who indeed the determines the purpose(s) of the processing, to carefully assess what purpose(s) the personal data will be used for (see no. 41).[456] At the same time, it is provided that an organisation may not process personal information in a way that is incompatible with the purposes for which it has been collected or subsequently authorized by the individual.[457] EU law also allows the further processing of personal data for purposes which are not incompatible with the initial processing purposes (see no. 41).[458] The 'Choice' Principle moreover provides a right to opt out where a new (changed) purpose is materially different but still compatible with the original purpose (see no. 130).[459]

137. This Principle also states that personal data must be limited to the information that is relevant for the purposes of the processing.[460] This relates to the 'proportionality' principle as provided by EU law (see no. 42), but is in any case insufficient in that regard. In order to meet the proportionality requirement, the data must also not be excessive in relation to the purpose for which they are collected and/or further processed and thus must prove to be really necessary in that regard.[461] The Article 29 Working Party had suggested to amend the final adequacy decision in that regard, in vain apparently.

138. As regards 'data integrity', this Principle states that *"to the extent necessary for those purposes, an organisation must take reasonable steps to ensure that personal data is reliable for its intended use, accurate, complete and current"*[462], which correspond with the EU requirements on data quality. The Working Party had suggested to leave out the first part of the quotation[463], however, this comment seemed to be fruitless as well.

f. Access

139. Privacy Principle No. 6 and Supplemental Principle No. 8, both on 'Access', read together, provide that data subjects have a right to obtain from an organisation confirmation of whether or not the organisation is processing personal data related to him, to have communicated to them such data, and to subsequently have the data corrected, amended or deleted where it is inaccurate, or has been processed in violation of the Principles.[464] These Principles, however, also allow the restriction of the right to access in spite of the fact that EU law does not foresee this possibility.[465] First of all, the right to access can always be restricted where *"the burden or the expense of providing access would be disproportionate*

[456] Privacy Shield Decision, Privacy Principle No. 5.
[457] Ibid.
[458] Directive 95/46/EC, art 6(1)(b).
[459] Privacy Shield Decision, recital 22.
[460] Privacy Shield Decision, Privacy Principle No 5.
[461] Working Party WP238, 23.
[462] Privacy Shield Decision, Privacy Principle No. 5.
[463] Working Party WP238, 24.
[464] Privacy Shield Decision, Privacy Principle No. 6 and Supplemental Principle No. 8.
[465] Directive 95/46/EC, art 12.

to the risks to the individual's privacy in question".[466] Furthermore, while unjustly referring to the directive, it is stated that where personal information is processed solely for research or statistical purposes, access may be denied.[467] Finally, the Principles also provide an additional list of circumstances under which access may be denied or limited, which does not even require any balancing of rights.[468]

g. Lack of a data retention limitation principle

140. Even though the 'data retention limitation' principle is a fundamental principle in EU data protection law imposing that personal data can only be kept in a form which permits identification of data subjects for as long as this is necessary for the purposes for which the data were collected or for which they were further processed (see no. 44)[469], the Principles do not include such a principle.[470] This implies that certified organisations are not obliged to limit the period of retention of personal data whatsoever, which of course is clearly in breach of the EU requirements in this regard.[471] Both the EDPS and the Working Party made comments in this regard when making an assessment of the draft adequacy decision. However, it seems that they have not been taken into consideration.[472]

h. Automated individual decision

141. Contrary to EU law (see no. 55), the Principles also do not provide for any specific rules regarding automated decision-making. In this case as well, despite the fact that the European Data Protection Supervisor, the Article 29 Working Party and the European Parliament have expressed their concern in this regard, this omission has not yet been remedied.[473]

2. Procedural/enforcement mechanisms

142. In this subsection it will be examined to what extent the EU 'procedural/enforcement' requirements as identified by the Article 29 Working Party are reflected in the EU-U.S. Privacy Shield framework (b). Thereto, the procedural/enforcement mechanisms as set out in the adequacy decision will first be discussed (a).

---

[466] Privacy Shield Decision, Privacy Principle No. 6.
[467] Privacy Shield Decision, Supplemental Principle No. 8.
[468] Privacy Shield Decison, Supplemental Principle No. 8; Working Party 29 WP238, 26.
[469] Directive 95/46/EC, art 6(1)(e).
[470] Working Party 29 WP238, 17.
[471] EDPS Opinion on the EU-U.S. Privacy Shield draft adequacy decision, 7; Working Party 29 WP238, 17.
[472] Ibid.
[473] EDPS Opinion on the EU-U.S. Privacy Shield draft adequacy decision, 7; Working Party 29 WP238, 17-18; European Parliament Resolution 2016/3018(RSP), points H and 12.

i. Procedural/enforcement mechanisms

143. Adherence to the Privacy Shield principles can be enforced on initiative of the data subject itself or as a result of the monitoring activities the U.S. Department of Commerce has committed to.[474]

By virtue of Privacy Principle No. 7 on 'recourse, enforcement and liability' the certified organisations are required to provide recourse for individuals who are affected by non-compliance and more specifically enable EU data subjects to lodge complaints in that regard and to have these complaints resolved, if necessary by way of a decision providing an effective remedy.[475] Moreover, this Principle requires that there should be consequences for companies that fail to comply.[476] The Privacy Shield framework provides data subjects, in that regard, with a number of possibilities: first, EU data subjects may pursue cases of non-compliance through direct contacts with the U.S. self-certified company itself, which must respond *within 45 days*; second, individuals can bring a complaint directly to the independent dispute resolution body, either in the United States or in the Union, such as an Alternative Dispute Resolution (ADR) body or a national Data Protection Authority (DPA) (i.e. the supervisory authorities established by article 28 of Directive 95/46/EC)[477], designated by an organisation, which will investigate the complaint and expeditiously resolve it *at no cost* to the individual; third, complaints may also be brought to a DPA, when the organisation has voluntarily submitted to the oversight by DPAs, which in that case serves as the organisation's dispute resolution body, or, in the reverse case, in order to have the complaint referred to the Department of Commerce or the FTC, and in any event when it concerns the processing of human resources data collected in the context of an employment relationship; fourth, the Department of Commerce has committed, upon referral by a DPA, to receive, review and undertake *best efforts* to resolve complaints; fifth, a Privacy Shield organisation must be subject to the investigatory and enforcement powers of the U.S. authorities, in particular the FTC (or the U.S. Department of Transportation if the complaint relates to an airline or ticket agent)[478], which will *give priority consideration* to referrals of non-compliance with the Principles received from independent dispute resolution bodies, the Department of Commerce and DPAs in order to verify whether Section 5 of the FTC Act has been breached, and which will in addition *accept* complaints directly from individuals; sixth, as a 'last resort' recourse mechanism in case the organisation itself, the independent recourse mechanism or the Department of Commerce upon referral by a DPA[479] have not satisfactorily resolved an individual's complaint, an EU data subject may invoke binding arbitration by the 'Privacy Shield Panel', which has the authority to impose "'*individual-specific', non-monetary equitable relief"*, such as access, correction, deletion, or

[474] Privacy Shield Decision, recitals 30-63.
[475] Guide to the EU-U.S Privacy Shield, 12.
[476] Privacy Shield Decision, Privacy Principle No. 7.
[477] Guide to the EU-U.S. Privacy Shield, 12.
[478] Ibid.
[479] Privacy Shield Decision, Annex I.

return of the individual's data in question; seventh, additional judicial remedies may be available under the law of the U.S. States; and lastly, a DPA, upon receival of a complaint by an EU data subject, may still exercise its powers vis-à-vis the data exporter and even order the suspension of the data transfer, including when the EU data exporter has reason to believe that the organisation is not complying with the Principles.[480] Apart from the arbitral panel, which thus demands certain remedies to be exhausted before it can be invoked, individuals are free to pursue any or all of the redress mechanism of their choice, and do not have to choose one option over the other or to follow a certain sequence.[481] The order used above is merely the one that is advised in the Privacy Shield Decision.[482] Sanctions and remedies imposed by an independent dispute resolution body must be sufficiently rigorous to ensure compliance by organisations with the Principles and can consist of a reversal or correction by an organisation of the effects of non-compliance and, depending on the circumstances, the termination of the further processing of the personal data at stake and/or their deletion, as well as publicity for non-compliance.[483] In cases where the organisation fails to comply with the ruling of a dispute resolution body, the latter must notify such non-compliance to the Department of Commerce and the FTC, or to a competent court.[484] The FTC *can* enforce compliance through administrative orders.[485] Where organisations fail to comply, the FTC *may* refer the case to the competent court in order to seek civil penalties and other remedies, including for any injury caused by the unlawful conduct. The FTC *may* also directly seek a preliminary or permanent injunction or other remedies form a federal court.[486] The arbitration option is only available for 'remedying' purposes and not, for example, with respect to the exceptions to the Principles or with respect to an allegation about the adequacy of the Privacy Shield.[487] Judicial review and enforcement of the arbitral decisions is possible pursuant to U.S. law under the Federal Arbitration Act.[488]

The Department of Commerce has committed to *ex officio* monitor any false claims of Privacy Shield participation or the improper use of the Privacy Shield certification mark, and DPAs can refer organisations for review to a dedicated contact point.[489] Moreover, the Department will conduct *ex officio* compliance reviews of self-certified organisations.[490] It will also monitor organisations that are no longer members of the EU-U.S. Privacy Shield to verify whether they will return, delete or retain, in which case organisations are obliged to continue to apply the Principles to them, the personal data received

[480] Privacy Shield Decision, recitals 38-60 and Privacy Principle No. 7 and Supplemental Principle No. 7.
[481] Privacy Shield Decision, recital 41.
[482] Ibid.
[483] Privacy Shield Decision, recital 45.
[484] Privacy Shield Decision, recital 47.
[485] Privacy Shield Decision, recital 55.
[486] Ibid.
[487] Privacy Shield Decision, Supplemental Principle 11.
[488] Ibid.
[489] Privacy Shield Decision, recital 36.
[490] Privacy Shield Decision, recital 37.

previously under the framework.[491] The FTC will also undertake Privacy Shield investigations on its own initiative, and in particular as part of its wider investigations of privacy issues.[492]

144. It is also stated in the decision that the effective application of the Principles is further guaranteed by rules on transparency and commitments by the Department of Commerce as regards the administration of the Privacy Shield.[493] More specifically, the Department has undertaken to maintain and make available to the public a list of organisations that have self-certified their adherence to the Principles.[494] The list will be updated on the basis of an organisation's annual recertification submissions and whenever an organisation withdraws or, in case an organisation persistently fails to comply, is removed from the EU-U.S. Privacy Shield.[495] The Department will also keep a record of organisations that have been removed and of the reason thereof.[496]

145. Organisations must also have follow-up procedures in place for verifying that the attestations and assertions that they make about their privacy practices are true and are correctly implemented, and can opt for either self-assessment or for outside compliance review in that regard.[497]

j. Fulfilment of the EU requirements

146. Under the Safe Harbour scheme, EU data subjects were encouraged to first raise complaints with the relevant organisations themselves, companies had to provide a readily and *affordable* independent recourse mechanism, the FTC had committed to reviewing on a priority basis referrals received from the independent recourse mechanism and from EU Member States alleging non-compliance with the Safe Harbour Principles as to determine whether Section 5 of the FTC Act had been violated, and the Department of Commerce had a number of administrative and monitoring functions, which were however less extended than those it committed to under the Privacy Shield.[498] Accordingly, the Privacy Shield framework is definitely upgraded compared to its predecessor, though is in essence not fundamentally different.

147. However, due to the complexity and the lack of clarity of the overall architecture of the multi-layered mechanism, the effective exercise of data subject's rights might nevertheless, in practice, be

---

[491] Privacy Shield Decision, recital 34.
[492] Privacy Shield Decision, recital 54.
[493] Privacy Shield Decision, recital 62.
[494] Privacy Shield Decision, recital 31.
[495] Ibid.
[496] Ibid.
[497] Privacy Shield Decision, Privacy Principle No. 7 and Supplemental Principle No. 7.
[498] COM (2013) final 847, 3-4; Safe Harbour Decision, FAQ No. 11; Wilmer Hale, 'United States: Comparison of Requirements Under The Privacy Shield/Safe Harbor Principles' (Mondaq, 26 July 2016) <http://www.mondaq.com/unitedstates/x/513810/Data+Protection+Privacy/Comparison+Of+Requirements+Under+The+Privacy+ShieldSafe+Harbor+Principles> accessed 29 April 2017.

undermined.[499] Also, as the adequacy decision does not go into detail with regard to the possibilities for individuals to bring cases to U.S. Courts, it might be difficult for data subjects to actually pursue that option.[500] Moreover, the Commission did not follow the recommendation, made by the Article 29 Working Party in a letter of 10 April 2014 to former Justice Commissioner Viviane Reding, according to which individuals should be *"[en]able[d] to bring claims for damages in the European Union"* as well as should be *"granted the right to lodge a claim before a competent EU national court"* and should allow EU DPAs to represent the data subject, act on his behalf or act an intermediary in that regard.[501] Also the participating organisation might be discouraged by this wide array of avenues and potential fronts it has to respond to and instead may prefer to make use of SCCs or BCRs (see no. 27-30), which dispute resolution requirements seem to be less burdensome.[502]

148. Despite the fact that the U.S. Department of Commerce significantly expanded its oversight role, doubled the size of the program staff, has committed to dedicate the necessary resources in order to effectively fulfil its commitments and will undertake best efforts to facilitate resolution of complaints, and the Federal Trade Commission will give priority consideration to referred complaints and will even accept complaints directly from individuals, there is still no duty for the U.S. authorities to systematically monitor compliance with Privacy Shield Principles or to effectively deal with complaints.[503]

149. As regards the role of DPAs, it must however be noted that, as required by the CJEU in *Schrems* (see no. 94), the Privacy Shield Decision does not, contrary to the Safe Harbour Decision, limit the powers of the supervisory authorities.[504]

150. All in all, the Privacy Shield appears to pursue 'good compliance', provide sufficient 'support and help for individual data subjects' and guarantee 'appropriate redress'. However, if it appears from the first annual review in September 2017 that enforcement of the Principles is still problematic (see no. 125), the remarks in the proceeding paragraphs should be taken into account in view of remedying the situation.

---

[499] Working Party 29 WP238, 26; EDPS Opinion on the EU-U.S. Privacy Shield draft adequacy decision, 11.
[500] EDPS Opinion on the EU-U.S. Privacy Shield draft adequacy decision, 11.
[501] Working Party 29 WP238, 28.
[502] Sotirios Petrovas and Cynthia J. Rich, 'Privacy Shield vs. Safe Harbor: A Different Name for an Improved Agreement?' (Morrison Foerster, 3 March 2016) <https://www.mofo.com/resources/publications/privacy-shield-vs-safe-harbor-a-different-name-for-an-improved-agreement.html> accessed 29 April 2017 ['Sotirios Petrovas and Cynthia J. Rich, 'Privacy Shield vs. Safe Harbor: A Different Name for an Improved Agreement?'].
[503] Sotirios Petrovas and Cynthia J. Rich, 'Privacy Shield vs. Safe Harbor: A Different Name for an Improved Agreement?'; Working Party 29 WP238, 27; EDPS Opinion on the EU-U.S. Privacy Shield draft adequacy decision, 10.
[504] Privacy Shield Decision, art 3.

D. Adequacy assessment of the U.S. privacy and data protection policy in case of collection and further processing of personal data transferred under the EU-U.S. Privacy Shield by U.S. public authorities

151. The Privacy Shield Principles, as its predecessor[505], provides that adherence to the Principles may, *inter alia*, be limited *"to the extent necessary to meet national security, public interest, or law enforcement requirements"*.[506] The Court of Justice, in its *Schrems* judgment, noted that this means that self-certified companies are bound to disregard the substantive data protection principles without limitation where they conflict with such requirements and therefore prove incompatible with them (see no. 94).[507] On top of that, the Court, in that case, also stated that the Safe Harbour Decision did not contain any findings regarding the existence, in the United States, of rules adopted by the State intended to limit any interference in that regard.[508] After Snowden it was clear to everybody that such a general exception to the Principles had indeed let the U.S. authorities to completely undermine the privacy rights of EU data subjects.[509]

In its Privacy Shield adequacy decision, the Commission, however, alleges that:

> *"on the basis of the available information about the U.S. legal order, including the representations and commitments from the U.S. government, […] any interference by U.S. public authorities with the fundamental rights of the persons whose data are transferred from the Union to the United States under the Privacy Shield for national security, law enforcement or other public interest purposes, and the ensuing restrictions imposed on self-certified organisations with respect to their adherence to the Principles, will [now] be limited to what is strictly necessary to achieve the legitimate objective in question, and that there exists effective legal protection against such interference"*.[510]

Since the Snowden revelations mainly concerned the existence of mass surveillance programmes in the context of intelligence operations, and as the U.S. accordingly only adapted its legal framework in that regard as well as undertook to provide EU data subjects with an opportunity, via the 'Privacy Shield

---

[505] Safe Harbour Decision, Annex I, 1.
[506] Privacy Shield Decision, Annex II, 2.
[507] *Schrems*, para 86.
[508] *Schrems*, para 88.
[509] Glenn Greenwald and Ewen MacAskill, 'NSA Prism program taps in to user data of Apple, Google and others' *The Guardian* (7 June 2013) <https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data> accessed 1 May 2017; EU Co-Chairs of the Ad Hoc EU-US Working Group on Data Protection, 'Report on the Findings of the EU Co-Chairs of the Ad Hoc EU-U.S. Working Group on Data Protection' [2013] point 5 <http://ec.europa.eu/justice/data-protection/files/report-findings-of-the-ad-hoc-eu-us-working-group-on-data-protection.pdf> accessed 1 May 2015 ['Report of the EU Co-Chairs of the Ad Hoc EU-U.S. Working Group on Data Protection']; *Schrems*, paras 87 and 93-95.
[510] Privacy Shield Decision, recital 140.

