# ΕΘΝΙΚΟΝ ΚΑΙ ΚΑΠΟΔΙΣΤΡΙΑΚΟΝ ΠΑΝΕΠΙΣΤΗΜΙΟΝ ΑΘΗΝΩΝ

## ΣΧΟΛΗ ΟΙΚΟΝΟΜΙΚΩΝ & ΠΟΛΙΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ
## ΤΜΗΜΑ ΕΠΙΚΟΙΝΩΝΙΑΣ & ΜΕΣΩΝ ΜΑΖΙΚΗΣ ΕΝΗΜΕΡΩΣΗΣ

**ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ ΣΤΗΝ «ΕΠΙΚΟΙΝΩΝΙΑ ΚΑΙ ΤΑ ΜΕΣΑ ΜΑΖΙΚΗΣ ΕΝΗΜΕΡΩΣΗΣ»**
**ΚΑΤΕΥΘΥΝΣΗ: ΔΗΜΟΣΙΟΓΡΑΦΙΑ ΚΑΙ ΝΕΑ ΜΕΣΑ**


**Θέμα Διατριβής**

# The Adequacy of the EU – U.S. Privacy Shield, Particularly in the Social Networking Platforms


**Σπυρίδων Συρράκος**
(Α.Μ 9983201535011)


*Διπλωματική εργασία που κατατίθεται ως μέρος των απαιτήσεων του Προγράμματος Μεταπτυχιακών Σπουδών στην Επικοινωνία και τα Μέσα Μαζικής Ενημέρωσης*

Επιβλέπων Καθηγητής
**Αθανάσιος Τσεβάς**

**ΑΘΗΝΑ, Φεβρουάριος 2017**

# The Adequacy of the EU – U.S. Privacy Shield, Particularly in the Social Networking Platforms

*Στην οικογένειά μου*

# LIST OF CONTENTS

# INTRODUCTION

The aim of this dissertation is to answer one specific question: Does the new Privacy Shield Agreement guarantee in an adequate way the rights of EU citizens as far as the security of their personal data is concerned? Consequently, can the U.S. level of data protection be characterised as adequate, essentially equivalent to the European level of data protection? An answer to these questions cannot be considered for granted, since the field of data protection is constantly reshaped due to the rapid technological changes. At the same time, the dissertation offers a comparative and explanatory analysis of the EU and U.S. data protection systems, with regard to transborder data flows and other essential elements which will help the reader to get a better understanding of the relevant mechanisms. It may be true that the crucial topic of international data transfers, or, to be exact, data transfers from the European Union to the United States, is examined under a legal angle, however the reason behind the selection of this particular topic remains the deeper meaning of data transfers for many aspects of the socio – economic life, one of which refers to the omnipotent social networking platforms and the implications of their use.

Chapter 1 provides some useful insight into the general meaning of the notion of data and the importance they hold for the effective functioning of our societies. Moreover, general information are given about the meaning of international data transfers and the regimes, previous and current, which regulate the issue of the transfer of personal data from the European Union to the United States. The mission of Chapter 2 is to trace the essential legal guarantees of the European data protection framework. This task cannot be considered as simple since it demands the assessment of a vast range of mechanisms and principles of the EU legal order, taking into account multiple European legal instruments of the primary and secondary law, the case – law of the Court of Justice of the European Union and the practice of the implementation of these principles and rules. Special reference is made to the case of the social networking platforms regarding general legal issues on their functioning in the context of the information society. The last chapter, Chapter 3, attempts to assess the adequacy of the EU – U.S. Privacy Shield Agreement,

bearing, at the same time, in mind the European legal standards which must be respected whatsoever. Furthermore, it has been considered necessary to examine in a thorough basis some basic pillars of the U.S. legislation concerning the important issue of the access of the U.S. public authorities to EU citizens' data in order to assess the 'essentially equivalent' of the U.S. legal order. It is crucial to underline that the adequacy of the Privacy Shield Agreement is inextricably linked to the adequacy of the U.S. level of data protection, compared to the European level, therefore a detailed assessment of the Privacy Shield per se and relevant provision of the U.S. legal system was necessary. What is more, in Chapter 3 there is a special reference to the social networking platforms, and, more precisely, to Facebook, since Facebook has been the main protagonist of the *Schrems* case and constitutes the most popular social media platform worldwide. The adequacy of the Privacy Shield Agreement, as far as the case of the social networking platforms is concerned, will have to be assessed on the basis of the conclusion about the adequacy of the Privacy Shield in general cases.

It should be noted that this particular issue under study is subject to constant changes since the CJEU decisions and the EU and U.S. legislative measures shape the data protection field in an unprecedented way, hence there is no established bibliography on the issue of the Privacy Shield, which may be found as inadequate in the future and be invalidated. The reference system of this dissertation follows the Oxford University Standard for the Citation of Legal Authorities, due to its legal nature. I would also like to express my gratitude to Professor Athanassios Tsevas for his support and guidance during the whole period that was needed for me to write the dissertation.

# 1 THE CONCEPTUALISATION OF INTERNATIONAL DATA TRANSFERS

## A. The Role of Data in the Modern Societies

Data constitute the raw material of which information and knowledge are composed. One main characteristic of data is the multitude of the produced forms they can take, e.g. numbers, characters, symbols or, simply, bits. They usually are representative of a specific meaning (e.g. data related to one's location), or they can be implied, or derived from other data. They can either be recorded and stored in analogue form, or be encoded in digital form. The value of raw data is extremely essential, for they are the building block of each and every analysis carried out by individuals, private organisations or public authorities in an attempt to reach a specific aim and, ultimately, to change the world for the better. The data, in the form of abstracted elements, are linked and transformed into information through the procedure of the processing and organization, and, subsequently, information becomes organized through the analysis and interpretation and is characterized as knowledge, which, in its turn, leads to wisdom through the application of this knowledge[1].

Personal data constitute indispensable components of the global economy of the 21st century, contributing to the much-expected economic growth. It is a common fact that individuals, private organizations and governments are involved in an endless fight over the control of personal data[2], the processing of which increases dramatically in the contemporary societies, as a result of the technological developments. This special interest for the personal data is justified by their value as a commodity. For example, the existence and the functioning of the social media giant Facebook are solely based on the soaring

[1] Rob Kitchin, *The Data Revolution: Big Data, Open Data, Data Infrastructures and their Consequences* (1st edn, SAGE Publications, 2014) at 9 – 10.
[2] Orla Lynskey, *The Foundations of EU Data Protection Law* (1st edn, OUP, 2015) at 1.

profit[3] of the company stemming from the display of advertisements on the users' news feed. Facebook and Google constitute the two major companies ruling over the advertising market[3], a phenomenon which could potentially imply a negative impact on the functioning of free competition. The impressive growth of the social networking platforms is closely linked to their popularity, since approximately 2.31 billion people are social media users around the world[4], a number which does not cease to increase as the Internet becomes an essential element of our daily lives. There is no doubt about the fact that the international data transfers have risen at an exponential rate. Due to the importance and the extensive use of personal data, it is natural that issues related to the protection of the privacy of individuals and the security of their personal information would emerge.

There has been an alteration over the years around the meaning of the international data transfers. As Christopher Kuner notes[5], in the past the meaning of this term was mostly connected to the exchange of company administrative information, while in the contemporary era the transborder data transfers are not limited to information of such nature, as they include both legal entities and natural persons who communicate via social networking platforms, as well as other means, with the aid of the technology. The term Web 2.0 refers to the power given to the Internet users to generate their own content through their participation in the online social networking platforms. Interactivity constitutes the keyword which signifies the evolution from Web 1.0 (whose main developments were the internet forums and personal websites) to Web 2.0, where the absence of a gatekeeper facilitates the creation of user – generated content[6]. It should be borne in mind that the globalization, especially in economic terms, added to the technological evolutions, created the need for international transfer of personal data, holding great economic value. Beyond this financial aspect, the international data transfer can prove to be a valuable ally due to its social aspect, since it can foster the communication and could bring political changes. New phenomena, such as the cloud computing,

[3] See the Wall Street Journal, 'Facebook Profit Soars, but Growth Concerns Emerge', 2 November 2016, http://www.wsj.com/articles/facebook-profit-jumps-sharply-1478117646 accessed 26 November 2016.
[4] http://wearesocial.com/uk/special-reports/digital-in-2016, accessed 26 November 2016.
[5] Christopher Kuner, *Transborder Data Flows and Data Privacy Law* (1st edn, OUP, 2013) at 2.
[6] Andrew Murray, *Information Technology Law: The Law and the Society* (3rd edn, OUP, 2016) at 114 – 116.

constitute a more complex dimension, enabling the realization of data transfers in unprecedented ways. The importance of the data transfers is apparent by the fact that in the 21st century there is a developing cooperation between States, as well as between public authorities and private organisations for a variety of purposes, such as law enforcement and prevention of crimes, marketing and advertising purposes, or commercial growth.