Ombudsperson', to lodge individual complaints when they suspect they are or have been the subject of surveillance by U.S. intelligence services, the Commission, however, when assessing the adequacy of the U.S. data protection regime, mainly focused on the limitations upon U.S. authorities when they collect and further process personal data transferred under the EU-U.S. Privacy Shield for national security purposes as well as on the oversight and redress mechanisms in place that must ensure that those data are effectively protected against unlawful interferences and the risk against abuse in that regard.[511] Accordingly, the Privacy Shield adequacy decision does not *in extenso* elucidate the limitations and safeguards upon U.S. public authorities when they collect and further process such personal data for law enforcement and other public interest purposes.[512]

152. Bearing in mind the judgment of the Court of Justice in the *Schrems* case, the adequacy assessment of the U.S. privacy and data protection policy in case of collection and further processing of personal data transferred under the EU-U.S. Privacy Shield by U.S. public authorities, of course requires great scrutiny. As explained in Chapter 2, it is clear, after the Court's ruling in *Tele2 Sverige*, that the assessment of the 'strict necessity' of surveillance measures by or to the benefit of the government starts as soon as the personal data is collected or retained thereto. Both the CJEU and the ECtHR considered that the 'bulk' collection or retention of personal data is incompatible with respectively article 7 and 8 of the EU Charter and article 8 of the European Convention of Human Rights. Surveillance measures should moreover be authorised or, where the data are retained by the private sector instead of collected by the government, access to those data should be subjected to prior review by a judicial or an otherwise independent body. There should also be objective criteria for determining the length of the surveillance measures and rules concerning the storage and deletion of data. Lastly, there should be remedies available to the individual in case his or her fundamental rights have or might have been violated.

153. As a preliminary remark, it need be noted that the Commission, in its adequacy decision, refers to this aspect of the data protection framework in the United States as 'access and use of personal data transferred under the EU-U.S. Privacy Shield by U.S. authorities'.[513] This can be explained by the fact that there is a significance difference in interpretation of the concept of 'data acquisition', at least in the context of acquisition for security purposes, between the European Union and the United States.[514] For the EU, this concept is synonymous with the concept of 'data collection' and is a form of processing of

---

[511] Privacy Shield Decision, recitals 67 and 117; Office of the Press Secretary of the White House, 'FACT SHEET: Review of U.S. Signals Intelligence' (The White House – President Barack Obama, 17 January 2014) <https://obamawhitehouse.archives.gov/the-press-office/2014/01/17/fact-sheet-review-us-signals-intelligence> accessed 1 May 2017 ['Office of the Press Secretary of the White House, 'FACT SHEET: Review of U.S. Signals Intelligence''].
[512] Privacy Shield Decision, recitals 125-135.
[513] Privacy Shield Decision, recitals 64-135.
[514] Report on the Findings by the EU Co-Chairs of the Ad Hoc Working Group on Data Protection, point 3.

personal data (see nos. 8 and 72-73).[515] Any subsequent operation carried out on that data is considered 'further processing'.[516] In the United States, on the other hand, data is considered 'collected' only when data extracted in the context of SIGINT (see no. 155) have been filtered through the use of 'discriminants', and 'processed' only when those data are analysed by human intervention and not yet at the time of the initial acquisition of personal data.[517] Hence, in the U.S. data is only 'processed' where it would already be 'accessed' or 'used' at EU level. In any event, considering the clear manner in which the Court of Justice confirmed the EU approach in this regard in its recent case law (see no. 80), the fact that the European Commission seems to have neglected this explicit distinction and uses the words 'collection', 'access' and 'use' as if they are interchangeable is both confusing and suspicious.[518]

1. Limitations and safeguards regarding the collection and further processing of personal data in the interests of national security

154. As mentioned above, the Commission, given the context in which the Safe Harbour Decision has been invalidated, paid particular attention to the limitations and safeguards regarding the collection and further processing of personal data in the interests of national security (see no. 151). In this subsection it will accordingly be discussed to what extent the concerns in that regard have been resolved.

a. Strict necessity

155. As stated above (see no. 51), the United States, after Snowden, has, to some extent, adapted its legal framework on intelligence operations and, simultaneously, the surveillance programmes based thereon.[519] More in particular, the reforms relate to the U.S. signals intelligence (SIGINT) activities. SIGINT in essence consists of several types of intercepts. The term is frequently used to refer to the interception of communications between two parties (COMINT) and concerns the communication itself as well as data about the communications (metadata) (see no. 10).[520] The process of signals intelligence

---

[515] Directive 95/46/EC, art 2, (b); Report on the Findings by the EU Co-chairs of the Ad Hoc Working Group on Data Protection, point 3; *Digital Rights Ireland*, paras 33-35.
[516] Ibid.
[517] Report on the Findings by the EU Co-Chairs of the Ad Hoc Working Group on Data Protection, point 3.
[518] Gert Vermeulen, 'The Paper Shield', 7-8; National Research Council, Division on Engineering and Physical Sciences, Computer Science and Telecommunications Board, Committee on Responding to Section 5(d) of Presidential Policy Directive 28: The Feasibility of Software to Provide Alternatives to Bulk Signals Intelligence Collection, *Bulk Collection of Signals Intelligence: Technical Options* (National Academies Press 2015), s 2 ['National Research Council, *Bulk Collection of Signals Intelligence: Technical Options*'].
[519] Office of the Press Secretary of the White House, 'FACT SHEET: Review of U.S. Signals Intelligence; Privacy Shield Decision, Annex VI, 1.
[520] European Union Agency for Fundamental Rights, *Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU – Mapping Member States' legal frameworks* (Publications Office of the European Union 2015) 15 ['FRA, *Surveillance by the intelligence services: fundamental rights safeguards and remedies in the EU*']; Margaret Rouse, 'Definition COMINT (communications intelligence)' <http://whatis.techtarget.com/definition/COMINT-communications-intelligence> accessed 1 May 2017.

activities consists of taking in signals, extracting data therefrom about events, filtering those data according to one or more discriminants, the storing of the resulting data (in the U.S. data will be deemed collected only when it is stored for more than a few hours and not when it is merely extracted), analysing it by querying the store and finally disseminating the derived intelligence to other analysts and policy-makers.[521] When a discriminant is chosen to limit the collection to a set of targets determined, the collection is (again in the U.S.) considered to be 'targeted', and when a discriminant is chosen to collect a significant quantity of data that is not relevant to any current target at the time of the collection, the collection will be considered 'bulk'.[522] When queries on data collected in bulk are sufficiently tailored, very little of the stored data will ever be examined.[523] In that sense, those stores/databases can be considered as a huge 'black box' (see *mutatis mutandis* no. 200). In a more broad sense, however, SIGINT is the collective term covering both the means and the methods for the interception and analysis of radio, including satellite and cellular phone, and cable-borne communications, and has come to embrace almost any data stored on an electronic device.[524] Since surveillance programmes based on signals intelligence such as PRISM, which concerned the indiscriminate and large-scale collection of personal data from US internet and telecommunication service providers, and UPSTREAM, by virtue of which the U.S. was enabled to monitor data flows inside and outside the U.S. via the equally indiscriminate and large-scale collection of communications from fiber cables and infrastructure as data flows passed, also affected a significant number of individuals in the EU, especially considering the central position of US information and communications technology companies in the EU market, the said reforms are also of importance for EU data subjects.[525] The Safe Harbour Decision was invalidated in this context (see no. 90) and accordingly the current legal framework regarding U.S. signals intelligence activities must prove to be adequate in the light of the EU requirements in that regard.

156. On 17 January 2017, after the Snowden revelations and prior to the CJEU's judgment in Schrems, former U.S. President Obama gave a speech regarding various reforms to U.S. signals intelligence activities and issued President Policy Directive 28 (PPD-28), which sets out a number of principles and limitations relating to such activities, on whatever basis they may be authorised, and for all people,

---

[521] 'National Research Council, *Bulk Collection of Signals Intelligence: Technical Options*', s 2.
[522] Ibid.
[523] Ibid.
[524] FRA, *Surveillance by the intelligence services: fundamental rights safeguards and remedies in the EU* 15.
[525] Report on the Findings by the EU Co-Chairs of the Ad Hoc Working Group on Data Protection, point 1; Glenn Greenwald and Ewen MacAskill, 'NSA Prism program taps in to user data of Apple, Google and others' *The Guardian* (7 June 2013) <https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data> accessed 1 May 2017; James Ball, 'NSA's Prism surveillance program: how it works and what it can do' *The Guardian* (8 June 2013) <https://www.theguardian.com/world/2013/jun/08/nsa-prism-server-collection-facebook-google> accessed 1 May 2017; James Ball, 'Edward Snowden NSA files: secret surveillance and our revelations so far' *The Guardian* (21 August 2013) <https://www.theguardian.com/world/2013/aug/21/edward-snowden-nsa-files-revelations> accessed 1 May 2017; Privacy Shield Decision, recital 81.

regardless of nationality and location.[526] The latter observation is of significant importance as U.S. law often, including in the context of intelligence operations, distinguishes between U.S. citizens (and residents) and non-U.S. persons.[527]

157. PPD-28 states, and this is, seemingly as a preliminary remark, pointed out by the Commission, that signals intelligence may be *collected* exclusively where there is a foreign intelligence or counterintelligence purpose to support national and departmental missions, and not for any other purpose, such as to afford a competitive damage to U.S. companies.[528] This however does not contribute to narrowing down the general 'national security' exception and is thus an absolute minimum in that regard.[529]

Further, the European Commission takes the view that the principles and limitations set out in PPD-28, although not phrased in those legal terms, capture the essence of the principles of 'proportionality' and 'necessity' as interpreted by the Court of Justice.[530] The Commission, in the Privacy Shield adequacy decision, argues that, by virtue of PPD-28, *"targeted collection is clearly prioritised, while bulk collection is limited to (exceptional) situations where targeted collection is not possible for technical and operational reasons"*.[531] As regard the prioritising of targeted collection, it is more specifically stipulated in section 1 of PPD-28 on 'Principles Governing the Collection of Signals Intelligence' that signals intelligence activities shall be *"as tailored as feasible"* and that *"in determining whether to collect signals intelligence, the United States shall consider the availability of other information [...].[A]ppropriate and feasible alternatives to signals intelligence should be prioritized"*.[532] According to U.S. General Counsel Robert Litt of the Office of the Director of National Intelligence (ODNI), this means that *"whenever practicable, signals intelligence collection activities are conducted in a targeted manner rather than in bulk"* and this through focusing the collection *"on specific foreign intelligence targets or topics through the use of discriminants (e.g. specific facilities, selection terms and identifiers)"*.[533] Section 5(d) of PPD-28 required in that regard that the Director of National Intelligence (DNI) had to provide the President, within 1 year of the date of the directive, with a report *"assessing the feasibility of creating software that would allow the IC more easily to conduct targeted information acquisition rather than bulk collection"*. In this report, however, it concluded that privacy concerns about SIGINT data

---

[526] Privacy Shield Decision, Annex VI, 1; Office of the Press Secretary of the White House, 'FACT SHEET: Review of U.S. Signals Intelligence'.
[527] Report on the Findings by the EU Co-Chairs of the Ad Hoc Working Group on Data Protection, point 2; Cindy Cohn, 'Empty Promises on Privacy for Foreigners Abroad in PPD-28' (Electronic Frontier Foundation, 26 October 2016) <https://www.eff.org/nl/deeplinks/2016/10/empty-promises-privacy-foreigners-abroad> accessed 2 May 2017; Working Party 29 WP238, 37.
[528] Privacy Shield Decision, recital 70; The White House, Presidential Policy Directive 28: Signals Intelligence Activities (PPD-28) (Jan. 17, 2014), s 1(c) ['PPD-28'].
[529] Gert Vermeulen, 'The Paper Shield', 8.
[530] Privacy Shield Decision, recitals 69 and 76.
[531] Privacy Shield Decision, recital 76.
[532] PPD-28, s 1(d); Privacy Shield Decision, recital 71.
[533] Privacy Shield Decision, recitals 70-71 and Annex VI, 3.

will not be addressed by replacing bulk collection with targeted collection.[534] More in particular, it is argued in this report that there is no software technique that will fully substitute for bulk collection where it is relied on to answer queries about the past after new targets become unknown (where in Europe this reasoning would clearly be a problem, see no. 112), but that, in some circumstances, other sources of information might, however, provide a partial substitute for bulk collection.[535] It thus appears that targeted collection via the use of discriminants, is not very feasible and that accordingly, contrary to what the ODNI has stated, the exception for bulk collection might swallow the rule.[536] The examples of the discriminants are moreover extremely vague and cannot even be properly assessed in the light of the EU requirements on proportionality and necessity, and accordingly certainly do not guarantee their compliance in that regard.[537] The fact that those 'selectors' will be decided on by high-level policy makers and not will thus not left to the discretion of individual intelligence agents, is not sufficiently reassuring either.[538]

On top of that, PPD-28, in section 2, expressly provides that the United States must, due to technical or operational considerations, in certain circumstances collect signals intelligence in bulk in order to identify 'new or emerging threats' and 'other vital national security information'.[539] This means that PPD-28 thus already presumes that targeted collection most likely will not be considered feasible in those cases. The fact that bulk collection regarding internet communications performed by the U.S. Intelligence Community through SIGINT concern only a small proportion of the global internet, can also not be considered as valid argument to prove the 'strict necessity' of the data collection activities in the context of signals intelligence.[540] The Commission stresses, however, that even then the U.S. authorities will seek to narrow the collection 'as much as possible'.[541]

158. Furthermore, PPD-28 specifies that when signals intelligence is collected in bulk, the gathered data can only be *used* for purposes of detecting and countering: (1) espionage and other threats and activities directed by foreign powers or their intelligence services against the United States and its interests; (2) threats to the United States and its interests from terrorism; (3) threats to the United States and its interests from the development, possession, proliferation, or use of weapons of mass destruction; (4) cybersecurity threats; (5) threats to U.S. or allied Armed Forces or other U.S or allied personnel; and (6) transnational criminal threats, including illicit finance and sanctions evasion related to the other purposes

[534] National Research Council, *Bulk Collection of Signals Intelligence: Technical Options*, 6-9.
[535] National Research Council, *Bulk Collection of Signals Intelligence: Technical Options*, 4-5.
[536] Privacy Shield Decision, Annex VI, 3.
[537] Gert Vermeulen, 'The Paper Shield', 8.
[538] Ibid.
[539] Privacy Shield Decision, recital 72 and Annex VI, 3.
[540] Privacy Shield Decision, Annex VI, 3; Gert Vermeulen, 'The Paper Shield', 8
[541] Privacy Shield Decision, recital 73.

named in this section.[542] Even though the Commission and the ODNI present those purposes as being 'specific', they (again) clearly are not.[543]

The fact that analysts must structure the queries or other terms and techniques they use to search the store (see no. 155) in such a way that they are appropriate to identify intelligence information that is relevant to a valid foreign intelligence task, does not change the fact that the U.S. framework is by definition inadequate as the limitations in the phase of collection are not sufficient.

159. Lastly, as regards the length of the storage of the collected data, it is specified in PPD-28 that the retention period is generally limited to a maximum of five years, unless the DNI expressly determines that continued retention is in the national security interests of the United States, and that non-U.S. persons will be treated in the same way as U.S. persons.[544] Bearing in mind the case law of the Court of Justice in *Digitial Rights Ireland* case (see no. 80), in which the Court, with regard to retention period of maximum 24 months, stated that there should be made a distinction between the categories of data in this respect and that there should be an objective criteria justifying the length of the retention, also in this regard the U.S. does not meet the 'strict necessity' requirement.[545] The fact that the U.S. concept of 'reasonableness', as a bedrock principle of U.S. law, requires that Intelligence Community elements, although they will not be required to adopt any measures theoretically possible, will nevertheless have to *"balance their efforts to protect legitimate privacy and civil liberties interests with the practical necessities of signals intelligence"*, cannot remedy this situation.