## B. Data Transfers from the European Union to the United States: An Introduction.

As it will be elaborated in Chapter 2, European data protection law lays down that international data transfers from the European Union to third countries may occur only if the third country provides for an 'adequate level of protection' with respect to individuals' fundamental rights and freedoms. The assessment and verification of the adequacy of the third country's level of protection are carried out by the European Commission whose adequacy decisions constitute the legal basis for data transfers to third countries. Decision 2000/520[7] was adopted by the European Commission on 26 July 2000. According to this Decision, known as the Safe Harbour Decision, the United States ensure an adequate level of protection, within the meaning of the EU Data Protection Directive, allowing, thus, the transfer of personal data from the European Union to the United States. However, this finding does not constitute a general statement about the data protection law regime of the United States, as a whole, since the adequacy applies only for those organisations which would voluntarily subscribe to the Safe Harbour Principles. The U.S. Department of Commerce (DoC) undertook the responsibility for the definition of the Safe Harbour Principles, included in the Decision 2000/520. An organization may participate only if it has publicly disclosed its commitment to comply with the Safe Harbour Principles (art 1 – 2a), followed by self – certification.

[7] Commission Decision 2000/520/EC of 26 July 2000 pursuant to Directive 95/46/EC on the adequacy of the protection provided by the safe harbor privacy principles and related frequently asked questions issued by the US Department of Commerce, OJ 2000 L 215/7.

The crucial issue of data transfers from the European Union to the United States is closely related to the *Maximilian Schrems v. Data Protection Commissioner* decision[8]. The decision – landmark was issued by the Court of Justice of the European Union (CJEU) on 6 October 2015 and its great importance lies with the fact that it invalidated the Decision of the European Commission known as the EU – US Safe Harbour Agreement, which had found that the level of protection guaranteed by the USA had been adequate, allowing, thus, the cross – border data transfer. Maximillian Schrems had lodged a complaint with the Irish Data Protection Commissioner in June 2013 requesting the termination of each and every transfer of his personal data by Facebook Ireland to the United States, claiming that Facebook Ireland, which is the data controller responsible for the processing of his personal data, had not been entitled to transfer any longer his personal data to the United States on the legal basis of the Safe Harbour Framework in the light of the generalized access of the US authorities to users' personal data, as the Snowden revelations have pointed out. The Irish Commissioner rejected his complaint arguing that the Safe Harbour decision could not be challenged, and, therefore, Schrems sought the judicial review of the Irish Commissioner's decision before the Irish High Court, which decided that the complaint of Maximillian Schrems challenged the adequacy of the Safe Harbour Framework in the light of the revelations by Edward Snowden, hence the CJEU had to issue its judgment on this particular issue. The invalidation of the Safe Harbour Agreement by the CJEU was based, inter alia, on the shocking revelations of Edward Snowden, which caused great distrust especially among the European citizens about the safety of their own personal data. These revelations occurred in 2013 and they disclosed to the public the existence of several programs, run secretly by the intelligence agencies of the United States, notably the PRISM program, whose sole purpose was the bulk collection, processing and storage of internet communications data of US and EU citizens, whose data were transferred to the USA from technology companies, such as Facebook, Google and Apple, without any significant differentiation[9]. The revelations of Edward Snowden

[8] Case C-362/14 *Maximillian Schrems v Data Protection Commissioner* (Grand Chamber, 6 October 2015).
[9] The Edward Snowden's revelations have been the main story featured in many articles of the global press, for instance see Barton Gellman and Laura Poitras, U.S., 'British intelligence mining data from nine U.S. Internet companies in broad secret program', 7 June 2013, https://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-

became one of the main arguments of Maximilian Schrems, who claimed in his complaint that the transfer of personal data of European citizens by Facebook Ireland ltd to the United States under the Safe Harbour Decision is in fact endangered by the generalized access of the US intelligence agencies to US and EU citizens' personal data. It should be noticed that it is no coincidence that the invalidation of the Safe Harbour Decision was brought by the actions of two persons, Maximilian Schrems and Edward Snowden. The symbolism of this fact conveys the inability, or, perhaps, the deliberate absence of major actions, due to the existence of socio – economic interests, of the national and international public authorities to effectively guarantee the protection of individuals' fundamental rights[10].

Certainly, the decision of the CJEU has been appraised for the fact that it officially acknowledged the unlawfulness of the transfer of European citizens' personal data to the United States due to the existence of mass surveillance mechanisms implemented by the U.S. intelligence agencies, however, at the same time, the decision has been criticized on the premise that it reduces the importance of the transatlantic data flows which are considered of great importance for the international commerce and the enhancement of the digital economy[11]. The replacement of the former Safe Harbour Agreement had been, thus, a necessity. In February 2016, it was announced that a new agreement between the EU and the USA would be necessary in order for these transfers to be legitimized. Indeed, on 12 July 2016, a new decision was adopted by the European Commission, the 'E.U. – U.S. Privacy Shield'[12]. The new Commission Decision seeks to strengthen, on the one hand, the international data transfers from the European Union to the United States on a new legal basis which will not be declared invalid, like the Safe Harbour, and, on the other hand, enhance the rights of the European citizens with the aid of robust mechanisms which will ensure the effective protection of their personal data. The adequacy of the Privacy Shield will be examined in Chapter 3 with the aid of the European legal standards which will be

companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html?utm_term=.907cc3e8f9ee accessed 02 February 2017.

[10] Loïc Azoulai and Marijn van der Sluis, 'Institutionalizing personal data protection in times of global institutional distrust: *Schrems*', (2016) 53 Common Market Law Review at 1344.

[11] Yann Padova, 'The Safe Harbour is invalid: what tools remain for data transfers and what comes next?' (2016), 6 International Data Privacy Law at 140.

[12] Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU – U.S. Privacy Shield, OJ 2016 L 207/1.

analysed in Chapter 2 and be used as the model for the definition of the notion of the adequacy of the level of protection of a third country, and the adequacy of the Commission Decision regarding the data transfer to this third country.

# 2 A BRIEF ASSESSMENT OF THE EUROPEAN DATA PROTECTION LAW

## A. General European Standards to Data Processing

### 1. Sources of the Legal Protection of the Fundamental Rights to Privacy and Personal Data

The primary law of the European Union consists[13] of the Treaty on European Union (TEU)[14], the Treaty on the Functioning of the European Union (TFEU)[15], various Protocols and Annexes attached to the two Treaties, the Charter of Fundamental Rights of the European Union[16], as well as the general principles of the European Union law, as these have been shaped in the jurisprudence of the Court of Justice of the European Union, and judge – made principles (such as the principle of supremacy or the principle of direct effect). All these sources share the same legal value, therefore they should be regarded as a whole in terms of the primary law of the European Union. According to Article 6 (1) of the TEU, the Charter of Fundamental Rights of the European Union has the same legal value as the Treaties. The Charter was adopted in 2000, without legal binding value, since at that time it merely constituted a political declaration by the Council, Commission and Parliament. The secondary law of the European Union is composed of regulations, directives and decisions adopted by the EU institutions pursuant to the authorization granted under the EU primary law.

Before the coming into force of the Charter, it was the main task of the CJEU to identify and acknowledge the existence of fundamental rights within the European Union.

[13] Alan Dashwood, Derrick Wyatt and others, *European Union Law* (6th edn, Hart Publishing, 2011) at 23 – 37.
[14] Consolidated Version of the Treaty on European Union [2010] OJ C83/13.
[15] Consolidated Version of the Treaty on the Functioning of the European Union [2010] OJ C83/47.
[16] Charter of Fundamental Rights of the European Union [2000] OJ C364/01 and [2010] OJ C83/389.

In 1999, the Cologne European Council expressly emphasized in its Conclusions the need for the concentration of all the fundamental rights applicable in the level of European Union in a Charter, in order for the protection of these rights to become more evident to the European citizens[17]. Before the explicit protection of the fundamental rights in the EU level by the EU Charter, no specific provision existed in any Treaty about this issue. It was the CJEU which implicitly enshrined the protection of fundamental human rights in its case – law. The case of *Stauder*[18] is an example of the early acknowledgement of the fundamental rights in the EU level. The CJEU recognized the protection of fundamental rights within the EU, even if there was no explicit provision in the Treaties, considering them as part of the general principles of Community law[19]. This declaration became more evident in the case of *Internationale Handelsgesellshaft*[20], where the CJEU reaffirmed the statement that fundamental rights belong to the general principles of the Community, while it added that the protection of these fundamental rights is inspired by the constitutional traditions common to the Member States and must be safeguarded within the level of the Community[21]. In fact, in the Case of *Nold*[22], the CJEU extended the inspiration regarding the protection of the fundamental rights to international treaties for the protection of human rights on which the Member States have collaborated or of which they are signatories[23], a statement which implicitly refers to the European Convention of Human Rights (ECHR).

The Treaty of Lisbon[24] is the treaty which brought major changes to the protection of fundamental rights, reshaping in a fundamental manner the European data protection legal framework. Unlike in the past where an explicit legal basis for the individuals' right for the protection of their personal data was nowhere to be found[25], the Lisbon Treaty

[17] Cologne European Council, 'Conclusions of the Presidency', 3 – 4 June 1999, para 44.
[18] Case 29/69, *Stauder v City of Ulm* [1969] ECR 419.
[19] *Stauder* (n 18), para 7: 'Interpreted in this way the provision at issue contains nothing capable of prejudicing the fundamental human rights enshrined in the general principles of Community Law and protected by the Court'.
[20] Case 11/70, *Internationale Handelsgesellshaft mbH v Einfuhr- und Vorratsstelle für Getreide und Futtermittel* [1970] ECR 1125.
[21] *Internationale Handelsgesellshaft* (n 20), para 4.
[22] Case 7/73, *Nold v Commission* [1974] ECR 491.
[23] Nold (n 22), para 13.
[24] Treaty of Lisbon Amending the Treaty on European Union and the Treaty establishing the European Community [2007] OJ C306/01.
[25] The adoption of Directives 95/46/EC and 2002/58/EC was based on the general provision of Article 95 EC Treaty (which is Article 114 TFEU) with regard to the establishment and functioning of the internal market.

introduced such an explicit legal provision in Article 16 of the Treaty of the Functioning of the European Union (TFEU). According to Article 16 TFEU:

> '1. Everyone has the right to the protection of personal data concerning them.
>
> 2. The European Parliament and the Council, acting in accordance with the ordinary legislative procedure, shall lay down the rules relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies, and by the Member States when carrying out activities which fall within the scope of Union law, and the rules relating to the free movement of such data. Compliance with these rules shall be subject to the control of independent authorities.
>
> The rules adopted on the basis of this Article shall be without prejudice to the specific rules laid down in Article 39 of the Treaty on European Union.'

Furthermore, the enshrinement, for the first time, of the separate, from the right to privacy of Article 7, right for protection of one's personal data in Article 8 of the EU Charter of Fundamental Rights is considered to be a step of utmost importance towards the enhancement of the EU data protection mechanism. Articles 7 and 8 specify that:

> 'Article 7: Respect for private and family life
>
> Everyone has the right to respect for his or her private and family life, home and communications.
>
> Article 8*:* Protection of personal data
>
> 1. Everyone has the right to the protection of personal data concerning him or her.
>
> 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.

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

Despite these changes concerning the European primary law, the majority of the EU data protection rules stem from the secondary European law. The most important European legal instrument is the EU Data Protection Directive 95/46/EC[26], adopted in 1995. The Directive is legally binding for the 27 EU Member States and the three EEA member countries. However, the effective regulation of the data protection area cannot solely rely on one and only Directive. Therefore, the need for a more effective protection of individuals' rights with respect to processing of their personal data led to the adoption of the E – Privacy Directive 2002/58/EC[27], which acts as lex specialis and applies to special cases concerning issues which arise in the electronic communications sector, wherever the provisions of Directive do not provide for sufficient protection. It has to be noted that Directive 2002/58/EC has been amended by Directive 2009/136/EC[28]. Directive 2006/24/EC[29] referred to the retention of personal data in publicly available electronic communications services or public communications networks, however it was invalidated by the CJEU in the *Digital Rights Ireland* case[30]. Finally, Regulation EC No. 45/2001[31] establishes a complementary data protection legal framework referring to data processing by institutions and bodies of the European Union. It is crucial to highlight that the Data

[26] 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.
[27] 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.
[28] Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws [2009] OJ L337/11.
[29] 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 networks and amending Directive 2002/58/EC [2006] OJ L 105/54.
[30] Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others* and *Kärntner Landesregierung and Others* [2014] OJ C175/6.
[31] 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.

Protection Directive 95/46/EC will be replaced by the General Data Protection Regulation (GDPR)[32] which, along with Directive 2016/680[33], aims to strengthen the protection afforded in European level in the data protection area and safeguard more effectively the right to personal data and privacy of the European citizens. The GDPR is due to enter into application on 25 May 2018 without the need to be transposed by the EU Member States due to its legal nature as a Regulation.

It should be noted that a key element of the European data protection system is the fact that it lays down an omnibus EU regime[34] which covers both public and private actors, is characterized by the neutrality of its rules, and its application is safeguarded by independent supervisory authorities. In spite of the horizontal character of the EU data protection legislation, there is still a distinction among EU primary and secondary legislation regarding the data processing for Common Foreign and Security Policy (including Police and Judicial Cooperation), and the data processing for other purposes. This distinction is affirmed by Article 16 of TFEU, which refers to Article 39 of the Treaty on European Union (TEU), imposing the obligation of the adoption of a decision by the Council for the processing of personal data for CFSP matters. In addition to 39 TEU, Declaration 21[35] of the Lisbon Treaty acknowledges the need for the existence of specific rules for the protection of personal data in the area of judicial cooperation in criminal matters and police cooperation. This distinction is also present in the new reform package of the data protection, where the Directive is applicable only to data processing for law enforcement purposes.

The individuals' right to privacy is enshrined in international legal instruments as well. The European Convention on Human Rights (ECHR) constitutes an international

[32] 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.
[33] Directive 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.
[34] Orla Lynskey, *The Foundations of EU Data Protection Law* (1st edn, OUP, 2015) at 15.
[35] Declaration on the protection of personal data in the field of judicial cooperation in criminal matters and police cooperation annexed to the final act of the intergovernmental conference that adopted the Treaty of Lisbon [2008] OJ C115/345.

treaty drafted by the Council of Europe and its objective is the protection of the fundamental rights and freedoms in Europe. The rights to privacy and data protection are enshrined in Article 8 which stipulates that:

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

Article 12 of the United Nations Universal Declaration of Human Rights of 1948[36] and Article 17 of the International Covenant on Civil and Political Rights[37] expressly forbid any arbitrary interferences with one's privacy and enshrine the right to the protection of it. However, the only legally binding international instrument that is dedicated to data protection is Convention No 108[38] which is a Council of Europe data protection convention opened for signature in 1981. Its main objectives are the protection of the individuals against abuses related to processing of their own personal data, as well as the promotion of the free transborder data flows. It should be noted that all EU Member States have ratified Convention No 108.

[36] Universal Declaration of Human Rights (adopted 10 December 1948 UNGA Res 217 A(III) (UDHR) art 12.
[37] International Covenant on Civil and Political Rights (adopted 16 December 1966, entered into force 23 March 1976) 999 UNTS 171 (ICCPR) art 17.
[38] Council of Europe, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data ETS No 108, 28.I.1981: http://www.conventions.coe.int/Treaty/EN/Treaties/Html/108.htm accessed on 13 November 2016.

## 2. Unlocking the Meaning of Personal Data. Right to Privacy and Right to Personal Data

The official definition of the term 'personal data' is enshrined in Article 2 (a) of the Directive 95/46/EC. Personal data are information which are related to an identified, or at least, identifiable person, called the data subject. An identified person is the one that can be distinguished from other people, while an identifiable person, according to Article 2 (a) is the person who can be identified, directly or indirectly, with regard to an identification number or factors that relate to the physical, physiological, mental, economic, cultural or social identity. The last sentence implicitly refers to the meaning of 'indirectly' identifiable person, suggesting that in this case the identification may take place only with the combination of information related to these factors[39]. It should be noted that the CJEU, in the *Lindqvist*[40] case, considered the name of a person, the telephone coordinates, as well as information about the working conditions or hobbies[41] as personal data, while in *Satamedia*[42] the CJEU explicitly included in the notion of personal data the total amount of one's income[43]. Generally, it can be concluded that the definition given by the Directive is relatively broad. The Article 29 Working Party, in its opinion on the concept of personal data, has affirmed[44] this observation, stipulating that the notion of personal data encompasses objective and subjective information related to a person, concerning not only their private of family life, but also any kind of activities that this person is involved in.[45] The meaning of the processing of personal data, as it is explained in Article 2 (b) encompasses any operation, or set of operations, upon personal data, namely the collection, the storage, the retrieval, the transmission and dissemination or the erasure of personal data, as well as other operation referred in the abovementioned provision. It should be noted that, according to the wording of the Directive, it is possible for the processing of personal data to be realized by automatic means, therefore information stored in a computer

[39] Article 29 Working Party, 'Opinion 4/2007 on the concept of personal data' (WP 136, 20 June 2007) at 13.
[40] Case C-101/01 *Bodil Lindqvist* [2003] ECR I – 12971.
[41] *Lindqvist* (n 40), para 24.
[42] Case C-73/07 *Tietosuojavaltuutettu v. Satakunnan Markkinapörssi OY, Satamedia* [2008] ECR I – 09831.
[43] *Satamedia* (n 42), para 35.
[44] Article 29 Working Party (n 39) at 6.
[45] Article 29 Working Party (n 39), at 6 – 7.

memory are considered to be personal data. The existence of two different actors is essential for the comprehension of data protection law; the 0controller and the processor. The controller (Article 2 (d)) is the natural or legal person or authority entitled to determine the terms and the means of the processing of personal data, while the processor (Article 2 e)) is the natural or legal person or authority who processes the personal data on the controller's account.