160. The main legal bases that may be used in the U.S. to collect (and subsequently process) personal data of EU data subject transferred under the EU-U.S. Privacy Shield via signals intelligence operations are the following: (1) Executive Order 12333, which lays down the general framework on intelligence gathering inside and outside the U.S. and serves as the basis for surveillance programmes, the scope of which is at the discretion of the President[546]; (2) Section 501 of FISA (Foreign Intelligence Surveillance Act) (formerly: Section 2015 of the U.S. Patriot Act), which allows the collection of any 'tangible' things (such as books, records, papers, documents and other items) for an investigation to protect against international terrorism or clandestine activities, and which formed the legal basis for the intelligence programme that enabled U.S. intelligence services to collect the telephone records of millions US customers of Verizon[547]; (3) Section 702 of FISA, which permits the *"targeting of [non-U.S.] persons*

---

[542] PPD-28, s 2.
[543] Privacy Shield Decision, recital 74 and Annex VI, 3; Gert Vermeulen, 'The Paper Shield', 8; Working Party 29 WP238, 28.
[544] PPD-28, s 4(a)(i); Privacy Shield Decision, recitals 85-86 and Annex VI, 5.
[545] European Parliament Resolution 2016/3018(RSP), 17.
[546] Privacy Shield Decision, recital 68; Daniel Severson, 'American Surveillance of Non-U.S. Persons: Why New Privacy Protections Offer Only Cosmetic Change' (2015) 56 Harvard International Law Journal 465, 499.
[547] Foreign Intelligence Serivce Act 1978 (United States), s 501; Report on the Findings by the EU Co-Chairs of the Ad Hoc Working Group on Data Protection, point 2.2; Glenn Greenwald, 'NSA collecting phone records of

reasonably believed to be located outside of the United States to acquire foreign intelligence information" and this with the compelled assistance of U.S. electronic communications service providers, and which provides the basis for the aforementioned intelligence programmes PRIMS and UPSTEAM[548].[549]

As regards section 501 FISA, it must be noted that the USA FREEDOM Act of June 2015, apart from PPD-28, also aims at prohibiting the bulk collection of personal data, and more specifically of 'records', on that legal basis, and instead requires, again, the use of 'selection terms'.[550] As stipulated above, this legal basis permitted the U.S. authorities to collect the telephone records of millions US customers of Verizon (see no. 155). The disclosure of this 'phone records' programme has undoubtedly attracted the most attention in the United States.[551] Accordingly, the U.S. Congress passed the USA FREEDOM Act in June 2015 and ordered the halt of the programme in November of the same year.[552] However, as noted by the U.S. Center for Constitutional Rights, U.S. intelligence services might have other ways to grab these records from private companies, such phone companies, your bank or Google and this by way of a subpoena (see no. 170-172) , especially in the form of 'National Security Letters'.[553] The changes in the law in this regard also do not prevent the American government from collecting personal data of individuals in bulk.[554]

As regards section 702 FISA, the ODNI argues that this legal authority, it itself and thus irrespective of the limitations set out in PPD-28, restricts interference by public authorities to targeted collection access.[555] More specifically, it points at the fact that Section 702 authorises the Attorney General and the DNI to submit annual certifications identifying specific categories of foreign intelligence, such as intelligence related to counterterrorism or weapons of mass destruction, to be collected, to the FISA Court

---

millions of Verizon customers daily' *The Guardian* (6 June 2013) <https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order> accessed 2 May 2017.

[548] Foreign Intelligence Service Act 1978 (United States), s 702; Report on the Findings by the EU Co-Chairs of the Ad Hoc Working Group on Data Protection, point 2.1.1; Privacy Shield Decision, 81 and Annex VI, 8.

[549] Bruce Schneier, *Data and Goliath – The Hidden Battles to Collect Your Data and Control Your World* (W. W. Norton & Company Ltd, first edition 2015) 65-66; Office of the Press Secretary of the White House, 'FACT SHEET: Review of U.S. Signals Intelligence.

[550] Privacy Shield Decision, recital 79.

[551] Shayana Kadial, 'Surveillance After the USA Freedom Act: How Much Has Changed?' (The Center for Constitutional Rights, 17 December 2015) <http://www.huffingtonpost.com/the-center-for-constitutional-rights/surveillance-after-the-us_b_8827952.html> accessed 2 May 2017 ['Shayana Kadial, 'Surveillance After the USA Freedom Act: How Much Has Changed?'].

[552] Ellen Nakashima, 'NSA's bulk collection of Americans' phone records ends Sunday' *The Washington Post* (27 November 2015) <https://www.washingtonpost.com/world/national-security/nsas-bulk-collection-of-americans-phone-records-ends-sunday/2015/11/27/75dc62e2-9546-11e5-a2d6-f57908580b1f_story.html?utm_term=.1290ae49daa5> accessed 13 May 2017.

[553] Shayana Kadial, 'Surveillance After the USA Freedom Act: How Much Has Changed?'.

[554] Ibid.

[555] Privacy Shield Decision, recital 80.

(FISC).[556] That way, it is reasoned, the unrestricted collection of information about foreigners is not permitted.[557] Those certifications must also provide 'targeting' and 'minimisation' procedures in order to limit the acquisition, dissemination, and retention of data incidentally acquired about U.S persons.[558] The U.S. stresses that non-U.S. persons may also indirectly benefit from those procedures, however, it must be noted that those benefits are not legally binding or statutorily established since Section 702 itself does not provide for procedures that specifically aim at reducing the incidental collection and further processing of personal data of non-U.S. persons.[559] Similarly, the fact that, according to the U.S., in 2014 only 90000 individuals out of 3 billion internet users have been targeted and that the data is stored in databases with strict access control, does not, in any way, demonstrate the strict necessity of the collection in the light of the EU requirements.[560]

161. In sum, it is clear that bulk collection of personal data is still possible under U.S. law, that it is moreover by no means clear if there are objective criteria set out by which to determine the limits of the subsequent access by the authorities to the collected data and that the length of the period of retention also cannot be justified. The interferences by the government can thus not be considered 'strictly necessary'. Accordingly, it is does not appear from the Privacy Shield adequacy decision that the U.S., as required by the CJEU in *Schrems*, ensures an adequate level of data protection when U.S. authorities collect and further process personal data transferred from the Union to the United States under the EU-U.S. Privacy Shield in the interests of national security.

b. Oversight

162. The conduct of the U.S. intelligence services is subject to a multi-layered oversight process that involves the three branches of the State.[561] More specifically, there are internal and external bodies within the executive branch, a number of Congressional Committees and a judicial supervision by the aforementioned FISC related to FISA activities.[562]

163. Before evaluating the adequacy of the actual supervision process, it must be noted, bearing in mind the findings in a., that it is hard to see how all the bodies involved in it would be able to keep the interference of the authorities to what is 'strictly necessary' considering that the national provisions, which constitute the basis for their assessment, do not themselves meet this requirement.

---

[556] Privacy Shield Decision, Annex VI, 8.
[557] Ibid.
[558] Ibid.
[559] Report on the Findings by the EU Co-Chairs of the Ad Hoc Working Group on Data Protection, point 2.1.2; Working Party 29 WP238, 39.
[560] Privacy Shield Decision, Annex VI, 9.
[561] Privacy Shield Decision, recital 92; Working Party 29 WP238, 40.
[562] Privacy Shield Decision, recital 92.

164. With regard to the internal oversight mechanisms, which of course are a part of the executive, the Article 29 Working Party has pointed that, overall, those can be considered as 'fairly robust'.[563] However, the Working Party also considered that the 'civil liberties and privacy officers', which exist at various departments with intelligence responsibilities, do not meet the by the CJEU and ECtHR required level of independence.[564] The Inspectors-General, whose primary task is to assess compliance of the activities of the agencies with the legislation, in their opinion does. However, they can only issue non-binding recommendations for corrective action.[565]

165. As regards the external supervision mechanisms, the Commission pointed out that the Privacy and Civil Liberties Oversight Board (PCLOB) is an independent agency within the executive branch, which is composed of a bipartisan, five-member Board, and based itself on the assessment of the Working Party in that regard. According to the latter, the PCLOB has in the past demonstrated its independence.[566] It has both an oversight and an advisory role: in the context of the former, it has the competence to review and analyse actions the executive branch takes to protect the U.S. from terrorism, ensuring that the need for such actions is balanced with the need to protect privacy and civil liberties; with regard to the latter, it is authorised to review proposed legislation, regulations, and policies related to efforts to protect the nation from terrorism in order to ensures that that liberty concerns are appropriately considered by the President and the executive branch agencies.[567] It must be noted, however, that its mandate is thus restricted to activities of the Intelligence Community in the field of counterterrorism.[568] Its oversight is performed after the fact and it also has no enforcement power.[569] It can go to court like anyone else, however, it cannot oblige or order any government agency to change its practices or otherwise enforce the law.[570] What is really, on the other hand, alarming is that the PCLOB has lost its quorum on 7 January 2017.[571] With just one part-time board member left, after the rest have rotated off or resigned, the board is now largely unable to take action.[572] Indeed, without the statutory

---

[563] Working Party 29 WP238, 41.
[564] Working Party 29 WP238, 41; Privacy Shield Decision, recital 96.
[565] Privacy Shield Decision, recital 97; Working Party 29 WP238, 40.
[566] Privacy Shield Decision, recital 95; Working Party 29 WP238, 42.
[567] Working Party 29 WP238, 42; Website Privacy and Civil Liberties Oversight Board, 'About the Board' <https://www.pclob.gov/about-us.html> accessed 3 May 2017.
[568] Jan Stanley, 'What Powers Does the Civil Liberties Oversight Board Have?' (American Civil Liberties Union, 4 November 2013) <https://www.aclu.org/blog/what-powers-does-civil-liberties-oversight-board-have> accessed 3 May 2017 ['Jan Stanley, 'What Powers Does the Civil Liberties Oversight Board Have?'']; Privacy Shield Decision, 98.
[569] Working Party 29 WP238, 42; Jan Stanley, 'What Powers Does the Civil Liberties Oversight Board Have?'.
[570] Ibid.
[571] European Parliament Resolution 2016/3018(RSP), point 18.
[572] Tim Johnson, 'Watchdog board that keeps eye on U.S. intelligence agencies barely functions' (McClatchy DC BUREAU, 7 March 2017) <http://www.mcclatchydc.com/news/nation-world/national/national-security/article136960048.html> accessed 3 May 2017; Website Privacy and Civil Liberties Oversight Board, 'Board Member Biographies' <https://www.pclob.gov/about-us.html> accessed 3 May 2017.

quorum of three members, it cannot initiate new oversight or advice projects nor offer advice to the intelligence community.[573] Up until the moment new Board Members are nominated by President Trump and confirmed by the U.S. Senate, this situation will remain unchanged.[574]

As the European Court of Human Rights, in *Szabó and Vissy v. Hungary*, made clear that it was not satisfied with supervision mechanisms within the executive branch (see no. 108), the other external mechanisms should also be assessed. In that regard it must be noted that in addition to oversight mechanism within the executive branch, the House and Senate Intelligence and Judiciary Committee of the U.S. Congress also have supervision competences as regards all U.S. foreign intelligence activities, including SIGINT.[575] It is, however, not clear to what extent they can debate and discuss the processing of personal data of individual persons.[576] Lastly, intelligence activities based on FISA allow for review, and in some cases prior authorisation, by the FISC.[577] In order to ensure that privacy considerations are properly reflected in the Court's assessment, the Court is, since the enactment of the USA FREEDOM Act, supported by amicus curiae.[578] Under Section 501 FISA, the application for an *ex ante* order from the FISC must contain a statement of facts that must demonstrate there are reasonable grounds to believe that the 'tangible' things sought are *relevant* to an authorised investigation conducted to obtain foreign intelligence information not concerning a U.S person or to protect against international terrorism or clandestine intelligence activities.[579] The term relevant is understood broadly: information that might not be relevant at the time of acquisition might prove to be so at a later point in time.[580] Also, not every piece of information needs to be relevant to the investigation, but rather the database in its entirety.[581] Under Section 702, the FISC also does not authorise individual surveillance measures, but instead authorises surveillance programmes on the basis of annual certifications (see no. 160).[582] The certifications thus rather identify categories of foreign intelligence information and do not contain information about the individual person to be targeted.[583] It must be noted that no judicial oversight or review mechanisms are provided when surveillance is conducted on the basis of Executive Order 12333.[584] It is thus clear

[573] Jenna McLaughlin, 'The U.S. Government's Privacy Watchdog Is Basically Dead, Emails Reveal' (The Intercept, 3 March 2017) <https://theintercept.com/2017/03/03/the-governments-privacy-watchdog-is-basically-dead-emails-reveal/> accessed 3 May 2017.
[574] European Parliament Resolution, 2016/3018(RSP), 18.
[575] Privacy Shield Decision, recital 102.
[576] Working Party 29 WP238, 42.
[577] Privacy Shield Decision, recital 105.
[578] Privacy Shield Decision, recital 106; Working Party 29 WP238, 41.
[579] Privacy Shield Decision, recital 108; Working Party 29 WP238, 41.
[580] Report on the Findings by the EU Co-Chairs of the Ad Hoc Working Group on Data Protection, point 3.2.1.
[581] Ibid.
[582] Privacy Shield Decision, recital 109.
[583] Ibid.
[584] Working Party 29 WP238, 42.

that the FISC does not provide effective judicial oversight, as required by the CJEU and especially the ECtHR, on targeting of non-U.S. persons.[585]

166. In conclusion, the Privacy Shield adequacy decision also does not provide sufficient oversight mechanisms in order to be considered adequate in the light of the European standards in that respect.

c. Redress: Privacy Shield Ombudsperson

167. In the *Schrems* case, the Court of Justice of the European Union found that the legislation in the United States did not respect the essence of the fundamental right to effective judicial protection, as embodied in article 47 of the EU Charter on Fundamental Rights, as it did not provide for any possibility for an individual to pursue legal remedies in order to have access to personal data relating to him, or to obtain the rectification or erasure of such data in case of the acquisition and further processing thereof by the U.S. authorities (see no. 94). The right to judicial protection should be understood as a remedy before a 'court'. In the context of the European Convention of Human Rights it suffices to have an effective remedy before a 'national authority'.

168. Accordingly, the United States decided to create the Privacy Shield Ombudsperson mechanism.[586] The functions of the Privacy Shield Ombudsperson are carried out by the Under-Secretary of the U.S. Department of State, which, assisted by a number of staff, has to investigate and address complaints in a timely manner, and has to ensure that the plaintiff receives confirmation that the concerned U.S. law has been complied with or in the reverse case, that the situation has been remedied.[587] To that end, the Ombudsperson will be able to rely, *inter alia*, on independent oversight bodies with investigatory powers (such as the aforementioned Inspectors-General and the PCLOB).[588] The individual data subject can lodge a complaint with their national supervisory authorities which will pass it on to a centralised EU body wherefrom it will be sent to the Ombudsperson.[589] Individuals do not have to prove that their personal data in fact has been processed by the U.S. authorities.[590]

The U.S., and thus also the Commission, stress that this mechanism is independent *"and thus free from instructions by the U.S. Intelligence Community"*.[591] The latter statement is of course the very least that can be expected from a body addressing complaints about the conduct of that community, and, in any event does not suffice. Moreover, it is very questionable whether the Ombudsperson is created within the most suitable department, as this department is clearly not impartial in terms of national security,

---

[585] Ibid.
[586] Privacy Shield Decision, recital 116-117.
[587] Guide to the EU-U.S. Privacy Shield, 19; Privacy Shield Decision, recital 117.
[588] Ibid.
[589] Privacy Shield Decision, recital 119.
[590] Ibid.
[591] Privacy Shield Decision, recital 121.

whether it is sufficiently independent from that department itself and whether criteria for dismissal of the Ombudsperson are the same is for the dismissal of an Under Secretary.[592] Despite the fact that the U.S. has, during the negotiations with regard the Privacy Shield, indicated that the Ombudsperson will objectively perform its task and will not be influenced in an intolerable manner, the existence of corresponding obligations in that regard is nowhere formally confirmed in the Privacy Shield.[593] Again, it is rather obvious that the European requirements have not been met. Moreover, and as has been noted with regard to the oversight mechanisms, the Ombudsperson, even if it would be considered sufficiently independent, can merely make an assessment of compliance with rules that are in itself unsatisfactory.

2. Limitations and safeguards regarding the collection and further processing of personal data for law enforcement and public interest purposes

169. As mentioned above (see no. 151), the Privacy Shield adequacy decision does not *in extenso* elucidate the limitations and safeguards incumbent upon U.S. public authorities when they collect and further process personal data transferred under the EU-U.S. Privacy Shield for law enforcement and other public interest purposes.

170. As regards the processing by the U.S. authorities for law enforcement purposes, the Commission, strangely enough, starts its argumentation by pointing at the Fourth Amendment of the U.S. Constitution, of which the application does not extend to non-U.S. persons that are not resident in the United.[594] In particular, this Amendment provides that *"the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized"*.[595] This thus means that searches and seizures by law enforcement authorities principally require a court-ordered warrant upon demonstration of a 'probable cause' and that in the allegedly *"few specifically established and exceptional cases where the warrant requirement does not apply"*, law enforcement is subjected to the abovementioned 'reasonableness' test (see no. 159).[596] The Commission argues that these concepts correspond with the idea of

---

[592] European Ombudsman (Emily O'Reilly), 'Use of the title 'ombudsman' in the 'EU-US Privacy Shield' agreement' (European Ombudsman, Letter to Ms Věra Jourová, 22 February 2016) <https://www.ombudsman.europa.eu/resources/otherdocument.faces/en/64157/html.bookmark> accessed 3 May 2017; Working Party 29 WP238, 49; EDPS Opinion on the EU-U.S. Privacy Shield draft adequacy decision; European Parliament Resolution 2016/2727 (RSP), point 8; European Parliament Resolution 2016/3018(RSP), point 27; Gert Vermeulen, 'The Paper Shield', 11.