Regarding the nature of the rights to privacy and personal data, the fact that the EU Charter proceeds to the distinguishment of the right to respect for private and family life, enshrined in Article 7, from the right to protection of personal data, enshrined in Article 8, does not entail that these rights are not related. In fact, there is an inextricable link between the right to privacy and the right to personal data, which has been affirmed in the *Schecke*[46] case. It should be made reference to the attempt of the illustration of this connection between them with the aid of the notion of informational self – determination. Its roots can be found within the jurisprudence of the Federal Constitutional Court of Germany[47] (Bundesverfassungsgericht) and it is based on the idea that any person has the right of self – determination, in order to decide whether they should act or not upon their personal data (e.g. disclosure, dissemination etc.), stemming from the person's dignity as a member of the democratic society[48]. However, Kranenborg[49] contends that this notion is not sufficient enough for the two rights to be considered as one, due to the fact that the notion of consent is important in the EU legal framework, but not the sole legitimate ground for the lawful data processing. It is no mere coincidence that the EU Charter enshrines the two rights in two separate articles, meaning that even if they do share a deeper connection, this does not entail that they can be regarded as the one and the same right[50]. Generally, the issue of the

[46] Joined Cases C-92/09 and C-93/09 *Volker und Markus Schecke and Hartmut Eifert* [2010] ECR I – 11063, para 47.
[47] There are cases where, instead of the term 'informational self – determination', the term 'individual right to protection from data processing' is also apparent in the Jurisprudence of the Bundesverfassungsgericht. For a more specific and complete analysis, see Athanassios Tsevas, *Προσωπικά Δεδομένα και Μέσα Ενημέρωσης (Personal data and media)* (1st edn, Nomiki Vivliothiki, 2010) at 75.
[48] Athanassios Tsevas (n 47) at 76.
[49] Herke Kranenborg, 'Interpretation of Article 8' in Steve Peers, Tamara Hervey and others, *The EU Charter of Fundamental Rights: A Commentary* (1st edn, Hart Publishing, 2014) at 229.
[50] This observation has also been shared by the Article 29 Working Party, which in its Opinion 4/2007 on the concept of personal data (WP136, 20 June 2007) at 7, has expressed the opinion that the right to personal data is an autonomous one, going beyond the protection of the broad concept of the right to respect for private and family life.

specification of the characteristics of the correlation between the right to privacy and the right to personal data is a complex one, which accounts for the proposal of various models[51]. However, it would be reasonable to suggest that the two rights may be independent, since the right to personal data serves a number of purposes that the right to privacy does not, and vice – versa[52], nonetheless, this cannot mean that the rights are totally different between them, as it has already been elaborated.

## 3. Fundamental Principles Enshrined in Directive 95/46/EC

The main objectives of the Directive 95/46/EC are laid down in Article 1. Firstly, the Data Protection Directive aims at ensuring that the Member – States protect the fundamental rights and freedoms of natural persons, with particular reference to the right to privacy in the context of the processing of personal data[53], and, secondly, it forbids any restrictions and prohibitions, on behalf of the State – Members, which could undermine the free flow of data[54]. These objectives have already been emphasized in Recital 3 of the Preamble of the Directive as well. Thus, the Directive is not solely focused on the regulation of the functioning of the internal market, since it considers, as well, that the effective protection of the individuals' rights and freedoms is a necessary condition for the attainment of this objective[55]. Article 3 (1) defines the Directive's scope, specifying that 'the Directive shall apply to the processing of personal data wholly or partly by automatic means, and to the processing otherwise than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system'. Paragraph 2 of Article 3 reports two exemptions from the general application of the Directive. The first one refers to processing operations which concern public security, defence, State security (including the economic well – being of the State when the processing operation relates to State security matters) and activities in the area of criminal law[56], while the second one is

[51] See Orla Lynskey, *The Foundations of EU Data Protection Law* (1st edn, OUP, 2015) at 94 – 106.
[52] Lynskey (n 51) at 103.
[53] Data Protection Directive Article 1(1).
[54] Data Protection Directive Article 1(2).
[55] Athanassios Tsevas (n 47) at 108.
[56] Data Protection Directive, Article 3 (2).

connected with the processing by a natural person in the course of a personal or household activity[57].

*(i) Data Quality Principles*

The principles relating to data quality are provided for by Article 6 of the Directive and are considered to be one of the fundamental cornerstones of the European data protection law. Firstly, the processing of personal data has to be carried out fairly and lawfully[58]. The understanding of the fair and lawful processing is linked[59] with the content of Article 52 (1) of the Charter, which, generally, sets the three fundamental conditions for the justification of limitations on the exercise of rights and freedoms enshrined in the Charter, as well as the similar conditions set in ECHR Article 8(2). As far as the part of the fairness of the processing is concerned, transparency constitutes a sine qua non condition which entails the obligation of the data controller to keep the data subjects fully and constantly informed with regard to the exact procedure which is followed during the processing of their personal data[60]. It is crucial that the data controllers should be able to offer effective safeguards, in order for the data subjects to believe and honour this trust[61]. Transparency is inevitably linked to the idea of clarity about what has happened, what is happening and what will happen[62], therefore it constitutes an essential component of the fair processing. Articles 10 and 11 of the Directive are the core of the transparency principle and they refer to the importance of providing, on behalf of the controller, the proper information to the data subjects about the identity of the controller, the purposes of the processing and further information related to the procedure to be followed and the data subjects' rights, whether the data have been collected from him or not.

The collection of personal data has to be made for specified, explicit and legitimate purposes, while the further processing, in an incompatible way with these purposes, is not

[57] Data Protection Directive Article 3 (2).
[58] Data protection Directive, Article 6 (1a).
[59] European Union Agency for Fundamental Rights, 'Handbook on European data protection law', April 2014 , http://www.echr.coe.int/documents/handbook_data_protection_eng.pdf accessed 27 November 2017, at 62.
[60] European Union Agency for Fundamental Rights (n 59) at 74.
[61] European Union Agency for Fundamental Rights (n 59) at 74.
[62] Kranenborg (n 49) at 254.

allowed[63]. This principle of utmost importance is known as the 'purpose limitation principle'. Taking into consideration the valuable observations of the Article 29 Working Party, in its Opinion on purpose limitation[64], the reason of the great value of this principle lies with the fact that it limits the actions of the collection and further processing of personal data only to what is truly necessary with regard to legitimate and specific purposes, ensuring thus the legal certainty and promoting trust among the data subjects[65], who will feel reassured since their personal data will not be exploited in an incompatible way with the initial purpose they have been collected and processed for. Nevertheless, the wording of the purpose limitation principle can be characterized as quite broad, which leads to different interpretations and the absence of a consistent approach[66]. It is essential to emphasise that, according to Article 6 (1b) of the Directive, the purpose has to be specified and be explicit, which means that the purpose has to be clearly defined and unambiguously expressed, as well as legitimate, i.e. be based on a clear legal provision. It is the existence of this specified and explicit purpose that limits the powers of the controllers, imposing the obligation of the compatible use and processing of the data subjects' personal data with this purpose, promoting, thus, transparency and predictability. The meaning of the requirement of the processing for a legitimate purpose is a clear reference to Article 7, namely the processing can only occur for a legitimate purpose as long as one, at least, of the criteria of Article 7 is satisfied. However, the meaning of the legitimate purpose is not just limited to Article 7, for the purpose must be compatible with the total amount of legal provisions of data protection law[67], as well as other applicable laws depending on the case. It should, also, be noted that the fundamental value of the principle laid down in Article 6 (1b) sets this data quality principle as a prerequisite for the other data quality principles of Article 6 (1c, d, e)[68]. The assessment of the compatibility of further processing with the initial purposes has to take into account the following key factors[69], the comparison of the purposes of the collection and further processing, the context of the collection, the data

[63] Data Protection Directive Article 6 (1b).
[64] Article 29 Working Party, 'Opinion 03/2013 on purpose limitation' (WP 203, 2 April 2013).
[65] Article 29 Working Party (n 64), at 4.
[66] Article 29 Working Party (n 64), at 5.
[67] Article 29 Working Party (n 64), at 19 – 20.
[68] Article 29 Working Party (n 64), at 12.
[69] Article 29 Working Party (n 64), at 23 – 27.

subjects' expectations and the safeguards adopted by the controller to ensure that the purpose limitation requirement is met.

With regard to the rest of the data quality principles, the Member States must ensure that the personal data should be adequate, relevant and not excessive, in relation to the purposes for which they have been collected and/or processed[70]. It should be underlined that the principle which is enshrined in Article 6 (1c), in conjunction with Article 6 (1b), constitutes part of the 'data minimization' principle. Moreover, the data have to be accurate and kept up to date, where necessary, while a very important safeguard is the fact that the Member – States and the controllers are responsible for the erasure and rectification of the data which are inaccurate or incomplete[71]. Finally, the period during which the data can remain in such a form so as to permit the data subjects' identification must be the absolutely necessary one, taking into account the purposes for which the data have been collected and processed[72]. The extension of the retention period beyond what is necessary can only be achieved by means of the anonymization of the personal data at issue, so that they no longer be able to be related to an identified or identifiable person, seizing, thus, to constitute personal data[73]. Paragraph 2 of the Article 1 clarifies that it is the controller who must ensure that the data quality principles are being respected, thus the controllers are subject to the principle of accountability.

*(ii) Legal grounds for a legitimate data processing*

It is a general principle of the Directive that the processing of non – sensitive personal data has (1) to respect the data quality requirements of Article 6, and (2) to be based on one of the criteria – legal grounds of Article 7 which legitimize the processing. This has been affirmed in the EU jurisprudence, such as *Rundfunk*[74] and *Huber*[75]. The existence of the data subjects' unambiguous consent is the first legal ground under which the processing of personal data is authorized pursuant to Article 7 of the Directive. The Article 29 Working

[70] Data Protection Directive, Article 6 (1c).
[71] Data Protection Directive, Article 6 (1d).
[72] Data Protection Directive, Article 6 (1e).
[73] European Union Agency for Fundamental Rights (n 59) at 44.
[74] Joined Cases C-465/00, C-138/01 and C-139/01, *Österreichischer Rundfunk and Others* [2003] ECR I-4989, para 65.
[75] Case C-524/06, *Heinz Huber v Bundesrepublik Deutschland* [2008] ECR I-09705, para 48.

Party (WP), in its opinion on the definition of consent[76], outlines the crucial role of consent in the European data protection law and attempts to clarify its meaning for the preventions of divergences in the legislations of the State – Members[77]. It should be pointed out that the existence of consent is also present in Article 8, which refers to the processing of special categories of data, and Article 26 with regard to data transfers. As the Article 29 WP has explicitly highlighted, the fact that the existence of consent is cited as the first legal ground which legitimizes the processing of personal data does not entail that it is always the most appropriate one, or that is more important that the other legal grounds[78], nor the existence of consent nullifies the data quality principles, which have to be followed by the controller no matter what[79]. Article 2(h) of the Directive defines the notion of the data subject's consent, explaining that consent refers to 'any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed'. Thus, the essential component of the notion of consent is the indication of the data subject's wishes, which could take any form, even the form of a signal which could clearly enough indicate the data subject's wishes[80], as long as the data subject willingly signifies his or her agreement. However, despite the wide meaning of the consent, it is necessary that some kind of action occur, as this is suggested by the word 'unambiguously' of Article 7(a). As the definition of the Directive suggests, the data subject's consent must be 'freely given', meaning that it must result from the data subject's own willingness, without any external interventions. Finally, the data subject's consent must be 'specific', namely it must clearly and precisely refer to the purposes and the limits of the processing of the personal data that relate to the data subject[81], while a general agreement cannot be deemed as adequate. It is, also, essential that the data subjects be properly informed about the meaning and the consequences of the action of consenting to the processing of their personal data.

[76] Article 29 Working Party, 'Opinion 15/2011 on the definition of consent' (WP187, 13 July 2011).
[77] Article 29 Working Party (n 76), at 4.
[78] Article 29 Working Party (n 76), at 7.
[79] Article 29 Working Party (n 76), at 7.
[80] Article 29 Working Party (n 76), at 11.
[81] Article 29 Working Party (n 76), at 17.

The second legal ground[82] is the necessity of the performance of a contract to which the data subject is party of, including the phase prior to entering into a contract as well. For instance, the common case of the processing of personal data within the workplace is legitimized on the existence of the contract of employment between the employer and the employee[83]. Thirdly[84], the processing is legitimized when it is deemed as necessary for the compliance with a legal obligation to which the controller is subject. This specific criterion refers to private organisations acting as controllers, since the public authorities fall within the Article 7 (e). For instance, due to obligations imposed by employment law on the employer with regard to social security issues, the processing of related personal data of the employee is deemed as necessary[85]. Another criterion[86] refers to the vital interest of the data subjects, mostly evident in health issues. Article 7 (e) provides that the processing of personal data can be deemed as necessary 'for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed'. The meaning of this criterion has been elaborated in *Huber* case, where the CJEU stressed that the meaning of the necessity of Article 7 (e) cannot be subject to different interpretations between the Member – States as it must be in accordance with the core objectives of the Directive as they have been set in Article 1[87]. The 'necessity' in Article 7 (e) implies that the personal data that can be collected and processed have to be the absolutely necessary for the application of the national legislation, while these have to enable the, as effective as possible, application of the national legislation[88]. The last criterion refers to the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, with the exception of the supremacy of other interests (f)or[89] fundamental rights and freedoms of

[82] Data Protection Directive, Article 7 (b).
[83] Article 29 Working Party, Opinion 8/2001 on the processing of personal data in the employment context' (WP 48, 13 September 2001), at 15.
[84] Data Protection Directive, Article 7 (c).
[85] Article 29 Working Party (n 83), at 15.
[86] Data Protection Directive, Article 7 (d).
[87] *Huber* (n 75), para 52.
[88] *Huber* (n 75), para 66.
[89] As the Article 29 WP underlines, 'or' was mistakenly typed as 'for' due to misspelling, thus the correct text is 'interests or fundamental rights and freedoms'. See Article 29 Working Party, 'Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC', (WP 217, 9 April 2014), at 29.

the data subject[90]. The Article 29 WP, in its Opinion on the notion of legitimate interests of the data controller of Article 7 (f), notes that this particular legal ground has been particularly open to wide interpretations, leading to a constant exploitation of this legal ground each time the processing cannot be legitimized under one of the rest legal grounds of Article 7[91]. It follows from the wording of Article 7 (f) that two conditions have to be met for the legitimization of the processing. Firstly, the processing must be necessary for the purposes of the legitimate interests of the controller or the third party to whom the data have been disclosed, and, secondly, these interests must not be overridden by the fundamental freedom and rights of the data subject. Any additional requirement imposed by the national legislation is not compatible[92] with the meaning of Article 7 (f). The CJEU concluded that the conditions laid down in Article 7 (f) preclude any national rules that additionally require that the personal data at issue appear in public sources, excluding, thus, in a generalized manner the processing of the personal data who do not appear in public sources, without any prior balancing of the opposing rights and interests[93]. The CJEU, also, held that Article 7 (f) of the Directive has direct effect[94]. The difference of the sixth legal ground, compared to the legal grounds (a) to (e) of Article 7, is that the latter legitimize a priori the data processing, whereas in the case of 7 (f) a specific test needs to take place for the cases which do not fall within one of the previous legal grounds, requiring the balancing of the opposing interests and fundamental rights[95]. The Article 29 WP puts emphasis on the fact that the notion of the 'legitimate interest' signifies that the interest must be lawful, i.e. consistent with European and national legal rules, sufficiently articulated and specific, as well as real and present[96]. During the balancing test, account must be taken of the nature and source of the legitimate interests, as well as of the impact on the data subjects[97].

[90] Data Protection Directive, Article 7 (f).
[91] Article 29 Working Party (n 89), at 5.
[92] Joined Cases C-468/10 and C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) and Federación de Comercio Electrónico y Marketing Directo (FECEMD) v Administración del Estado* [2011] ECR I – 12181, para 39.
[93] *ASNEF and FECEMD* (n 92), paras 47 – 49.
[94] *ASNEF and FECEMD* (n 92), para 55.
[95] Article 29 Working Party (n 89), at 9 – 10.
[96] Article 29 Working Party (n 89), at 25.
[97] Article 29 Working Party (n 89), at 50.