[593] 'The Article 29 Data Protection Working Party ("WP29") remain concerned about the recently adopted Privacy Shield as follows from their recent statement dated 1 July 2016" (Stibbe, 13 October 2016) <https://www.stibbe.com/en/news/2016/october/privacy-authorities-remain-concerned-about-the-privacy-shield> accessed 3 May 2017.

[594] Privacy Shield Decision, recital 126-127.

[595] Privacy Shield Decision, Annex VII, 1; "The Constitution of the United States", Amendment 4.

[596] Privacy Shield Decision, recital 126.

'necessity' and 'proportionality' in the EU.[597] Going back to the relevance of the Fourth Amendment: EU data subjects would directly benefit from its protection given the fact that their data is held by U.S. companies whereto the Amendment does apply.[598] Moreover, further protections are supposedly laid down by special statutory authorities.

A warrant is, *inter alia*, not required is in cases where federal statutes authorise the use of 'administrative subpoenas'. Administrative subpoena authority is the power conferred, by statute, upon numerous administrative agencies to oblige for example a Privacy Shield company (a 'third party') to produce documents or to provide testimony.[599] Administrative subpoenas are usually for acquiring data for administrative reasons, however, might also reveal evidence that could serve the purpose of criminal prosecution.[600] Accordingly, several federal statutes have authorised the use of administrative subpoenas in the criminal law enforcement context to produce or make available business records, electronically stored information, or other tangible items in investigations involving health care fraud, child abuse, Secret Service protection, controlled substance cases, and Inspector General investigations implicating government agencies.[601] The 'reasonableness', because the recipient considers the subpoena to be overbroad, oppressive or burdensome, of a subpoena can only be challenged when the government seeks to enforce the subpoena in court.[602] It is, however, not a secret that such subpoenas make it possible to gather data in bulk.[603] Bearing in mind the SWIFT-affaire, the EU should nonetheless be aware of this (see no. 198).[604] Hence, it is needless to say that the Privacy Shield, as this issue has not even been addressed in it, can also in this regard not be considered adequate.

---

[597] Ibid.
[598] Privacy Shield Decision, recital 127.
[599] Privacy Shield Decision, Annex VII, 2; Els De Busser, *Data Protection in EU and US Criminal Cooperation – A Substantive Law Approach to the EU Internal and Transatlantic Cooperation in Criminal Matters between Judicial and Law Enforcement Authorities* (Maklu 2009), 272 ['Els De Busser, *Data Protection in EU and US Criminal Cooperation*']; Charles Doyle, 'Administrative Subpoenas in Criminal Investigations: A Brief Legal Analysis' (CRS Report for Congress, 17 March 2006), summary <https://fas.org/sgp/crs/intel/RL33321.pdf> accessed 4 May 2017 ['Charles Doyle, 'Administrative Subpoenas in Criminal Investigations: A Brief Legal Analysis'].
[600] Els De Busser, *Data Protection in EU and US Criminal Cooperation*, 273.
[601] Privacy Shield Decision, Annex VII, 2.
[602] Privacy Shield Decision, Annex VII, 2; Els De Busser, *Data Protection in EU and US Criminal Cooperation*, 272.
[603] Shayana Kadial, 'Surveillance After the USA Freedom Act: How Much Has Changed?'.
[604] Directorate-General for Internal Policies – Policy Department C: Citizens's Rights and Constitutional Rights (European Parliament), 'The US legal system on data protection in the field of law enforcement – Safeguards, rights and remedies for EU citizens' [2015] Study, 17 <http://www.europarl.europa.eu/RegData/etudes/STUD/2015/519215/IPOL_STU%282015%29519215_EN.pdf> accessed 4 May 2016 ['Directorate-General for Internal Policies – Policy Department C, The US legal system on data protection in the field of law enforcement'].

171. Administrative subpoenas can also be used for public interest purposes.[605] In a letter from the U.S. Department of Justice, annexed to the Privacy Shield, it is stipulated that agencies with civil and regulator (i.e., 'public interest') responsibilities may issue subpoenas to corporations for business records, electronically stored information, or other tangible things.[606] Here too, the various agencies that hold subpoena authority are specified in a number of statutes and are subjected to the 'reasonableness' test.[607] What is exactly is meant by 'public interest' is, however, nowhere specified in the Privacy Shield. The only limitations concerning the use of this power relate, again, to the 'reasonableness' of the subpoena and the requirement of 'relevance' of the data that has to be provided.[608]

172. Other than the fact that administrative subpoenas can be challenged in court when the governments seeks to enforce them, there seems to be no other way to supervise the use thereof. As regards the condition of 'reasonableness', the Fourth Amendment only requires that the subpoena (1) satisfies the terms of the authorising statute, (2) requests documents that are *relevant* to the investigation, (3) seeks information that is not already in the government's possession, and (4) will not constitute an abuse of the court's process when it is enforced.[609] Note moreover that only the recipient can challenge the subpoena and not the person whose data has been requested. There are, however, a number of other judicial redress avenues for individuals where a public authority or one of its officials process their personal data. In particular, these avenues include (1) the Administrative Procedure Act, (2) the Freedom of Information Act, and (3) the Electronic Communications Privacy Act, which are open to all individuals regardless of nationality.[610] As these remedies did not seem to suffice in the context of processing of data by the government for national security reasons (as the Privacy Shield Ombudsperson mechanism has been established in that context), it is very questionable whether these do suffice in the context processing of law enforcement or public interest purpose.

173. In the light of the above, it appears that the Commission, in the Privacy Shield adequacy decision, did not demonstrate that the United States in this context in fact ensures an adequate level of protection by reason of its domestic law or its international commitments.[611]

---

[605] Privacy Shield Decision, recital 129.
[606] Privacy Shield Decision, Annex VII, 3.
[607] Privacy Shield Decision, recital 129; Els De Busser, *Data Protection in EU and US Criminal Cooperation*, 272-273.
[608] Privacy Shield Decision, Annex VII, 3.
[609] Charles Doyle, 'Administrative Subpoenas in Criminal Investigations: A Brief Legal Analysis', summary.
[610] Privacy Shield Decision, recital 130.
[611] *Schrems*, para 97.

3. Lack of purpose limitation

174. A last point of concern regarding the gathering of personal data by government authorities relates to the fact that the United States generally lacks a requirement of purpose limitation as regards the processing of personal data for government purposes.[612]

175. As the scope of Directive 95/46/EC does not extend to processing operations concerning public security, defence, State security (including the economic well-being of the State when the processing operation relates to State security matter) and the activities of the State in areas of criminal law (see no. 14) the purpose limitation as laid down in this directive cannot apply to the EU Member States' governments to that extent. However, this requirement is nevertheless incumbent on them by virtue of Convention 108 (see no. 37), which applies to both the private and the public sector for all purposes.[613] Derogations to this principle are only allowed *"when such derogation is provided for by the law of the Party and constitutes a necessary measures in a democratic society in the interests of: (a) protecting State security, public safety, the monetary interests of the State or the suppression of criminal offences; (b) protecting the data subject or the rights and freedoms of others".*[614]

176. In the United States, however, this issue is addressed in a different manner.[615] The Privacy Act of 1974, which applies, *inter alia*, to *"any Executive department"*, stipulates, as the basis rule in that regard, that *"[n]o agency shall disclose any record which is contained in a system of records by any means or communication to […] another agency, except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains [subject to 12 exceptions]"*.[616] One of these exceptions concerns 'routine uses' of records, which means that a records may be used for a purpose *"which is compatible with the purpose for which it was collected"*.[617] Convention 108 also provides that stored data may not be used in a way incompatible with those purposes, however, in the United States this condition is interpreted in a broader sense.[618] In Europe, a compatible use is a use that is both similar and foreseeable.[619] In the U.S., the notion of compatibility encompasses 'functionally equivalent use' (comparable to 'similar use' in Europe), and other, non-equivalent and divergent uses, that are necessary and proper.[620] Accordingly, in the U.S., data gathered for intelligence purposes may for example be used for law enforcement purposes and *vice versa*.[621]

---

[612] Els De Busser, *Data Protection in EU and US Criminal Cooperation*', 298.
[613] CoE Convention 108, art 3, §1 and 5, (b).
[614] CoE Convention 108, art 2, (b).
[615] Els De Busser, *Data Protection in EU and US Criminal Cooperation*, 298.
[616] 5 U.S.C. § 552a(1) and § 552a(b) (Privacy Act 1974 (United States)).
[617] 5 U.S.C. § 552a(b)(3) (Privacy Act 1974 (United States)).
[618] Els De Busser, *Data Protection in EU and US Criminal Cooperation*, 300.
[619] Ibid.
[620] Ibid.
[621] Els De Busser, *Data Protection in EU and US Criminal Cooperation*, 301.

Similarly, with regard to the collection of SIGINT, it is merely stated in PPD-28 that the Intelligence Community shall establish policies and procedures reasonably designed to minimize the dissemination of personal information and that such dissemination overall is only allowed if the dissemination of comparable information concerning U.S. persons would be permitted under Section 2.3 of Executive Order 12333.[622] According to this Section, however, Agencies within the Intelligence Community are, amongst others, authorised to collect, retain and disseminate information concerning U.S. persons *"necessary for administrative purposes".*[623] This observation is not reassuring at all.

4. Conclusion

177. Neither U.S. domestic law, nor the commitments and representations by the U.S. government have demonstrated that the United States' privacy and data protection policy in case of collection and further processing of personal data transferred under the EU-U.S. Privacy Shield by U.S. public authorities is adequate in the light of the EU requirements. Bulk collection is still possible, the oversight and redress mechanisms are flawed, there is very little information available in the Privacy Shield concerning interferences for law enforcement and public interest purposes and the U.S lacks a general purpose limitation requirement.

178. Finally, it should be noted that adherence to the Principles may also be limited *"[…] by statute, government regulation, or case law that creates conflicting obligations or explicit authorizations, provided that, in exercising any such authorization, an organization can demonstrate that its non-compliance with the Principles is limited to the extent necessary to meet the overriding legitimate interests furthered by such authorization, […] or if the effect of the Directive or Member State law is to allow exceptions or derogations, provided such exceptions or derogations are applied in comparable contexts".*[624] However, no further information regarding the extent of these derogations is available in the Privacy Shield.[625] Moreover, this clearly, especially considering the last exception, illustrates that the U.S. government may interfere with the privacy rights of EU data subjects more than the governments of the Member States.

E. Conclusion: a 'Pricy' Shield

179. From the assessment made above it is clear that the United States does not, in the light of the EU data protection requirements, ensure an adequate level of data protection, and this neither with regard to the substantive standards to which the self-certified companies have to adhere, nor in relation to the

---

[622] PPD-28, s 4(a)(i) Privacy Shield Decision, recital 84.
[623] Ronald Reagan, "Executive Order 12333—United States Intelligence Activities," US Federal Register, Dec. 4, 1981, s 2.3 ['Executive Order 12333'].
[624] Privacy Shield Decision, Annex II, I, point 5.
[625] EDPS Opinion on the EU-U.S. Privacy Shield draft adequacy decision, 7-8.

limitations and safeguards meant to ensure that interferences by the U.S. government with the privacy and data protection rights of EU data subjects are justifiable.

180. It appears that this is the high price the Commission is willing to pay in exchange for the continuation of commercial data flows for commercial reasons between the Union and the United States. Despite the fact that the Commission however clearly put a lot of effort in the negotiation of a more robust framework, it will most likely not satisfy the Court of Justice, nor the EU data subjects themselves.

CHAPTER 4. EU POLICY REGARDING BULK COLLECTION OF PERSONAL DATA AFTER *TELE2 SVERIGE* AND FEASIBILITY OF (STANDARD) CONTRACTUALS CLAUSES AND BINDING CORPORATE RULES AFTER *SCHREMS*: EUROPE TANGLED UP IN ITS OWN DATA PROTECTION REQUIREMENTS?

181. From the previously discussed case law, and especially from the judgment of the Court of Justice of the European Union in *Tele2 Sverige*, it is clear that the 'bulk' retention/collection of personal data, as a matter of principle and thus regardless of whether objective criteria exist by which to determine the limits of access of the competent national authorities to data and their subsequent use or by which to determine the period of retention, cannot be considered a strictly necessary and justified interference with the right to privacy and the right to data protection of EU data subjects (see no. 86). Moreover, from the findings in the *Schrems* case, it can be deducted that an assessment of the adequacy of the data protection regime in place in a third country, prior to transfer of commercial data, cannot be limited to an evaluation of the substantive data protection principles private companies have to adhere to. Instead, the ability of government to collect and further use such data, once they have been transferred, also needs to be analysed. In this Chapter, the consequences and repercussions of this case law, and especially of the said findings regarding mass surveillance, for EU instruments, other than the Data Retention Directive, the Safe Harbour Decision and the EU-U.S. Privacy Shield, will be examined.

182. More particularly, the EU has entered into several agreements with third countries, such as the EU-U.S. Terrorist Finance Tracking Program (TFTP) agreement and a number of Air Passenger Name Record Data (PNR) agreements, that provide for the transfer of personal data in bulk, has as well adopted its own PNR Directive, and allows companies to transfer personal data to third countries, such as the U.S., based on (Standard) Contractual Clauses ((S)CCs) and Binding Corporate Rules (BCRs) while these clearly, like the Privacy Shield, cannot prevent governments from interfering with EU fundamental rights in a unjustified manner.

183. These instruments will be treated in the following order: firstly, the PNR agreements and Directive will be discussed (A); secondly, the TFTP agreement will be analysed (B); thirdly, the value of BCRs or SCCs for the protection of personal data, especially in relation to the United States, will be assessed (C); and lastly, there will be a conclusion summing up the main findings in this Chapter (D).

A. Air Passenger Name Record Data (PNR) – Agreements and Directive

184. In the aftermath of 9/11, the United States, and by extension the entire Western world, have instituted major changes in the way security matters are handled, this often at the expense of the privacy

rights of individuals.[626] It is in that context, considering how the terrorist attacks took place, that governments began to require air carriers to provide them with certain reservation information (PNR) of all passengers.[627] Such data is primarily being processed for purposes of preventing, detecting, investigating, and prosecuting terrorist offences, however, also to combat other serious crime that is transnational in nature.[628] Considering the latter types of crimes, PNR data are thus also used for purposes that have no link with the original justification thereof (i.e. an extraordinary terrorist threat).[629]

185. The EU has concluded PNR agreements with the United States and Australia, and is currently awaiting an opinion of the Court of Justice of the European Union concerning the compatibility of the draft agreement between Canada and the European Union on the transfer of PNR data with article 7, 8 and 52, §1 of the EU Charter, which has to replace the existing agreement from 2006.[630] Those agreements all concern the transfer of PNR data from the Union to one of those countries. Moreover, the EU adopted its own PNR Directive on 27 April 2016.[631]

1. Air Passenger Name Record Data (PNR)

186. In the PNR Directive, a 'passenger name record' is defined as:

> *"a record of each passenger's travel requirements which contains information necessary to enable reservations to be processed and controlled by the booking and participating air carriers for each journey booked by or on behalf of any person, whether it is contained in reservation systems, departure control systems used to check passengers onto flights, or equivalent systems providing the same functionalities".*

---

[626] European Union Committee, *The EU/US Passenger Name Record (PNR) Agreement* (HL 2006-07, 108) 7.
[627] Niovi Vavoula, 'I Travel, therefore I am a Supsect': an overview of the EU PNR Directive' (FREE Group, 27 October 2016) <https://free-group.eu/2016/10/27/i-travel-therefore-i-am-a-suspect-an-overview-of-the-eu-pnr-directive/> accessed 9 May 2017.
[628] U.S. Customs and Border Protection (CBP) (U.S. Department of Homeland Security (DHS)), 'U.S. Customs and Border Protection Passenger Name Record (PNR) Privacy Policy' (2013) 1<https://www.cbp.gov/sites/default/files/documents/pnr_privacy.pdf> accessed 7 May 2017.
[629] Working Party on the Protection of Individuals with regard to the Processing of Personal Data, 'Opinion 7/2010 on European Commission's Communication on the global approach to transfers of Passenger Name Record (PNR) data to third parties' [2010] Opinion WP178, 3 <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2010/wp178_en.pdf> accessed 8 May 2017 ['Working Party 29 WP178'].
[630] 'Transfer of Air Passenger Name Record (PNR) Data and Terrorist Finance Tracking Programme (TFTP)' (Website Commission) <http://ec.europa.eu/justice/data-protection/international-transfers/pnr-tftp/pnr-and-tftp_en.htm> accessed 7 May 2017; Council of the European Union, 'Signature of the EU-Canada agreement on Passenger Name Records (PNR) (Press release, 25 June 2014) <http://www.consilium.europa.eu/en/press/press-releases/2014/06/pdf/signature-of-the-eu-canada-agreement-on-passenger-name-records-(pnr)/> accessed 7 May 2017.
[631] Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime [2016] OJ L119/132 ['PNR Directive'].

To all the aforementioned PNR documents a list specifying the same 19 categories of data has been annexed. These include, *inter alia*, data of reservation/issue of ticket, date(s) of intended travel, name(s), address and contact information (telephone number, e-mail address), all forms of payment information (including billing address) and baggage information.

187. Typically, air carriers must transfer PNR data to the government authorities, via the 'push' method, one day or a few days before the scheduled flight departure time and additionally immediately after flight closure (i.e. after the passengers have boarded).[632]

188. PNR data can be used reactively (historical data), proactively (patterns), or in real time (present data).[633] The data is used in a reactive manner in investigations and prosecutions, or in order to unravel networks *after* a crime has been committed.[634] Proactive use makes it possible to analyse trends, to create fact-based travel and general behaviour patterns and to determine (combinations of) characteristics that could identify someone or something as 'potentially worth investigating'.[635] This is called 'data profiling'. Real time use of PNR data, on the other hand, must *prevent* a crime from taking place or must enable competent authorities to survey or arrest persons *before* a crime is committed or *because* a crime is being or has been committed.[636] Complex algorithms are used to search the databases in order to detect someone or something matching the profile.[637] This is called 'data mining'.[638] In order to be able to use PNR in a reactive and proactive manner, the data must be retained for a certain period.[639]

2. PNR Agreements

189. The PNR agreements with the United States and Australia, and the draft agreement with Canada all concern the transfer of PNR data by air carriers operating passenger flights between the European Union and one of those third countries to the governments of the latter.[640]

---

[632] E.g.: PNR Directive, art 8; Draft agreement between Canada and the European Union on the transfer and processing of Passenger Name Record [2013] art 21 <http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%2012657%202013%20REV%201> ['Draft EU-Canada PNR Agreement']; Agreement between the United States of America and the European Union on the use and transfer of passenger name records to the United States Department of Homeland Security [2012] OJ L215/5, art 15.
[633] Commission, 'Communication from the Commission on the global approach to transfers of Passenger Name Record (PNR) data to third countries' COM(2010) 492 final, point 2.1 ['COM(2010) 492 final'].
[634] Ibid.
[635] COM(2010) 492 final, point 2.1; European Union Committee, *The EU/US Passenger Name Record (PNR) Agreement* (HL 2006-07, 108) 10.
[636] Ibid.
[637] European Union Committee, *The EU/US Passenger Name Record (PNR) Agreement* (HL 2006-07, 108) 10.
[638] Ibid.
[639] Ibid.
[640] Draft EU-Canada PNR Agreement, art 2(a); EU-U.S. PNR Agreement, art 2(2); Agreement between the European Union and Australia on the processing and transfer of Passenger Name Record (PNR) data by air carriers to Australian Customs and Border Protection Service [2012] OJ L186/4, art 2(d).

190. As mentioned above, the draft agreement between Canada and the European Union on the transfer of PNR data, which was signed on 25 June 2014[641], is currently being reviewed by the CJEU. It was the European Parliament, which has to vote on such agreements after they have been negotiated and concluded by respectively the Commission and the Council, who referred the matter to the Court for an opinion.[642] To that end it adopted, on 25 November 2014, a resolution, in which it instructed its President to take the *"necessary measures to obtain such an opinion"*, and in which it specifically referred to the opinion of the former European Data Protection Supervisor of 30 September 2013 on the proposals for the EU-Canada agreement, to the opinion of the Article 29 Working Party on the European Commission's Communication on the global approach to transfers of Passenger Name Record (PNR) data to third countries, and to the *Digital Rights Ireland* case.[643] In its opinion, which preceded the said judgment, the EDPS questioned the necessity and proportionality of the PNR schemes as such as they provide for *"massive and routine processing of data of non-suspicious passengers".*[644] He added that he had not seen convincing elements that demonstrated that other less intrusive methods, due to which the same result could be attained, are not available.[645] These observation are in line with the said opinion of the Article 29 Working Party, in which is stated that *"there are no objective statistics or evidence which clearly show the value of PNR in the international fight against terrorism and serious transnational crime"*.[646] In *Digital Rights Ireland*, as extensively discussed in Chapter 2, the CJEU invalidated the Data Retention Directive because it required the retention of personal data in a generalised and indiscriminate manner, it lacked objective criteria by which to determine the limits of access to this data by the competent authorities and did not justify the length of the retention period (see no. 80 randnummer).

191. On 8 September 2016, Advocate General Mengozzi delivered his opinion in this case.[647] He came to the conclusion, bearing in mind the judgments of the CJEU in *Digital Rights Ireland* and *Schrems*, the latter of which had in the meantime been given on 6 October 2015, that the agreement *"cannot be*

---

[641] Council of the European Union, 'Signature of the EU-Canada agreement on Passenger Name Records (PNR) (Press release, 25 June 2014) <http://www.consilium.europa.eu/en/press/press-releases/2014/06/pdf/signature-of-the-eu-canada-agreement-on-passenger-name-records-(pnr)/> accessed 7 May 2017.

[642] European Parliament Resolution 2014/2966(RSP), 'Seeking an opinion from the Court of Justice on the compatibility with the Treaties of the Agreement between Canada and the European Union on the transfer and processing of Passenger Name Record data' (2014) <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-%2F%2FEP%2F%2FNONSGML%20TA%20P8-TA-2014-0058%200%20DOC%20PDF%20V0%2F%2FEN> accessed 8 May 2017 ['European Parliament Resolution 2014/2966(RSP)']; Consolidated version of the Treaty on the Functioning of the European Union [2007] OJ C326/47, art 218(6) and (11) ['TFEU'].

[643] European Parliament Resolution 2014/2966(RSP), points F and J.

[644] European Data Protection Supervisor, 'Opinion on the Proposals for Council Decisions on the conclusion and signature of the Agreement between Canada and the European Union on the transfer and processing of Passenger Name Record data' [2013] Opinion, 2 <https://edps.europa.eu/sites/edp/files/publication/13-09-30_canada_en.pdf> accessed 8 May 2017.

[645] Ibid.

[646] Working Party 29 WP238, 3.

[647] Opinion 1/15 *Request for an Opinion pursuant to article 218(11) TFEU* (CJEU), Opinion of AG Mengozzi [Opinion of AG Mengozzi EU-Canada PNR Agreement'].

entered into in its current form".[648] More specifically, he considered that the agreement is *per se* incompatible with the Charter, and in particular article 7 and 8 thereof, on 5 points. However, that it would be compatible therewith for the rest provided that it would be adapted in accordance with another 11 points of concern he listed.[649] One of those concerns relates to the principles and rules that govern the processing operations which are performed upon the PNR data once they have been transferred.[650] The Advocate General noted in that regard that *"the main added value of the processing of PNR data is the comparison of the data received with scenarios or predetermined risk assessment criteria or databases which, with the assistance of automated processing, makes it possible to identify 'targets' who can subsequently be subjected to more thorough checks"*.[651] He found, however, that none of the terms in the agreement specifically relate to the determination of those scenarios, criteria, or databases and that accordingly, the Canadian authorities would continue to be in charge thereof.[652] In order to prevent cases in which false positive 'targets' would be identified, he considered that the agreement should contain a number of principles and explicit rules pertaining thereto, which *"should make it possible to arrive at results targeting individuals who might be under a 'reasonable suspicion' of participating in terrorism or serious transnational crime"*.[653] As such, he in fact suggested to introduce the 'reasonable suspicion' test, as put forward by the European Court of Human Rights in *Zakharov v. Russia (*see no. 103), into the case law of the Court of Justice. However, the ECtHR applied this test already in the phase of collection, while the Advocate General makes only use of it in a later phase.

Indeed, Mengozzi did not consider it possible, while referring to the Court's case law in *Digital Rights Ireland*, to actually limit the scope *ratione personae* of the envisaged agreement in such a way that PNR data of individuals would no longer have to be transferred to the Canadian authorities in 'bulk' as alternative measures that would be less restrictive of individuals' fundamental rights *"would [not] be able of attaining with comparable effectiveness the public security aim pursued"*.[654] The Advocate General, unlike the European Data Protection Supervisor and the Article 29 Working Party, thus appears to tolerate that data is transferred to third countries in 'bulk' as he considered that PNR schemes are specifi-

---

[648] Court of Justice of the European Union, 'Advocate General's Opinion in the Request for an Opinion 1/15' (Press release, 8 September 2016) <https://curia.europa.eu/jcms/upload/docs/application/pdf/2016-09/cp160089en.pdf> accessed 8 May 2017; Committee on Civil Liberties, Justice and Home Affairs of the European Parliament (LIBE), 'EU-Canada PNR: legal opinion affirms Parliament's privacy concerns' (Press release, 8 September 2016) <http://www.europarl.europa.eu/news/en/news-room/20160908IPR41656/eu-canada-pnr-legal-opinion-affirms-parliament%E2%80%99s-privacy-concerns> accessed 8 May 2017.
[649] Opinion of AG Mengozzi EU-Canada PNR Agreement, para 328.
[650] Opinion of AG Mengozzi EU-Canada PNR Agreement, paras 252-261 and 328.
[651] Opinion of AG Mengozzi EU-Canada PNR Agreement, para 252.
[652] Opinion of AG Mengozzi EU-Canada PNR Agreement, para 253.
[653] Opinion of AG Mengozzi EU-Canada PNR Agreement, paras 255-256.
[654] Opinion of AG Mengozzi EU-Canada PNR Agreement, paras 238-245.

cally tailored to analyse such massive amounts of data in order to identify previously unknown individuals or situations, and that they are the most effective tool in that regard.[655] Thus, he did not question the use of PNR, collected in 'bulk', as such.

It is important to note, however, that the Court of Justice of the European Union since then delivered its judgment in the *Tele2 Sverige* case. As explained before (see no. 80), the Court, in that case, found that the general and indiscriminate retention of personal data is, as a matter of principle, is not compatible with articles 7, 8 and 52, §1 of the EU Charter on Fundamental Rights.[656] Considering that the Court of Justice is of course aware that it has to deliver an opinion on the EU-PNR Canada agreement, it is not unthinkable that the Court would extend its *Tele2* case law to PNR-instruments, especially considering that the data of 28 million (!) passengers have been transferred to Canada alone between April 2014 and March 2015 and this to newly identify only 9500 'targets'.

192. It goes without saying that the judgment of the Court of Justice, in any event, will have a great impact also for other PNR agreements.[657] Not in the least if the CJEU would indeed confirm its previous case law, but also given the fact that the opinion of the Advocate General contained numerous other remarks. The latter will, however, not further be discussed in the context of this thesis. In the words of Sophie in 't Veld, the Parliament's rapporteur in this dossier, *"it should be clear that any agreement, present or future, must be compatible with [the] EU treaties and fundamental rights and must not be used to lower European data protection standards via the back door"*.[658]

3. PNR Directive

193. As mentioned before, the EU recently adopted its own PNR Directive. As this directive has been adopted in accordance with the ordinary legislative procedure, the EU Parliament was involved in the decision-making process and has approved the final text (by 461 votes to 179, with 9 abstentions).[659] Considering the Parliament's referral of the PNR Canada agreement after the CJEU's ruling in *Digital Rights Ireland*, it seems that the Parliament is thus not entirely consistent in its policy regarding PNR.[660] Of course the overall data protection regime in the European Union, as opposed to the one of third

---

[655] Opinion of AG Mengozzi EU-Canada PNR Agreement, para 241.
[656] *Tele2 Sverige AB*, para 112.
[657] Opinion of AG Mengozzi EU-Canada PNR Agreement, para 4.
[658] European Parliament, 'MEPs refer EU-Canada air passenger data deal to the EU Court of Justice' (Press release, 25 November 2014) <http://www.europarl.europa.eu/news/en/news-room/20141121IPR79818/meps-refer-eu-canada-air-passenger-data-deal-to-the-eu-court-of-justice> accessed 8 May 2017.
[659] European Parliament, 'Parliament back EU directive on use of Passenger Name Records (PNR)' (Press release, 14 April 2016) <http://www.europarl.europa.eu/news/en/news-room/20160407IPR21775/parliament-backs-eu-directive-on-use-of-passenger-name-records-(pnr)> accessed 8 May 2017.
[660] Note that the Parliament did not equally refer the previously concluded agreements with the United States and Australia.

countries, is considered to be adequate by definition and the PNR Directive contains more data safeguards than the aforementioned agreements. However, that does not change the fact that the PNR data of *all* passengers of *all* flights flying from a third country to the territory of a Member State or *vice versa* have to be provided in 'bulk' the competent national authorities (*in casu* to the national 'Passenger information units (PIUs)').[661] As the judgment of the Court of Justice is expected to also have an impact on this directive, it is difficult to understand why the Parliament did not await this ruling, especially considering that the *Tele2 Sverige* was also pending at the time of the adoption of the directive.[662]

4. Conclusion

194. It appears from the considerations above that the European Commission, this time in the context of PNR, again failed to adequately protect the privacy and data protection rights of EU data subjects.[663] As the EU-Canada PNR agreement was signed only after the Court of Justice gave its judgment in *Digital Rights Ireland*, the Commission should have renegotiated the agreement before its signature took place.

The European Parliament, from its side, has proved to be an important counterbalance to the Commission. However, considering the recent adoption of the EU PNR Directive, the credibility of the EU Parliament in this respect has also been reduced.

195. Considering the recent judgment of the Court of Justice in the *Tele2 Sverige* case, it is, however, not unlikely that the Court, in the pending PNR Canada case, would rule that bulk collection is also prohibited when it concerns PNR data.

196. What is certain, on the other hand, is that this judgment will have, or at least should have, an important effect on the future policy of the EU as regards the processing of PNR or other personal data for public interest purposes.

B. EU-U.S. Terrorist Finance Tracking Programme (TFTP) Agreement

197. After the 9/11 terrorist attacks, the United States, and more in particular the U.S. Department of the Treasury, also initiated the so called 'Terrorist Finance Tracking Program' (TFTP).[664] As part of this programme, the U.S. also collects and further processes personal data in 'bulk'. Considering that the

---

[661] PNR Directive, art 1(1)(a), 3(2), 4, 6(1), and 8(1).
[662] Opinion of AG Mengozzi EU-Canada PNR Agreement, para 4; 'European Court Opinion: Canada PNR deal cannot be signed' (European Digital Rights (EDRi), 8 September 2016) <https://edri.org/european-court-opinion-canada-pnr-deal-cannot-be-signed/> accessed 8 May 2017 ['EDRi, 'European Court Opinion: Canada PNR deal cannot be signed']; The request for a preliminary ruling in the *Tele2 Sverige AB* case dates from 4 May 2015: <http://curia.europa.eu/juris/document/document.jsf?text=&docid=165124&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=262745>.
[663] EDRi, 'European Court Opinion: Canada PNR deal cannot be signed'.
[664] 'Terrorist Finance Tracking Program (TFTP) (Website U.S. Department of the Treasury) <https://www.treasury.gov/resource-center/terrorist-illicit-finance/Terrorist-Finance-Tracking/Pages/tftp.aspx> accessed 9 May 2017 ['Website U.S. Department of the Treasury, 'TFTP'].

EU-U.S. TFTP Agreement ensures the transfer of a substantial amount of this data from the Union to the U.S. Department of the Treasury it will also be impacted by the recent case law of the Court of Justice, and especially by the *Tele2 Sverige* judgment.

1. Terrorist Finance Tracking Programme (TFTP): functioning and SWIFT

198. In June 2006, a number of American newspapers revealed the existence of a counterterrorism programme, the so called 'Terrorist Finance Tracking Programme' (TFTP), under which the U.S government covertly collected and examined worldwide financial transactions data.[665]. Via administrative subpoenas (see 170-172), the U.S. Department of the Treasury, which had initiated the programme, required the U.S. hub of a Belgian-based cooperative, called SWIFT, to produce millions of banking records.[666] This company, the 'Society for Worldwide Interbank Financial Telecommunication', provides a network that enables financial institutions to securely send each other instructions via a standardised system of codes.[667] Via a SWIFT payment transfer message one bank can instruct another bank to credit the account of one of its customers.[668] Considering that SWIFT's market share of is around 80% globally and the company routes trillions of messages between different kinds of financial institutions daily, it is clear that the U.S. Treasury could gain access to massive amounts of banking data from individuals all around the world.[669] As the data originated within the European Union, SWIFT's U.S. hub needed to be self-certified under the former Safe Harbour scheme, though it was not.[670] However, as extensively discussed in Chapter 3, self-certification would not have prevented the U.S. government from gaining access to the said data.

At that point in time, SWIFT had two operational centres, one in United States and one in Europe.[671] All messages processed by SWIFT were stocked in both of these centres in order to, in case of a dispute

---

[665] Pepijn Terra, 'SWIFT en het 'Terrorist Finance Tracking Program': triomf voor de burger of voor het Europees Parlement?' (2010) 64 Internationale Spectator 577, 1 ['Pepijn Terra, 'SWIFT en het 'Terrorist Finance Tracking Program': triomf voor de burger of voor het Europees Parlement?']; Gert Vermeulen, 'The Paper Shield', 1; Eric Lichtblau and James Risen, 'Bank Data is Sifted by U.S. in Secret to Block Terror' *The New York Times* (23 June 2013) <http://www.nytimes.com/2006/06/23/washington/23intel.html> accessed 9 May 2017 ['The New York Times, 'Bank Data is sifted by U.S. in Secret to Block Terror'].

[666] The New York Times, 'Bank Data is sifted by U.S. in Secret to Block Terror'; Website U.S. Department of the Treasury, 'TFTP'; Gert Vermeulen, 'The Paper Shield', 1.

[667] Shobhit Seth, 'How The SWIFT System Works' (Investopedia, 5 May 2015) <http://www.investopedia.com/articles/personal-finance/050515/how-swift-system-works.asp> accessed 9 May 2017 ['Shobhit Seth, 'How The SWIFT System Works'].