*(iii) Rights of data subjects protected under Directive 95/46/EC*

The Directive enshrines a list of rights for the sake of the data subject, the most important of which are the right of access, the right to rectification, erasure or blocking and the data subject's right to object. According to Article 12, the data subject has the right to obtain from the controller confirmation about whether data that relate to him or her are processed, information on the purposes of the processing, the categories of data and the recipients to whom the data are disclosed. The data subjects can obtain communication, in an intelligible form, of the data under processing and knowledge of the logic involved in the automatic processing of data. Moreover, the right of access can take the form of the rectification, erasure or blocking of the data whose processing is incompatible with the basic provisions of the Directive. The fundamental essence of the right of access is emphasized in the *Rijkeboer* case[98], in which the CJEU was asked to decide whether the data subjects' right of access to information on the recipients or categories of recipient of personal data and to the content of the data can be limited to a one – year time period prior the request for access. The CJEU held that the effective protection of individuals' privacy entails that they should be assured that their personal data are processed in a lawful and fair manner with respect to the data quality principles. In this context, the right of access can be a particularly important step towards this aim[99]. Moreover, the existence and safeguarding of the right of access constitutes a precondition for the exercise of the data subject's right to object, enshrined in Article 14, and the exercise of the right to judicial remedies and compensation from the controller for the damage suffered, according to Articles 22 and 23[100]. The Court of Justice, also, specified that the right of access must 'of necessity' refer to the past[101] in order for the effective exercise of the data subjects' right of access to be ensured. It concluded that it is the responsibility of the Member States to determine the time – limit for the storage of information on the recipients or the categories of recipient of personal data and on the content of the data disclosed and to provide access to these data. This presupposes that a fair balance should be struck between the interests of

[98] C-553/07, *College van burgemeester en wethouders van Rotterdam v M.E.E. Rijkeboer* [2009] ECR I – 03889.
[99] *Rijkeboer* (n 98), para 49.
[100] *Rijkeboer* (n 98), para 52.
[101] *Rijkeboer* (n 98), para 54.

the data subjects and the burden imposed on the controller caused by the storage of the data[102]. An aspect of the right to rectification and the right to object refers to the right to be forgotten[103], which has been one of the crucial points of the decision of the CJEU on the *Google Spain* case[104]. It is emphasized that personal information, which over the course of time, seem to be inaccurate or inadequate with regard to the purposes they have been collected for, have to be erased upon request of the data subjects[105]. The right to be forgotten specifically applies to the case of search engines which, upon request, must remove links with personal information about them in the abovementioned cases, having also taken into account potential interferences with the freedom of expression[106]. Overall, the enshrinement of critical rights for the data subjects in the Directive 95/46, such as the right of access, rectification, erasure and blocking of data, can be considered as essential for the attainment of individual control over the personal data that relate to the data subjects[107].

*(iv) The role of national supervisory authorities*

Chapter VI of the Directive 95/46 refers to the functioning of the national supervisory authorities, which act as an additional safeguard for the effective protection of the data subjects' rights and the processing of their personal data. Article 28 of the Directive regulates the existence and the terms of the functioning of the supervisory authorities, as well as the scope of their powers.

Article 28, paragraph 3 of Directive 95/46/EC constitutes the legal basis for the supervisory powers of the national data protection authorities. In particular, they possess investigative powers, which can take the form of the access to data at issue, and of the collection to data necessary for their operations. Moreover, they are endowed with powers of intervention, the most important of which are the issuance of opinions prior the data

[102] *Rijkeboer* (n 98), para 64.
[103] See also Andrew Murray (n 6) at 575 – 578.
[104] Case C-131/12, *Google Spain SL and Google Inc. v AEPD and Mario Costeja González* [2014] OJ C212/4.
[105] *Google Spain* (n 104), para 93 – 94.
[106] *Google Spain* (n 104), para 94, 85.
[107] Lynskey (n 51) at 185.

processing, the blocking, erasure or destruction of the data, if this is deemed as necessary, and the temporary or definitive prohibition of the processing. Furthermore, the national supervisory authorities are competent to intervene by addressing warnings to the controller, in case the latter does not comply with the obligations set out in the Directive, as well as by referring a case involving a breach of the European data protection rules to the national parliaments or political institutions. Finally, the national data protection authorities possess the power to engage in legal proceedings, whenever the national provisions are violated, and hear claims lodged by any person about such issues[108]. It should be taken into account that, according to Article 28, paragraph, 2, the Member States are obliged to consult with the national data protection authorities prior the implementation of measures related to the processing of personal data.

The independence of the supervisory authorities is emphasized in Article 28, paragraph 1 of the Data Protection Directive, as well as in Article 16, paragraph 2 of the TFEU and Article 8, paragraph 3 of the EU Charter. The CJEU has expressed its opinion on the requirement of independence of supervisory authorities in *Commission v Germany*[109]. The Court of Justice held that the requirement of the 'complete independence' in the Directive means that, on the basis of proper safeguards, the supervising body is able to act completely freely on its own, without being obliged to account for its actions to a higher body or follow instructions given by others[110]. The adjective 'complete' indicates the absolute power of the supervisory authorities, not subject to direct or indirect external influences[111]. Taking into account the fundamental objectives of the Directive, the most crucial of which is the guarantee for a high level of protection of the fundamental rights and freedoms with respect to the processing of personal data, the CJEU estimates that the supervisory authorities are the 'guardians of those fundamental rights and freedoms'[112] and the main responsible ones for the balancing of the protection of these rights with the need

[108] Data Protection Directive Article 28 (4).
[109] Case C-518/07 *Commission v Germany* [2010] ECR I – 1885.
[110] *Commission v Germany* (n 109), para 18.
[111] *Commission v Germany* (n 109), para 19. The CJEU reiterated the same findings in Case C-614/10 *Commission v Republic of Austria* EU:C:2012:631, paras 40, 41 and in Case C-288/12, *European Commission v Hungary* [2014] OJ C175/6, para 51.
[112] *Commission v Germany* (n 109), para 23.

for free flow of personal data[113], tasks which require the successful cooperation of the different national supervisory authorities. In a nutshell, the CJEU outlines the obligation of the supervisory authorities to 'act objectively and impartially'[114] as an essential inherent component of their very existence and functioning. Moreover, the CJEU examined whether the existence of State scrutiny[115] is compatible with the requirement of independence pursuant to the Directive. The Court of Justice expressly considered that State scrutiny cannot be considered as compatible with the notion of independence of the supervisory authorities, since the mere risk of the potential exertion of political influence on them can endanger their capability of acting independently[116]. In *European Commission v Hungary*, the CJEU elaborated that Member States are competent to determine the terms of the functioning and, in general, the institutional model of the national supervisory authorities, however they must whatsoever ensure that the 'complete independence' of Article 28 (1) be safeguarded. It is, thus, against the notion of the 'complete independence' the premature termination of the functioning of the national supervisory authority, as well as the threat of the termination during the term of office, since it results in the circumvention of the safeguards of Article 28 (1) of the Directive[117].

*(v) Confidentiality and Security of data processing. Remedies for the data subjects.*

Section VIII of the Directive is dedicated to the safeguarding of the confidentiality and the security of data processing. According to Article 17, both the controller and the processor must implement the appropriate technical and organizational measures for the protection of personal data against accidental or unlawful destruction, loss, disclosure or access to third parties. Data security does not refer solely to the required hardware or software, it encompasses, as well, internal organizational measures which relate to the need for information to all employees about the data security rules and their responsibilities and

[113] *Commission v Germany* (n 109), para 24.
[114] *Commission v Germany* (n 109), para 25.
[115] As the CJEU explains in *Commission v Germany* (n 109), para 32, State scrutiny, in the case of Germany (but also existent in other countries as well) allows the government, or an administrative body to wield influence on the supervisory authorities' decisions, or even to nullify their effects and replace them.
[116] *Commission v Germany* (n 109), paras 36, 37.
[117] *European Commission v Hungary* (n 111), paras 54, 49, 62.

the proper distribution of the competences during the procedure of data processing[118]. Article 16 enshrines the confidentiality of processing, analyzing that each and every person who acts under the authority of the controller, including the processor as well, must strictly follow the controller's instructions, unless he or she is required not to do so by law.

It is a general rule that the rights of the data subject enshrined in the Directive can be exercised only by the data subject, or by their representatives pursuant to the national provisions. Firstly, the data subject, whose rights have been infringed, can refer to the controller[119] who is responsible for processing the personal data that relate to him or her, with respect to the specific provisions of the national law, while the controller will have to provide the data subject with a written answer to the official request of the latter. Afterwards, the next available solution for the data subjects is the resort to administrative remedies before the national supervisory authority, provided that their request before the controller is rejected or remains unanswered. According to Article 28 (4), data subjects are entitled to lodge their claims before the supervisory authorities, especially for matters on the lawfulness of data processing, and be informed on the outcome of the claim. Finally, Article 22 provides for the data subjects' right to judicial remedy in the case of a breach of their rights.