[668] 'A simple explanation of how money moves around the banking system' (Richard Gendal Brown) <https://gendal.me/2013/11/24/a-simple-explanation-of-how-money-moves-around-the-banking-system/> accessed 9 May 2017; Shobhit Seth, 'How The SWIFT System Works'.

[669] The New York Times, 'Bank Data is sifted by U.S. in Secret to Block Terror'; Pepijn Terra, 'SWIFT en het 'Terrorist Finance Tracking Program': triomf voor de burger of voor het Europees Parlement?', 1.

[670] Gert Vermeulen, 'The Paper Shield', 1.

[671] Commissie voor de bescherming van de persoonlijke levenssfeer, 'Advies betreffende de doorgifte van persoonsgegevens door de CVBA SWIFT ingevolge de dwangbevelen van de UST (OFAC)' (2006) Advies Nr 37/2006, 3

with a client or of loss of data, always have a back-up of the data in one of the two centres.[672] Following pressure from the European Parliament, SWIFT, however, started storing the intra-EU money transfer data in a newly built backup server in Switzerland at the end of 2009.[673] More particularly, SWIFT created a 'Distributed Architecture' – namely two separate continental messaging zones: a European zone and a Trans-Atlantic one.[674] Intra-zone messages of customers located in the European Zone (EEA, Switzerland and other territories that are considered to be a part of the EU or are associated therewith) must remain in that zone – i.e. in the SWIFT operational centres in the Netherlands and Switzerland.[675] Customers located in the United States are allocated to the Trans-Atlantic Zone, which operating centres are in the United States and Switzerland.[676] Their intra-zone data must also be kept in their zone.[677] Data of other customers are allocated to one of these zones, as appropriate.[678] Messages transmitted between these different zones are stored in the U.S, in the Netherland and in Switzerland.[679] Accordingly, the U.S. Treasury Department could no longer use subpoenas to be provided with, according to the U.S., 'critical data' that is now merely stored on servers on European territory.[680] This is where the EU-U.S. TFTP Agreement comes in.

2. EU-U.S. Agreement

199. Under strong U.S. pressure, the EU and the U.S., in 2010, concluded the 'Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program'.[681] Pursuant to this agreement the intra-European payment transactions data may be transferred ('pushed'), in 'bulk', on a case-by-case basis, directly to the U.S. Treasury Department.[682] More specif-

<https://www.privacycommission.be/sites/privacycommission/files/documents/advies_37_2006_0.pdf> accessed 9 May 2017 ['CBPL, 'SWIFT advies''].
[672] Ibid.
[673] Ariadna Ripoll Servent, *Institutional and Policy Change in the European Parliament: Deciding on Freedom, Security and Justice* (Springer 2015) 110 ['Ariadna Ripoll Servent, *Institutionals and Policy Change in the European Parliament*']; Gert Vermeulen, 'The Paper Shield', 2; Website U.S. Department of the Treasury, 'TFTP'.
[674] Ariadna Ripoll Servent, *Institutional and Policy Change in the European Parliament* 110.
[675] Website SWIFT, 'SWIFT and data' <https://www.swift.com/about-us/swift-and-data> accessed 10 May 2017.
[676] Ibid.
[677] Ibid.
[678] Ibid.
[679] Ibid.
[680] Website U.S. Department of the Treasury, 'TFTP'.
[681] Ian Traynor, 'EU threatens to suspend deal with US on tracking terrorists' funding' *The Guardian* (24 September 2013) <https://www.theguardian.com/world/2013/sep/24/eu-threat-us-data-sharing-terrorist-funding> accessed 9 May 2017; Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program [2010] OJ L195/5 ['EU-U.S. TFTP Agreement'].
[682] EU-U.S. TFTP Agreement, art 4; Gert Vermeulen, 'The Paper Shield', 2; Ariadna Ripoll Servent, *Institutional and Policy Change in the European Parliament* 115.

ically, the U.S. Department of the Treasury may issue 'production orders' ('requests') upon a 'Designated Provider' (in the annex to the agreement identified as 'SWIFT') present in the territory of the United States to obtain financial payment messaging and related data necessary for the purpose of the prevention, investigation, detection, or prosecution of terrorism or terrorist financing *"that are stored in the territory of the European Union"*.[683] These request must identify the data, including the specific categories of data, *"as clearly as possible"*, shall clearly substantiate the necessity of the data, and must be *"as tailored as possible"*.[684] As explained in Chapter 3 (see no. 157), these conditions do not at all guarantee that the interference is limited to what is 'strictly necessary'. In any event, Europol is required to verify, prior to transfer, whether the aforementioned conditions are fulfilled.[685] If so, the Designated Provider is thereby authorised and required to provide the data to the U.S. Treasury Department.[686]

200. Similarly to the collection and further processing of signals intelligence, the collected data are stored in a sort of 'black box' (see no. 155).[687] This 'store' is subsequently queried and only the data that result from the queries are being examined.[688] However, as argued before in the context of the adequacy assessment of the EU-U.S Privacy Shield and the examination of PNR schemes, the Court of Justice clearly stated in *Tele2 Sverige* that 'bulk' collection of personal data, even where there are sufficient access-restraints in place, cannot be reconciled with the fundamental rights, and in particular article 7 and 8 of the EU Charter, of EU data subjects.

201. As explained before (see no. 198), messages exchanged between the European and the Transatlantic Zone are still stored in the United States. This means that the U.S. Department of the Treasury may still issue subpoenas in order to be provided with that set of data. According to EU law, that data also must be adequately protected as they partly originate from within the European Union (see no. 11). This data may, at best, still benefit from the representations the United States has unilaterally made in 2007, which concerned the 'processing of EU originating personal data by the United States Treasury Department for counterterrorism purposes'.[689] These were issued in July 2007 after the TFTP programme had been disclosed by American newspapers and were meant to reassure the EU at a point in time where also intra-EU data was still transferred to the United States. As such, it is unclear whether trans-Atlantic data flow still benefit therefrom. Furthermore, unlike the commitments of the U.S. in the TFTP Agreement,

[683] EU-U.S. TFTP Agreement, arts 2 and 4(1).
[684] EU-U.S. TFTP Agreement, art 4(2).
[685] EU-U.S. TFTP Agreement, art 4(4.
[686] EU-U.S. TFTP Agreement, art 4(6).
[687] 'CBPL, 'SWIFT advies', 5.
[688] Ibid.
[689] Terrorist Finance Tracking Program – Representations of the United States Department of the Treasury [2007] OJ C166/18.

these representations are not legally binding.[690] Their legal value is thus similar to that of the commitments and representations annexed to the EU-U.S. Privacy Shield (see no. 123). The fact that SWIFT is neither self-certified under the EU-U.S. Privacy Shield, nor, for data protection purposes, seems to make use of Binding Corporate Rules (BCRs) moreover implies that the company itself does not consider that such data partly originates within the European Union.[691]

202. On top of that, in September 2013, NSA documents disclosed by Edward Snowden showed that the United States even circumvent the TFTP Agreement as they clearly designated the SWIFT computer network as a 'target'.[692] As a result, the European Commission threatened to end agreement and the European Parliament adopted a resolution calling for a suspension thereof.[693] However, the agreement still exists today and the Commission recently reported on the fourth joint review of the implementation of the TFTP Agreement concluding that *"the Agreement and its safeguards and controls are properly implemented"*, as if nothing happened.[694]

203. Lastly, it should be noted that the European Commission, notwithstanding the observations made above, will analyse the need for complementary mechanisms to the EU-U.S. TFTP Agreement to fill any potential gaps – the EU also benefits from the TFTP Agreement to some extent as the U.S. authorities may transfer useful data and Member States' authorities may also request information – and notably as regards transactions which are excluded from the agreement.[695]

3. Conclusion

204. Considering the United States, by virtue of this agreement, is again provided with personal data of EU data subjects in 'bulk', it is clear that the TFTP Agreement is yet another EU instrument that does not pass the 'strict necessity' test as set out by the Court of Justice of the European Union. As it is

---

[690] General Secretariat of the Council of the EU, 'EU-US agreement on the processing and transfer of financial messaging data for purposes of the US Terrorist Finance Tracking Programme (TFTP) – Questions and Answers' (Information note, November 2009) <https://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/jha/111559.pdf> accessed 10 May 2017.

[691] 'Privacy Shield List' (Website Privacy Shield Framework (United States)), <https://www.privacyshield.gov/participant_search> accessed 10 May 2017.

[692] Laura Poitras, Marcel Rosenbach and Holger Stark, 'NSA Monitors Financial World' *Spiegel Online* (16 September 2013) <http://www.spiegel.de/international/world/how-the-nsa-spies-on-international-bank-transactions-a-922430.html> accessed 10 May 2017.

[693] Ian Traynor, 'EU threatens to suspend deal with US on tracking terrorists' funding' *The Guardian* (24 September 2013) <https://www.theguardian.com/world/2013/sep/24/eu-threat-us-data-sharing-terrorist-funding> accessed 10 May 2017; European Parliament Resolution 2013/2831(RSP), 'Suspension of the SWIFT agreement as a result of NSA surveillance' (2013) <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+TA+P7-TA-2013-0449+0+DOC+PDF+V0//EN> accessed 10 May 2017.

[694] Commission, 'Report from the Commission to the European Parliament and the Council on the joint review of the implementation of the Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program' COM(2017) 31 final, 3.

[695] EU-U.S. TFTP Agreement, arts 9-10; 'Terrorist Finance Tracking Programme' (Website Commission) <https://ec.europa.eu/home-affairs/what-we-do/policies/crisis-and-terrorism/tftp_en> accessed 10 May 2017.

moreover difficult to understand how such 'bulk' access to intra-EU financial messaging data is justifiable in the light of the WTC terrorist attacks, it appears that 9/11 has merely become a great excuse for our 'partner' – which meanwhile still covertly collects data from SWIFT - to monitor the comings and goings of everyone on the entire planet. Before *Digital Rights Ireland*, *Schrems* and *Tele2 Sverige* this agreement was already controversial, keeping it still, on the other hand, is completely unacceptable.

C. (Standard) contractual clauses and binding corporate rules

205. As explained in Chapter 1, transfers of personal data to a third country that does not ensure an adequate level of data protection may still be authorised *"where the controller adduces adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals and as regards the exercise of the corresponding rights"*.[696] Such safeguards may in particular result from appropriate (standard) contractual clauses ((S)CCs) or binding corporate rules (BCRs) (see nos. 27-30).[697]

206. It must be noted, however, that (S)CCs or BCRs might not take precedence over legislation of a third country by which the recipient may be required to disclose the transferred personal data to the state in certain circumstances.[698] In the EU, as discussed before, such disclosures can only take place within the limits of article 13(1) of Directive 95/46/EC or article 15, §1 of Directive 2000/58/EC, and must, as is clear from the case law of the Court of Justice, in particular be considered 'strictly necessary' in the light of article 7, 8 and 52(1) of the EU Charter on Fundamental Rights. From the *Schrems* judgment of the CJEU it became particularly clear that third countries, in view of the adequacy requirement, must have 'essentially equivalent' limitations in place in that regard. The assessment made in part D of Chapter 3, however, clearly illustrates that the ability of a state to require companies and organisations on their territory to provide competent authorities with personal data is not at all limited to what is 'strictly necessary' in all third countries, especially having regard to the Court's interpretation of this requirement in the *Tele2 Sverige* case. As (S)CCs and BCRs thus cannot remedy the inadequacy of the data protection regime of a third country in that respect, they can merely be used where this is not necessary and thus only where the level of data protection provided by third country organisations themselves cannot be considered to be adequate.

207. On the contrary, following the invalidation of the Safe Harbour Decision, the Article 29 Working Party, and, in consequence, the Commission both took the view that these (S)CCs or BCRs could still

[696] Directive 95/46/EC, art 26(2).
[697] Ibid.
[698] Working Party 29 WP12, 21.

be used as alternative tools for the transfer of personal data to the United States (see no. 119).[699] However, the two sets of standard contractual clauses for transfers from data controllers to data controllers established outside the EU as well as the set for the transfer from data controllers to data processors established outside the EU adopted by the Commission (see no. 28) all foresee that data may not be transferred if the law to which the data importer is subject goes beyond what is necessary in a democratic society on the basis of one of the interests listed in article 13(1) of Directive 95/46/EC.[700] After *Schrems*, it was of course clear to everyone that this was indeed the case. The reason why the Working Party and the Commission nonetheless suggested the use of (S)CCs and BCRs surely related to the fact that data flows between the U.S. and the EU could in practice not be discontinued overnight and there was simply no other option. Fortunately, the Working Party added that it would nonetheless continue to analyse the impact of the judgment on these alternative tools.[701] However, considering that not even a framework as the Privacy Shield can impede the United States from interfering with the fundamental rights of EU data subjects in an unjustified manner, it can only come to the conclusion that no contractual clauses or binding corporate rules would.

208. As clarified before, the adequacy requirement demands an assessment both of the private and the public sector privacy and data protection rules. Neither (standard) contractual clauses nor binding corporate rules, both commercial (private) sector tools, can thus be used to remedy the inadequacy of the limitations to the ability of a third state's government to require the provision of personal data by private sector actors who have received such data relating to EU data subjects.

D. Conclusion

209. It is clear that the recent judgments of the Court of Justice of the European Union (*Digital Rights Ireland*, *Schrems* and *Tele2 Sverige*) as well as those of the European Court of Human Rights (*Zakharov v. Russia* and *Szabó and Vissy v. Hungary*) also may have great consequences and repercussion for other EU instruments.

210. More particularly, it became apparent from these judgments that the 'bulk' collection of personal data cannot be permitted merely because it proves to be *useful*. To the contrary, an interference with the privacy and data protection rights of EU/European data subjects must always be *necessary*. Both the

---

[699] COM(2015) 566 final, point 1.
[700] Working Party 29 WP237, 4; Commission Decision 2001/497/EC of 15 June 2001 on standard contractual clauses for the transfer of personal data to third countries, under Directive 95/46/EC [2001] OJ L181/19, art 4(1)(a); Commission Decision 2004/915/EC of 27 December 2004 amending Decision 2001/497/EC as regards the introduction of an alternative set of standard contractual clauses for the transfer of personal data to third countries [2004] OJ L385/74; Commission Decision of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council [2010] OJ L39/5, art 4(1)(a).
[701] Ibid.

Court in Luxembourg and the Court in Strasbourg took the view that 'bulk collection' of personal data is not. As both PNR schemes and the TFTP are entirely based on such mechanism, they are thus fundamentally in conflict with the EU data protection standards. Accordingly, the pending case concerning the renewal of the PNR deal with Canada is definitely a very awaited judgment that will clarify a lot in that regard. Accordingly, the European Parliament should have postponed the vote on the EU PNR Directive instead of maintaining double standards. The fact that the European Commission is moreover still considering the introduction of an European TFTP system is equally mystifying.

211. From the CJEU's judgment in the *Schrems* case, it can moreover be deducted that an assessment of the limitations to the ability of a third state's government to require the provision of personal data by organisations that process personal data for commercial purposes, is equally important as an assessment of the adequacy of the data protection safeguards third country companies have to adhere to. Considering that (S)CCs and BCRs can only turn affirmative negative findings in the latter context, the usefulness of these instruments is thus particularly limited.

212. In sum, it must be concluded that the EU, after these judgments, is tangled up in its own data protection requirements. The findings above clearly indicate that the EU should reassess its policy as regards the fight against terrorism and other serious crime. The collection of personal data of everyone, without distinguishing between people that can be 'reasonably suspected' and people who cannot, is no longer possible. Both within and outside the European border personal data of EU data subjects deserves to be adequately protected against unjustified interferences by governments. The EU has failed to find an acceptable balance between legitimate security interests and the fundamental rights of its citizens. Luckily, the Court of Justice of the EU and the European Court of Human Rights now have provided crystal clear guidance in that regard.

MAIN FINDINGS

213. In order to transfer personal data, gathered within the European Union, to a third country for commercial purposes, European Union law, and more in particular article 25, §1 of Directive 95/46/EC, requires that this country ensures an 'adequate' level of data protection. 'Adequate', in terms of data protection, means 'essentially equivalent to the data protection standards in the EU'. In order to conclude that a third country indeed fulfils this requirement, it must be established that at least the 'core' principles of EU data protection law are mirrored in that particular country, provided that these principles are not undermined by the provision, in favour of the government, of very broad derogations thereto. Accordingly, an adequacy assessment requires not only the evaluation of a third country's substantive data protection standards, which must be observed by the recipient companies in the third country in question, but also the examination of the formulation and the implications of derogations to such substantive standards.

214. The 'core' EU substantive data protection standards consist of 'content' principles as well as 'procedural/enforcement' requirements. The 'content' requirements concern the principles of 'purpose limitation', 'proportionality', 'data quality', 'transparency' and 'data security', the rights of 'access', 'rectification' and 'opposition', the 'restrictions on onward transfers' (adequacy requirement), and a number of 'additional principles' which apply to specific types of processing. The 'procedural/enforcement' requirements demand mechanisms that ensure good compliance with the rules, that support and help individual data subjects and that guarantee an injured party (data subject) the right to redress where rules are not complied with.