### *(vi) Issues related to interferences with the right to privacy and personal data*

Article 8 (2) of the ECHR provides for the emergence of potential interferences with the exercise of the right of Article 8 (1). The interference has to be 'in accordance with the law' and 'necessary in a democratic society', solely for the safeguarding of the legitimate aims of national security, public safety, the economic well-being of the country, the prevention of disorder or crime, the protection of health or morals, and the protection of the rights and freedoms of others. The general approach of the ECtHR regarding the lawfulness of an interference with the exercise of a specific right protected under Article 8, can be described as follows: Firstly, the Court examines whether the application concerns a legitimate interest protected by 8 (1), and whether an interference has occurred.

[118] European Union Agency for Fundamental Rights (n 59) at 91.
[119] European Union Agency for Fundamental Rights (n 59) at 119 – 120.

If this is the case, the Court assesses whether this interference (1) is prescribed in law, (2) pursues a legitimate aim, and (3) is necessary in a democratic society. As for the nature of the obligations imposed on the State, the ECtHR found, in the Case *X and Y v. The Netherlands*[120], that despite the fact that the main objective of Article 8 is the protection of individuals' rights to private and family life in general from harmful interferences of the public authorities, this by no means entails that the State has to abstain whatsoever the case may be. In fact, Article 8 suggests that the State, in certain cases, should undertake specific positive actions and appropriate measures to secure the safeguarded rights, even in relations between individuals themselves.

The ECtHR has expressed in many judgments the steadfast opinion that the collection of individuals' personal data from the public authorities without the individuals' initial consent constitutes an interference with their right to respect for private life. For example, in the Case *Murray v United Kingdom*[121] the ECtHR admitted that the action of the recording of the applicants' personal details, as well as the fact that they were photographed without their consent, constitute an indisputable interference with the right to respect for private life[122]. In this particular case, the ECtHR decided that the interference was prescribed in law, pursued the legitimate aim of the prevention of crime and was necessary in order to accomplish this aim. In the *Leander v Sweden* case[123], the storage of personal data about the applicant's private life in the context of the Swedish personnel control system, based on a secret police register, as well as their disclosure to the employer, were considered as an interference with the right to privacy[124], while this statement has been reiterated in *S. and Marper*[125] as well.

The ECtHR jurisprudence has clearly elaborated the meaning of the first prerequisite on the justification of the interference, regarding its accordance with the law. A certain measure, which triggers the interference at issue, must be based on the domestic law, yet, it is indispensable that the relevant legal provisions be accessible to the concerned

[120] *X and Y v The Netherlands* (1985) 8 EHRR 235.
[121] *Murray v United Kingdom* (1996) 23 EHRR 313.
[122] *Murray* (n 121), para 86.
[123] *Leander v Sweden* (1987) 9 EHRR 433
[124] *Leander* (n 123), para 48.
[125] *S. and Marper v United Kingdom* (2009) 48 EHRR 50, paras 67, 121.

persons, compatible with the rule of law, and their consequences be foreseeable for the individual[126]. In *Rotaru v* Romania[127], the ECtHR was asked to decide on the lawfulness of the use by the Romanian Intelligence Service of a file containing personal information of the applicant, such as his conviction because of two letters of protest he had written, when he was a student, against the abolition of the freedom of expression when the communist regime was established in 1946. The relevant legal provision, which authorized the collection, recording and storage of personal information related to national security in secret files, was found by the ECtHR as inadequate to meet the standards of the accessibility and foreseeability, since it laid no limits to the exercise of these powers, by not defining the kind of information to be recorded, the categories of the concerned people, the circumstances or the procedure that had to be followed, and the time length of their retention[128]. It is, additionally, essential that the legislation provide for adequate and effective safeguards against abuse, due to the inherent risks a system of secret surveillance may pose for the democracy[129]. One crucial aspect of this is the need for the existence of effective supervision with regard to the interference of the public authorities, provoked by the mechanism of the secret surveillance, which, according to the Court, can be well performed by the judiciary, however these standards were not met in the case at issue[130]. The case *Malone v United Kingdom*[131] dealt with the lawfulness of the interception of a telephone conversation, to which the applicant had been a party, from the Post Office on behalf of the police pursuant to a warrant issued by the Home Secretary. The applicant alleged that his rights, protected by Article 8 of the Convention, were violated by the interception of his postal and telephone communications by or on behalf of the police, as well as by the 'metering' of his telephone by or on behalf of the police[132]. In its assessment on the lawfulness of the interference caused by the interception of the communications, the ECtHR stipulates the requirements under which the interference has to be in accordance with the law. The Court stressed that this prerequisite does not solely refer to domestic law.

[126] *Kopp v Switzerland* (1999) 27 EHRR 91, para 55,
[127] *Rotaru v Romania* (App No 28341/95) (unreported) 4 May 2000
[128] *Rotaru* (n 127), para 57.
[129] *Rotaru* (n 127), para 59.
[130] *Rotaru* (n 127), para 59.
[131] *Malone v United Kingdom* (1985) 7 EHRR 14.
[132] *Malone* (n 131), paras 15, 16, 62.

It refers, as well, to the quality of law, which is necessary to comply with the fundamental principles of the ECHR. Therefore, domestic law would not be able to authorize a generalized arbitrary interference by the public authorities with individuals' rights safeguarded by Article 8 of the Convention. In the exceptional cases where secret surveillance measures must be undertaken by the public authorities, the law has to be clear as to the conditions and circumstances under which the public authorities are vested with the power to resort to measures of secret surveillance[133]. In the present case, the interception of the communications on behalf of the police, ordered by a warrant issued by the Secretary of State, was lawful under the law of England and Wales. However, the ECtHR concluded that the law of England and Wales was 'somewhat obscure and open to differing interpretations'[134].

Moreover, the interference must be necessary in a democratic society. According to the ECtHR judgment in the *Coster* case[135], an interference is necessary in a democratic society for a specific legitimate aim when it addresses a 'pressing social need' and is proportionate to the legitimate aim pursued[136]. The national authorities are endowed with a significant margin of appreciation, for they are aware of the local needs and conditions[137]. The importance of the existence of sufficient safeguards, as far as the right to personal data is concerned, is emphasized in *S. and Marper,* where the Court argues that the national legislation has to lay down rules which will determine the categories of data to be stored, the necessary time period of storage and the safeguards against their misuse and abuse[138]. The ECtHR, in *Malone,* reiterates that measures of secret surveillance inherently pose a serious threat for the democratic society, since the risk of abuse is relatively high, however in exceptional cases, such as whenever it is deemed necessary for the prevention of disorder or crime, they can be considered necessary, as long as the national legislation provides for adequate safeguards against abuse during the procedure of the functioning of the

[133] *Malone* (n 131), para 67.
[134] *Malone* (n 131), para 79.
[135] *Coster v the United Kingdom* (2001) 33 EHRR 20.
[136] *Coster* (n 135), para 104.
[137] *Coster* (n 135) para 105.
[138] *S. and Marper* (n 125), para 103.

mechanism of the secret surveillance[139]. Since the measure was found not to be in accordance with the law, the Court did not proceed to the examination of this requirement.

The lawfulness of surveillance measures used by the public authorities has been the main topic for several decisions issued by the ECtHR, notably the Case *Klass v Germany*[140] and the Case *Roman Zakharov v Russia*[141]. In the first case, the applicants claimed that the surveillance measures, prescribed in German law, were unlawful due to the absence of any obligation for the public authorities for notification of the person affected by these measures, as well as due to the absence of remedies before the courts against the ordering and execution of the measures[142]. The Court took into account the advanced technological means of espionage and surveillance, as well as the massive proportions terrorism has taken in Europe in recent years, admitting that the effective protection of the national security requires the undertaking, by the public authorities, of measures of secret surveillance over the post, mail and telecommunications, albeit under exceptional circumstances [143]. The Court acknowledged that the State enjoys a certain degree of discretion with regard to the selection of the appropriate means of surveillance, however, under no circumstances can this degree of discretion be unlimited. The lawfulness of such measures depends on the existence of 'adequate and effective guarantees against abuse'[144]. The ECtHR stressed that the assessment of the lawfulness and necessity of surveillance measures within the democratic measures cannot be determined beforehand, therefore there can be no general rule for the regulation of the issue. The assessment has to be carried out ad hoc, taking into consideration the circumstances of the case, such as the nature, the scope and the duration of the measures, the reasons for their authorization, the existence of competent authorities assigned with the task of the proper supervision on the whole procedure, as well as the existence of remedies pursuant to provisions of the national law[145]. In *Roman Zakharov v Russia,* the ECtHR clarifies that individuals must be fully informed about the precise scope

[139] *Malone* (n 131), para 81.
[140] *Klass v Germany* (1979) 2 EHRR 214.
[141] *Roman Zakharov v Russia* [2015] ECHR 1065.
[142] *Klass* (n 140), para 10.
[143] *Klass* (n 140), para 48.
[144] *Klass* (n 140), para 50.
[145] *Klass* (n 140), para 50.

of application of the secret surveillance measures in advance[146], while the target of these measures must be a specific person, since the authorization of the collection of data in a generalized manner is prohibited[147]. It is also emphasized that public authorities must be able to request access to one's personal data provided that they show the relevant judicial authorization to the communications service provider[148], while, as far as the issue of the notification of the data subjects is concerned, it is stated that data subjects must be notified as long as the notification does not endanger the purpose which triggered the surveillance measures at issue[149].