EU law allows Member States to adopt legislative measures to restrict the scope of a number of these obligations and rights when such a restriction constitutes a necessary measure to safeguard, *inter alia*, national security or the prevention, investigation, detection and prosecution of criminal offences. However, both the Court of Justice of the European Union and the European Court of Human Rights take the view that the collection, retention, access or use of personal data (i.e. surveillance measures), originally processed for other purposes, by or to the benefit of the government, constitute interferences with respectively articles 7 and 8 of the EU Charter on Fundamental Rights and article 8 of the European Convention on Human Rights, which may only be justified if they prove to be 'strictly necessary' to attain the legitimate objective(s) pursued. More specifically, both courts ruled that legislation providing for the general and indiscriminate collection/retention of personal data, originally processed for other purposes, does not pas this test. In other words, it is (finally) clear that mass surveillance of citizens is not compatible with the privacy and data protection rights of EU data subjects. From the jurisprudence of these courts, it should also be concluded that legislation regarding surveillance measures moreover has to lay down objective criteria with regard to the subsequent 'access' to and 'use' of the collected/retained data and as regards the duration of these measures, and must contain rules regarding the storage

and deletion of the data. The Court of Justice as well as the European Court of Human Rights also require the installation of (an) independent supervisory mechanism(s), which monitor(s) the surveillance practices so as to ensure 'good compliance' with the rules, and the provision of a right for every person to a (judicial) remedy in case his/her rights have nevertheless been breached.

215. The European Commission is entitled, on the basis of article 25, §6 of Directive 95/46/EC, to establish that the data protection regime in a third country, by reason of its domestic law or of the international commitments it has entered into, can be considered 'adequate'. The effect of such a finding is that personal data may be freely transferred from the EU to the third country in question. The Commission may thus analyse the data protection regime in place in a third country in the light of the EU standards, and conclude, if there are sufficient reasons thereto, that it indeed ensures an adequate level of data protection. In relation to the United States, the Commission has done so in its Decision 2016/1250 of 12 July 2016, in which it indeed came to the conclusion that the *"the United States ensures an adequate level of protection for personal data transferred from the Union to organisations in the United States under the EU-U.S. Privacy Shield"*.

From the assessment made in this thesis, however, it is clear that the United States, under the EU-U.S Privacy Shield, does not, in the light of the EU data protection requirements, ensure an adequate level of data protection, and this neither with regard to the substantive standards to which the self-certified companies have to adhere (*i.e.* the EU-U.S. Privacy Shield Framework Principles), nor in relation to the limitations and safeguards meant to ensure that interferences by the U.S. government with the privacy and data protection rights of EU data subjects are 'strictly necessary'. The disproportionality of the said interferences is particularly apparent from the fact that the U.S. administration is still allowed 'bulk' collection of personal data originally processed for commercial purposes, stores this data for at least five years, is not sufficiently accountable to sufficiently independent oversight bodies and does not provide EU data subjects with adequate redress options in case their privacy rights have been breached.

It thus appears that the Commission prioritises the continuation of commercial data flows from the Union to the United States over adequately protecting the privacy and data protection rights of EU data subjects.

216. The findings of the Luxembourg and Strasbourg Courts as regards the incompatibility of 'bulk' collection of personal data with fundamental rights also have repercussions for other EU instruments. As both PNR schemes and TFTP are entirely based on such mechanism, their sustainability as well as feasibility is highly questionably and has to be reconsidered.

In that context, the limitations to the use of (standard) contractual clauses ((S)CCs) and binding corporate rules (BCRs) have also been examined. (S)CCs and BCRs are private (commercial) sector tools that can be used to remedy the lack of adequacy of the data protection rules of a third country applicable to

organisations established in that country. However, neither (S)CCs nor BCRs can be used to remedy the inadequacy of the third state's limitations to its government's right to require the provision of personal data by private sector actors who have received such data of EU data subjects, and, as such, they cannot prevent the government of a third state to interfere with the privacy and data protection rights of EU data subjects in a disproportionate and unjustified manner. This also means that, after the invalidation of the Safe Harbour Decision, personal data transfers from the Union to the United States could not be legitimately based on these alternative transfer tools, albeit they were.

It thus appears that the EU is, currently, tangled up in its own data protection requirements and must fundamentally reconsider its policy regarding the protection of personal data where these might have to be collected or further processed for national security of law enforcement purposes.

BIBLIOGRAPHY

Primary Sources

European Union legal sources

Primary legislation

- Consolidated version of the Treaty on the Functioning of the European Union [2007] OJ C326/47
- Charter of Fundamental Rights of the European Union [2007] OJ C 326/391

Secondary legislation

- Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L281/31
- Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector [1997] OJ L024/1
- Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce [2000] OJ L215/7
- Commission Decision 2001/497/EC of 15 June 2001 on standard contractual clauses for the transfer of personal data to third countries, under Directive 95/46/EC [2001] OJ L181/19
- Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data [2001] OJ L8/1
- Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) [2002] OJ L201/37
- Commission Decision 2004/915/EC of 27 December 2004 amending Decision 2001/497/EC as regards the introduction of an alternative set of standard contractual clauses for the transfer of personal data to third countries [2004] OJ L385/74
- Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available

electronic communications services or of public communications networks and amending Directive 2002/58/EC [2006] OJ L 105/54

- Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters [2008] OJ L350/60
- Commission Decision of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council [2010] OJ L39/5
- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L119/1
- Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA [2016] OJ L119/89
- Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime [2016] OJ L119/132
- Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council of the adequacy of the protection provided by the EU-U.S. Privacy Shield [2016] OJ L207/1

Agreements

- Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program [2010] OJ L195/5
- Agreement between the European Union and Australia on the processing and transfer of Passenger Name Record (PNR) data by air carriers to Australian Customs and Border Protection Service [2012] OJ L186/4
- Agreement between the United States of America and the European Union on the use and transfer of passenger name records to the United States Department of Homeland Security [2012] OJ L215/5

- Draft agreement between Canada and the European Union on the transfer and processing of Passenger Name Record [2013] <http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%2012657%202013%20REV%201>

Court of Justice of the European Union

- Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, The Commissioner of the Garda Síochána, Ireland and the Attorney General, and Kärntner Landesregierung, Michael Seitlinger, Christof Tschohl and Others* [2014] ECLI:EU:C:2014:238
- Case C-362/14 *Maximilian Schrems v Data Protection Commissioner* [2015] ECLI:EU:C:2015:650
- Joined Cases C-203/15 and C-698/15 *Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others* [2016] ECLI:EU:C:2016:970
- Opinion 1/15 *Request for an Opinion pursuant to article 218(11) TFEU* (CJEU), Opinion of AG Mengozzi

Council of Europe legal sources

Treaties

- Convention for the Protection of Human Rights and Fundamental Freedoms [1950] ETS No. 5
- Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data [1981] ETS No.108
- Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authorities and transborder data flows [2001] ETS No. 181

Judgments of the European Court of Human Rights

- *Klass and others v Germany* (1978) Series A no 28
- *Zakharov v. Russia* ECHR 2015
- *Szabó and Vissy v. Hungary* ECHR App no 37138/14 (ECtHR, 12 January 2016)

Belgian legal sources

- Wet 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens (*BS* 18 March 1993, consolidated version *BS* 28 December 2015)

United States legal sources

- "The Constitution of the United States"
- Privacy Act 1974
- Foreign Intelligence Serivce Act 1978
- Ronald Reagan, "Executive Order 12333—United States Intelligence Activities," US Federal Register, Dec. 4, 1981
- The White House, Presidential Policy Directive 28: Signals Intelligence Activities (PPD-28) (Jan. 17, 2014)

Secondary Sources

Doctrine

- De Busser E, *Data Protection in EU and US Criminal Cooperation – A Substantive Law Approach to the EU Internal and Transatlantic Cooperation in Criminal Matters between Judicial and Law Enforcement Authorities* (Maklu 2009)
- Granger M-P and Irion K, 'The Court of Justice and the Data Retention Directive in Digital Rights Ireland: Telling off the EU legislator and Teaching a Lesson in Privacy and Data Protection' (2014) 20 European Law Review
- Haeck Y and Burbano Herrera C, *Procederen voor het Europees Hof voor de Rechten van de Mens* (Tweede editie, Intersentia, 2011)
- Hustinx P, 'EU Data Protection Law: The Review of Directive 95/46/EC and Proposed General Data Protection Regulation' [2014] <https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2014/14-09-15_Article_EUI_EN.pdf> accessed March 2017
- Ripoll Servent A, *Institutional and Policy Change in the European Parliament: Deciding on Freedom, Security and Justice* (Springer 2015)
- Schneier B, *Data and Goliath – The Hidden Battles to Collect Your Data and Control Your World* (W. W. Norton & Company Ltd, first edition 2015)
- Severson D, 'American Surveillance of Non-U.S. Persons: Why New Privacy Protections Offer Only Cosmetic Change' (2015) 56 Harvard International Law Journal

- Terra P, 'SWIFT en het 'Terrorist Finance Tracking Program': triomf voor de burger of voor het Europees Parlement?' (2010) 64 Internationale Spectator 577
- Tracol X, 'Legislative genesis and judicial death of a directive: The European Court of Justice invalidated the data retention directive (2006/24/EC) thereby creating a sustained period of legal uncertainty about the validity of national laws which enacted it' (2014) 30 Computer Law & Security Review
- Tracol X, '"Invalidator" strikes back: The harbour has never been safe' (2016) 32 Computer Law & Security Review
- Vermeulen G, 'The Paper Shield: On the degree of protection of the EU-US privacy shield against unnecessary or disproportionate data collection by the US intelligence and law enforcement services' in Svantesson, Dan J.B. and Dariusz Kloza (eds), *Transatlantic Data Privacy Relationships as a Challenge for Democracy; European Integration and Democracy Series,* vol 4 (Intersentia 2017)

European Commission documents

Communications

- Commission, 'Communication from the Commission on the global approach to transfers of Passenger Name Record (PNR) data to third countries' COM(2010) 492 final
- Commission, 'Communication from the Commission to the European Parliament and the Council on Rebuilding Trust in EU-US Data Flows' COM(2013) 846 final
- Commission, 'Communication from the Commission to the European Parliament and the Council on the Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Established in the EU' COM(2013) 847 final
- Commission, 'Communication from the Commission to the European Parliament and the Council on the Transfer of Personal Data from the EU to the United States of America under Directive 95/46/EC following the Judgment by the Court of Justice in Case C-362/14 (Schrems)' COM(2015) 566 final
- Commission, 'Report from the Commission to the European Parliament and the Council on the joint review of the implementation of the Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program' COM (2017) 31 final

Other documents

- Commission, 'Frequently Asked Questions relating to transfers of personal data from the EU to third countries' [2009], 23 <http://ec.europa.eu/justice/data-protection/international-transfers/files/international_transfers_faq.pdf> accessed 18 March 2017
- Directorate-General for Justice and Consumers (Commission), *2014 report on the application of the EU Charter of Fundamental Rights* (Publications Office of the European Union 2015
- Directorate-General for Justice and Consumers (Commission), *Guide to the EU-U.S. Privacy Shield* (Publications Office of the European Union 2016)

European Parliament documents

Resolutions

- European Parliament Resolution 2013/2831(RSP), 'Suspension of the SWIFT agreement as a result of NSA surveillance' (2013) <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+TA+P7-TA-2013-0449+0+DOC+PDF+V0//EN> accessed 10 May 2017
- European Parliament Resolution 2014/2966(RSP), 'Seeking an opinion from the Court of Justice on the compatibility with the Treaties of the Agreement between Canada and the European Union on the transfer and processing of Passenger Name Record data' (2014) <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-%2F%2FEP%2F%2FNONSGML%20TA%20P8-TA-2014-0058%200%20DOC%20PDF%20V0%2F%2FEN> accessed 8 May 2017
- European Parliament Resolution 2016/2727(RSP), 'Transatlantic data flows' (2016) <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+TA+P8-TA-2016-0233+0+DOC+PDF+V0//EN> accessed 25 April 2017
- European Parliament Resolution 2016/3018(RSP), 'Adequacy of the protection afforded by the EU-US privacy Shield' (2016) <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-%2F%2FEP%2F%2FNONSGML%20TA%20P8-TA-2017-0131%200%20DOC%20PDF%20V0%2F%2FEN> accessed 25 April 2017

Other documents

- LIBE (European Parliament), 'Questions relating to the judgment of the Court of Justice of 8 April 2014 in Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland* and *Seitlinger and others* – Directive 2006/24/EC on data retention – Consequences of the judgment'(legal opinion) SJ-0890/14
- Directorate-General for Internal Policies – Policy Department C: Citizens's Rights and Constitutional Rights (European Parliament), 'The US legal system on data protection in the field of

law enforcement – Safeguards, rights and remedies for EU citizens' [2015] Study, 17 <http://www.europarl.europa.eu/RegData/etudes/STUD/2015/519215/IPOL_STU%282015%29519215_EN.pdf> accessed 4 May 2016

Working Party on the Protection of Individuals with regard to the Processing of Personal Data (Article 29 Working Party) documents

- Working Party on the Protection of Individuals with regard to the Processing of Personal Data, 'First orientations on Transfers of Personal Data to Third Countries – Possible Ways Forward in Assessing Adequacy' [1997] Discussion Document WP4 <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/1997/wp4_en.pdf> accessed 28 March 2017
- Working Party on the Protection of Individuals with regard to the Processing of Personal Data, 'Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive' [1998] Working Document WP12 <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/1998/wp12_en.pdf> accessed 18 March 2017
- Working Party on the Protection of Individuals with regard to the Processing of Personal Data, 'Transfers of personal data to third countries: Applying Article 26 (2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers' [2003] Working document WP74 <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2003/wp74_en.pdf> accessed 18 March 2017
- Working Party on the Protection of Individuals with regard to the Processing of Personal Data, 'Setting Forth a Co-Operation Procedure for Issuing Common Opinions on Adequate Safeguards Resulting From "Binding Corporate Rules"' [2005] Working document WP107 <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2005/wp107_en.pdf> accessed 18 March 2017
- Working Party of on the Protection of Individuals with regard to the Processing of Personal Data, 'A common interpretation of Article 26 (1) of Directive 95/46/EC of 24 October 1995' [2005] Working Document WP114 <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2005/wp114_en.pdf> accessed 18 March 2017
- Working Party on the Protection of Individuals with regard to the Processing of Personal Data, 'Opinion 1/2010 on the concepts of "controller" and "processor" [2010] Opinion WP169 <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_en.pdf> accessed 26 April 2017

- Working Party on the Protection of Individuals with regard to the Processing of Personal Data, 'Opinion 7/2010 on European Commission's Communication on the global approach to transfers of Passenger Name Record (PNR) data to third parties' [2010] Opinion WP178 <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2010/wp178_en.pdf> accessed 8 May 2017
- Working Party on the Protection of Individuals with regard to the Processing of Personal Data, 'Opinion 03/2013 on purpose limitation' [2013] Opinion WP203 <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf> accessed 29 March 2017
- Working Party on the Protection of Individuals with regard to the Processing of Personal Data, 'Working Document 01/2016 on the justification of interferences with the fundamental rights to privacy and data protection through surveillance measures when transferring personal data (European Essential Guarantees)' [2016] Working Document WP237 <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2016/wp237_en.pdf> accessed 18 April 2017
- Working Party on the Protection of Individuals with regard to the Processing of Personal Data, 'Opinion 01/2016 on the EU-U.S. Privacy Shield draft adequacy decision' [2016] Opinion WP238 <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2016/wp238_en.pdf> accessed 25 April 2017

European Data Protection Supervisor (EDPS) documents

- European Data Protection Supervisor, 'Opinion on the Proposals for Council Decisions on the conclusion and signature of the Agreement between Canada and the European Union on the transfer and processing of Passenger Name Record data' [2013] Opinion <https://edps.europa.eu/sites/edp/files/publication/13-09-30_canada_en.pdf> accessed 8 May 2017
- European Data Protection Supervisor, 'The transfer of personal data to third countries and international organisations by EU institutions and bodies' [2014] Position paper <https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Papers/14-07-14_transfer_third_countries_EN.pdf> accessed 18 March 2017
- European Data Protection Supervisor, 'Guidance: Security Measures for Personal Data Processing, article 22 of Regulation 45/2001' [2016] Guidance document <https://edps.europa.eu/sites/edp/files/publication/16-03-21_guidance_isrm_en.pdf> accessed 30 March 2017
- European Data Protection Supervisor, 'Opinion on the EU-U.S. Privacy Shield draft adequacy decision' [2016] Opinion 4/2016 <https://edps.europa.eu/sites/edp/files/publication/16-05-30_privacy_shield_en.pdf> accessed 25 April 2017

European Union Agency for Fundamental Rights (FRA)

- European Union Agency for Fundamental Rights (FRA), Council of Europe and Registry of the European Court of Human Rights, *Handbook on European data protection law* (Publications Office of the European Union 2014)
- European Union Agency for Fundamental Rights, *Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU – Mapping Member States' legal frameworks* (Publications Office of the European Union 2015)

Websites

- 'EU Charter of Fundamental Rights' (Website Commission) <http://ec.europa.eu/justice/fundamental-rights/charter/index_en.htm> accessed 5 May 2017
- 'Information society, privacy and data protection' (Website European Union Agency for Fundamental Rights, (FRA)) <http://fra.europa.eu/en/theme/information-society-privacy-and-data-protection> accessed 5 May 2017
- <https://edwardsnowden.com/> (Website Edward Snowden) accessed 6 May 2017
- <https://edwardsnowden.com/2014/01/17/presidential-policy-directive-ppd-28-concerning-signals-intelligence-activities/> (Website Edward Snowden) accessed 26 April 2017
- Data transfers outside of the EU' (Website Commission) <http://ec.europa.eu/justice/data-protection/international-transfers/index_en.htm> accessed 18 March 2017
- 'Model Contracts for the transfer of personal data to third countries' (Website Commission) <http://ec.europa.eu/justice/data-protection/international-transfers/transfer/index_en.htm> accessed 18 March 2017
- 'Binding Corporate Rules' (Website Commission) <http://ec.europa.eu/justice/data-protection/article-29/bcr/index_en.htm> accessed 18 March 2017
- 'BCR Procedure' (Website Commission) <http://ec.europa.eu/justice/data-protection/international-transfers/binding-corporate-rules/procedure/index_en.htm> accessed 18 March 2017
- <https://www.digitalrights.ie/> (Website Digital Rights Ireland) accessed 4 April 2017
- 'Accession of the European Union' (Website ECHR) <http://www.echr.coe.int/Pages/home.aspx?p=basictexts/accessionEU&c> accessed 8 April 2017
- Press Unit of the European Court of Human Rights, 'Factsheet – Mass surveillance', 3 (Website ECHR, December 2016) <http://www.echr.coe.int/Documents/FS_Mass_surveillance_ENG.pdf > accessed 6 April 2017

- European Court of Human Rights, 'Legal summary – Szabó and Vissy v. Hungary' (Hudoc, January 2016) <http://hudoc.echr.coe.int/eng#{"itemid":["002-10821"]}> accessed 6 April 2017
- Office of the Press Secretary of the White House, 'FACT SHEET: Review of U.S. Signals Intelligence' (The White House – President Barack Obama, 17 January 2014) <https://obamawhitehouse.archives.gov/the-press-office/2014/01/17/fact-sheet-review-us-signals-intelligence> accessed 1 May 2017
- 'About the Board' (Website Privacy and Civil Liberties Oversight Board)<https://www.pclob.gov/about-us.html> accessed 3 May 2017
- 'Transfer of Air Passenger Name Record (PNR) Data and Terrorist Finance Tracking Programme (TFTP)' (Website Commission) <http://ec.europa.eu/justice/data-protection/international-transfers/pnr-tftp/pnr-and-tftp_en.htm> accessed 7 May 2017
- 'Terrorist Finance Tracking Program (TFTP) (Website U.S. Department of the Treasury) <https://www.treasury.gov/resource-center/terrorist-illicit-finance/Terrorist-Finance-Tracking/Pages/tftp.aspx> accessed 9 May 2017
- 'Privacy Shield List' (Website Privacy Shield Framework (United States)), <https://www.privacyshield.gov/participant_search> accessed 10 May 2017
- 'Terrorist Finance Tracking Programme' (Website Commission) <https://ec.europa.eu/home-affairs/what-we-do/policies/crisis-and-terrorism/tftp_en> accessed 10 May 2017

Blogs

- 'A simple explanation of how money moves around the banking system' (Richard Gendal Brown) <https://gendal.me/2013/11/24/a-simple-explanation-of-how-money-moves-around-the-banking-system/> accessed 9 May 2017
- 'European Court Opinion: Canada PNR deal cannot be signed' (European Digital Rights (EDRi), 8 September 2016) <https://edri.org/european-court-opinion-canada-pnr-deal-cannot-be-signed/> accessed 8 May 2017
- 'EU-US Privacy Shield review now promised for September' (Privacy Laws & Business, 5 May 2017) <http://www.privacylaws.com/int_enews_5_4_17> accessed 26 April 2017
- 'The Article 29 Data Protection Working Party ("WP29") remain concerned about the recently adopted Privacy Shield as follows from their recent statement dated 1 July 2016" (Stibbe, 13 October 2016) <https://www.stibbe.com/en/news/2016/october/privacy-authorities-remain-concerned-about-the-privacy-shield> accessed 3 May 2017
- De Hert P and Cristobal Bocos P, 'Case of Roman Zakharov v. Russia: The Strasbourg follow up to the Luxembourg Court's Schrems judgment' (Strasbourg Observers, 23 December 2015)

<https://strasbourgobservers.com/2015/12/23/case-of-roman-zakharov-v-russia-the-strasbourg-follow-up-to-the-luxembourg-courts-schrems-judgment/> accessed 6 April 2017

- Hale W, 'United States: Comparison of Requirements Under The Privacy Shield/Safe Harbor Principles' (Mondaq, 26 July 2016) <http://www.mondaq.com/united-states/x/513810/Data+Protection+Privacy/Comparison+Of+Requirements+Under+The+Privacy+ShieldSafe+Harbor+Principles> accessed 29 April 2017
- Johnson T, 'Watchdog board that keeps eye on U.S. intelligence agencies barely functions' (McClatchy DC BUREAU, 7 March 2017) <http://www.mcclatchydc.com/news/nation-world/national/national-security/article136960048.html> accessed 3 May 2017
- Kadial S, 'Surveillance After the USA Freedom Act: How Much Has Changed?' (The Center for Constitutional Rights, 17 December 2015) <http://www.huffingtonpost.com/the-center-for-constitutional-rights/surveillance-after-the-us_b_8827952.html> accessed 2 May 2017
- Lynskey O, 'Tele2 Sverige AB and Watson et al: continuity and radical change' (European Law Blog, 12 January 2017) <http://europeanlawblog.eu/2017/01/12/tele2-sverige-ab-and-watson-et-al-continuity-and-radical-change/> accessed 4 March 2017
- McLaughlin J, 'The U.S. Government's Privacy Watchdog Is Basically Dead, Emails Reveal' (The Intercept, 3 March 2017) <https://theintercept.com/2017/03/03/the-governments-privacy-watchdog-is-basically-dead-emails-reveal/> accessed 3 May 2017
- Petrovas S and Rich CJ, 'Privacy Shield vs. Safe Harbor: A Different Name for an Improved Agreement?' (Morrison Foerster, 3 March 2016) <https://www.mofo.com/resources/publications/privacy-shield-vs-safe-harbor-a-different-name-for-an-improved-agreement.html> accessed 29 April 2017
- Rouse M, 'Definition COMINT (communications intelligence)' <http://whatis.techtarget.com/definition/COMINT-communications-intelligence> accessed 1 May 2017
- Stanley J, 'What Powers Does the Civil Liberties Oversight Board Have?' (American Civil Liberties Union, 4 November 2013) <https://www.aclu.org/blog/what-powers-does-civil-liberties-oversight-board-have> accessed 3 May 2017
- Seth S, 'How The SWIFT System Works' (Investopedia, 5 May 2015) <http://www.investopedia.com/articles/personal-finance/050515/how-swift-system-works.asp> accessed 9 May 2017
- St.Vincent S, 'Did the European Court of Human Rights Just Outlaw "Massive Monitoring of Communications" in Europe?' (Center for Democracy & Technology (CDT), 13 January 2016) <https://cdt.org/blog/did-the-european-court-of-human-rights-just-outlaw-massive-monitoring-of-communications-in-europe/> accessed 9 April 2017

- Vavoula N, 'I Travel, therefore I am a Supsect': an overview of the EU PNR Directive' (FREE Group, 27 October 2016) <https://free-group.eu/2016/10/27/i-travel-therefore-i-am-a-suspect-an-overview-of-the-eu-pnr-directive/> accessed 9 May 2017

Press releases

- Court of Justice of the European Union, 'The Court of Justice declares the Data Retention Directive to be invalid' (Press release, 8 April 2014) <http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054en.pdf> accessed 3 April 2017
- Commission, 'Frequently Asked Questions: The Data Retention Directive' (Memo, 8 April 2014) <http://europa.eu/rapid/press-release_MEMO-14-269_en.htm> accessed 7 April 2017
- Council of the European Union, 'Signature of the EU-Canada agreement on Passenger Name Records (PNR) (Press release, 25 June 2014) <http://www.consilium.europa.eu/en/press/press-releases/2014/06/pdf/signature-of-the-eu-canada-agreement-on-passenger-name-records-(pnr)/> accessed 7 May 2017
- European Parliament, 'MEPs refer EU-Canada air passenger data deal to the EU Court of Justice' (Press release, 25 November 2014) <http://www.europarl.europa.eu/news/en/news-room/20141121IPR79818/meps-refer-eu-canada-air-passenger-data-deal-to-the-eu-court-of-justice> accessed 8 May 2017
- European Parliament, 'Parliament back EU directive on use of Passenger Name Records (PNR)' (Press release, 14 April 2016) <http://www.europarl.europa.eu/news/en/news-room/20160407IPR21775/parliament-backs-eu-directive-on-use-of-passenger-name-records-(pnr)> accessed 8 May 2017
- Commission, 'European Commission launches EU-U.S. Privacy Shield: stronger protection for transatlantic data flows' (Press release, 12 July 2016) <http://europa.eu/rapid/press-release_IP-16-2461_en.htm> accessed 25 April 2017
- Court of Justice of the European Union, 'Advocate General's Opinion in the Request for an Opinion 1/15' (Press release, 8 Septemeber 2016) <https://curia.europa.eu/jcms/upload/docs/application/pdf/2016-09/cp160089en.pdf> accessed 8 May 2017
- Committee on Civil Liberties, Justice and Home Affairs of the European Parliament (LIBE), 'EU-Canada PNR: legal opinion affirms Parliament's privacy concerns' (Press release, 8 September 2016) <http://www.europarl.europa.eu/news/en/news-room/20160908IPR41656/eu-canada-pnr-legal-opinion-affirms-parliament%E2%80%99s-privacy-concerns> accessed 8 May 2017

Newspaper articles

The Guardian

- Glenn Greenwald, 'NSA collecting phone records of millions of Verizon customers daily' *The Guardian* (6 June 2013) <https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order> accessed May 2017
- Glenn Greenwald and Ewen MacAskill, 'NSA Prism program taps in to user data of Apple, Google and others' *The Guardian* (6 June 2013) <https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data> accessed May 2017
- James Ball, 'NSA's Prism surveillance program: how it works and what it can do' *The Guardian* (8 June 2013) <https://www.theguardian.com/world/2013/jun/08/nsa-prism-server-collection-facebook-google> accessed 1 May 2017
- James Ball, 'Edward Snowden NSA files: secret surveillance and our revelations so far' *The Guardian* (21 August 2013) <https://www.theguardian.com/world/2013/aug/21/edward-snowden-nsa-files-revelations> accessed 1 May 2017
- Ian Traynor, 'EU threatens to suspend deal with US on tracking terrorists' funding' *The Guardian* 24 September 2013) <https://www.theguardian.com/world/2013/sep/24/eu-threat-us-data-sharing-terrorist-funding> accessed 9 May 2017

The Washington Post

- Ellen Nakashima, 'NSA's bulk collection of Americans' phone records ends Sunday' *The Washington Post* (27 November 2015) <https://www.washingtonpost.com/world/national-security/nsas-bulk-collection-of-americans-phone-records-ends-sunday/2015/11/27/75dc62e2-9546-11e5-a2d6-f57908580b1f_story.html?utm_term=.1290ae49daa5> accessed 13 May 2017

The New York Times

- Eric Lichtblau and James Risen, 'Bank Data is Sifted by U.S. in Secret to Block Terror' *The New York Times* (23 June 2013) <http://www.nytimes.com/2006/06/23/washington/23intel.html> accessed 9 May 2017

Spiegel Online

- Laura Poitras, Marcel Rosenbach and Holger Stark, 'NSA Monitors Financial World' *Spiegel Online* (16 September 2013) <http://www.spiegel.de/international/world/how-the-nsa-spies-on-international-bank-transactions-a-922430.html> accessed 10 May 2017

Other sources

- EU Co-Chairs of the Ad Hoc EU-US Working Group on Data Protection, 'Report on the Findings of the EU Co-Chairs of the Ad Hoc EU-U.S. Working Group on Data Protection' [2013] point 5 <http://ec.europa.eu/justice/data-protection/files/report-findings-of-the-ad-hoc-eu-us-working-group-on-data-protection.pdf> accessed 1 May 2015
- National Research Council, Division on Engineering and Physical Sciences, Computer Science and Telecommunications Board, Committee on Responding to Section 5(d) of Presidential Policy Directive 28: The Feasibility of Software to Provide Alternatives to Bulk Signals Intelligence Collection, *Bulk Collection of Signals Intelligence: Technical Options*
- European Ombudsman (Emily O'Reilly), 'Use of the title 'ombudsman' in the 'EU-US Privacy Shield' agreement' (European Ombudsman, Letter to Ms Věra Jourová, 22 February 2016) <https://www.ombudsman.europa.eu/resources/otherdocument.faces/en/64157/html.bookmark> accessed 3 May 2017
- Charles Doyle, 'Administrative Subpoenas in Criminal Investigations: A Brief Legal Analysis' (CRS Report for Congress, 17 March 2006), summary <https://fas.org/sgp/crs/intel/RL33321.pdf> accessed 4 May 2017
- European Union Committee, *The EU/US Passenger Name Record (PNR) Agreement* (HL 2006-07, 108)
- U.S. Customs and Border Protection (CBP) (U.S. Department of Homeland Security (DHS)), 'U.S. Customs and Border Protection Passenger Name Record (PNR) Privacy Policy' (2013) 1<https://www.cbp.gov/sites/default/files/documents/pnr_privacy.pdf> accessed 7 May 2017
- Commissie voor de bescherming van de persoonlijke levenssfeer, 'Advies betreffende de doorgifte van persoonsgegevens door de CVBA SWIFT ingevolge de dwangbevelen van de UST (OFAC)' (2006) Advies Nr 37/2006 <https://www.privacycommission.be/sites/privacycommission/files/documents/advies_37_2006_0.pdf> accessed 9 May 2017
- Terrorist Finance Tracking Program – Representations of the United States Department of the Treasury [2007] OJ C166/18
- General Secretariat of the Council of the EU, 'EU-US agreement on the processing and transfer of financial messaging data for purposes of the US Terrorist Finance Tracking Programme (TFTP) – Questions and Answers' (Information note, November 2009) <https://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/jha/111559.pdf> accessed 10 May 2017

ANNEX: NEDERLANDSTALIGE SAMENVATTING

217. De voornaamste onderzoeksvraag van deze thesis is de volgende: waarborgen de Verenigde Staten, op grond van hun nationale wetgeving of hun internationale verbintenissen, en meer in het bijzonder op grond van het EU-VS-privacyschild, een passend beschermingsniveau met het oog op de bescherming van de persoonlijke levenssfeer en de fundamentele vrijheden en rechten van personen in het licht van de Europese databeschermingsstandaarden? Is de gegevensoverdracht van persoonsgegevens naar de V.S. voor commerciële doeleinden op basis van het EU-VS-privacyschild bijgevolg legitiem?

218. Om deze vraag te kunnen beantwoorden wordt eerst onderzocht wat wordt bedoeld met een 'passend beschermingsniveau'. Vervolgens worden de Europese databeschermingsstandaarden uiteengezet en geanalyseerd. Deze standaarden spruiten in belangrijke mate voort uit enkele recente arresten van het Hof van Justitie van de Europese Unie en het Europees Hof voor de Rechten van de Mens. Daarbij is vooral de vaststelling dat persoonsgegevens niet in *bulk* verzameld mogen worden om daarna gebruikt te worden voor inlichtingen- en rechtshandhavingsdoeleinden van groot belang.

219. Om de eerste vraag meer in perspectief te kunnen plaatsen, wordt onderzocht in welke mate deze rechtspraak een effect heeft op andere EU instrumenten zoals de PNR akkoorden, de PNR Richtlijn en de TFTP overeenkomst met de Verenigde Staten. Daarenboven worden ook zogenaamde 'standard contractual clauses' ((S)CCS) en 'binding corporate rules' (BCRs) onder de loep genomen.

220. Na uitvoerig onderzoek moet de eerste onderzoeksvraag evenwel negatief beantwoord worden: noch de privacyschild Beginselen, noch de beperkingen aangaande de inmengingen van de Amerikaanse overheid in de uitoefening van privacy- en databeschermingsrechten van Europese datasubjecten voldoen aan de Europese standaarden. Dit betekent dat de Verenigde Staten dus geen passend gegevensbeschermingsniveau waarborgen op grond van het EU-VS-privacyschild en dat dit schild bijgevolg niet kan worden gebruikt als basis voor vrij, commercieel dataverkeer van de Unie naar de Verenigde Staten.

221. Bovendien is gebleken dat de *bulk* verzameling van PNR gegevens, in het licht van de gezegde rechtspraak, ook niet kan worden gehandhaafd. Hetzelfde geldt voor de *bulk* gegevensoverdracht van financiële gegevens naar het Amerikaans ministerie van Financiën op basis van het TFTP akkoord.

Tot slot is gebleken dat (standard) contractual clauses en binding corporate rules worden gebruikt voor gegevenstransfers naar een land waar de overheid de doorgegeven persoonsgegeven op een onvoldoende passende manier beschermt. (S)CCs en BCRs kunnen immers enkel het gebrek aan een passend gegevensbeschermingskader in de private sector van een derde land remediëren.