Respectively, the EU Charter, in Article 52, stipulates that any limitation on the exercise of the rights enshrined in the Charter, must be provided for by law, respect the essence of these rights, be necessary and pursue objectives of general interest or the need to protect others' rights or freedom, with respect to the principle of proportionality. The CJEU examined the interaction between the right to privacy and national security interests in the *Digital Rights Ireland* case[150]. The Court of Justice assessed the validity of Directive 2006/24/EC and reached the conclusion that the Data Retention Directive is incompatible with the basic safeguards of the EU Charter, therefore the Court of Justice invalidated the Directive 2006/24/EC. As the Article 1(1) stipulates, the Data Retention Directive's main object and aim was the regulation of the obligations of the providers of publicly available electronic communications services or of public communications networks regarding the issue of the retention of specific categories of personal data, in order for these data to be made available for the purpose of the investigation, detection and prosecution of serious crime. The scope of the Directive 2002/58/EC, as set out in Article 1 (2), is limited to traffic[151] and location data, as well as the necessary data for the identification of the subscriber or registered user, while both natural and legal entities fall within the personal

[146] *Roman Zakharov* (n 141), para 243.
[147] *Roman Zakharov* (n 141), para 264.
[148] *Roman Zakharov* (n 141), para 269.
[149] *Roman Zakharov* (n 141), para 287.
[150] Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others* and *Kärntner Landesregierung and Others* [2014] OJ C175/6.
[151] According to Article 2 (b) of the Directive 2002/58/EC, traffic data refer to the 'data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof'. In other words, the traffic data include the sender and recipient of communications, as well as the time of communication.

scope of the Data Retention Directive. The content of electronic communications, however, was excluded from the Data Retention Directive's scope. Article 7 lays down specific data security obligations on telecommunications providers. The retained data ought to have been of the same quality, subject to the same security and protection as other data retained on the network, as well as protected by appropriate technical and organizational measures against potential accidental of unlawful destruction, ensuring the access only by authorized personnel, and destroyed at the end of the retention period, except for those which had been accessed and preserved.

In both cases, joined for the purposes of the oral procedure and judgment, the applicants questioned the legality of the national legislative and administrative measures regarding the retention of data related to electronic communications. The CJEU was asked by the referring courts to examine the lawfulness of the Directive 2006/24 in the light of Articles 7, 8 and 11 of the Charter of Fundamental Rights in the EU. The CJEU notes that Article 5 of the Directive 2006/24 might pose a potential danger to the respect for private life and communications, as well as the right to the protection of personal data and the freedom of expression[152]. The danger for one's privacy stems from the fact that the ordered retention refers to the categories of data, as they are listed in Article 5[153]. Due to the wide range of the data falling within these categories, it is natural that potential interference with individuals' right to privacy might emerge, since it would be possible, under certain circumstances, to trace the location of users, discover their activities or social relationships[154], despite the ascertainment of Article 5, paragraph 2 regarding the unlawfulness of the retention of the content of the communication. Another challenge which has to be taken into account is the competence of the national authorities for access to the retained data, pursuant to Article 4 of the Directive. In a nutshell, the CJEU concluded that the abovementioned provisions constitute an interference with the rights

[152] Data Retention Directive para 25.
[153] According to Article 5, the data to be retained are only those which are necessary (a) to trace and identify the source of a communication,(b) identify the destination of a communication, (c) identify the date, time and location of a communication, (d) identify the type of communication, (e) identify users' communication equipment or what purports to be their equipment, and, (f) identify the location of mobile communication equipment.
[154] *Digital Rights Ireland* (n 150), para 27.

enshrined in Articles 7 and 8 of the Charter[155] and proceeded to the examination whether this interference can be justified or not. Article 52 (1) of the Charter lays down the rule that limitations on the exercise of rights or freedoms enshrined in the Charter must be provided for by law, respect their essence, be necessary and meet objectives of general interest, recognized by the EU, or the need to protect the rights and freedoms of others, in accordance with the principle of proportionality. The Court recognizes that in this specific case the retention of the data, pursuant to Directive 2006/24, is permitted solely for the purpose of the investigation, detection and prosecution of serious crime, which constitutes an objective of general objective, aiming at the safeguarding of the public security[156], while it admits that the use of data related to electronic communications can be a valuable ally to the fight against international terrorism[157]. The critical issue, since theoretically the provisions of the Directive serve the general objective of the protection of public security, is whether the interference was proportionate or not, which, according to the estimation of the CJEU in conjunction with its previous settled case – law, has the meaning that an act of EU institutions can be characterized as proportionate on condition that it should be appropriate for the attainment of the pursued legitimate objective and it should not exceed the limits of what is appropriate and necessary for this accomplishment[158]. The EU legislature's discretion has to be reduced, taking into account a multitude of factors and circumstances[159]. While the retention of data can be considered as appropriate for the achievement of the legitimate aim of the fight against serious crime[160], it is by no means considered as necessary. It is required that EU legislation lay down precise and clear rules regarding the scope of the proposed measure, and impose sufficient safeguards for the protection of individuals' personal data against potential risks, especially in cases of automatic processing[161].

[155] *Digital Rights Ireland* (n 150), paras 32, 34, 35, 36.
[156] *Digital Rights Ireland* (n 150), paras 41, 42.
[157] *Digital Rights Ireland* (n 150), para 43.
[158] *Digital Rights Ireland* (n 150), para 46.
[159] *Digital Rights Ireland* (n 150), paras 46, 47.
[160] *Digital Rights Ireland* (n 150), para 49.
[161] *Digital Rights Ireland* (n 150), paras 54, 55.

The CJEU has found that this requirement is not met in the case of Directive 2006/24[162]. The main argument is the fact that its provisions enable the retention of all traffic data, related to a very wide range of means of electronic communication, affecting, thus, all European citizens[163]. The main concern lies within the generalized manner of the whole procedure of the retention of personal data, without any differentiation, limitation or exception being made in the light of the objective of fighting against serious crime[164]. The Court of Justice stipulates that there is no association between the data to be retained and a particular time period or geographical zone or a circle of particular persons, while the existence of limits and substantive and procedural conditions of the access of the competent national authorities is totally absent, which could potentially lead to the use of data beyond what is strictly necessary[165]. In addition, there are no rules about any prior review by a court or an independent administrative body for the limitation of access to the data and their use to what is strictly necessary for the pursued objective[166]. Finally, the retention period, according to Article 6, varies from six (6) months to two (2) years, however no distinction is made with regard to the different categories of data, nor any objective criteria are set out limiting the determination of the retention period to what is strictly necessary[167]. Taking into account the inadequacy of Article 7 regarding the absence of specific rules, the Court has accepted that Directive 2006/24 constitutes a wide – ranging interference with the rights enshrined in Article 7 and 8 of the Charter, exceeding the limits imposed by the principle of proportionality[168], declaring, thus, the Directive 2006/24 invalid.

Furthermore, it is important to make a reference to the recent decision of the CJEU on the case of *Tele2 Sverige AB v Post – och telestyrelsen*[169] whose main object is the interpretation of Article 15(1) of the E – Privacy Directive (2002/58/EC), which authorizes Member – States to provide for exceptions from the principle of the confidentiality of personal data and the obligations stemming from Articles 6, 8, 9 of the E – Privacy

[162] *Digital Rights Ireland* (n 150), para 65.
[163] *Digital Rights Ireland* (n 150), para 56.
[164] *Digital Rights Ireland* (n 150), para 57.
[165] *Digital Rights Ireland* (n 150), paras 59, 60, 61.
[166] *Digital Rights Ireland* (n 150), para 62.
[167] *Digital Rights Ireland* (n 150), paras 63, 64.
[168] *Digital Rights Ireland* (n 150), para 69.
[169] Joined Cases C-203/15 and C-698/15 *Tele2 Sverige AB v Post – och telestyrelsen* and *Secretary of State for Home Department v Tom Watson and Others* (Grand Chamber, 21 December 2016).

Directive with regard traffic data, calling identification and location data. One of the most crucial points of the Court was that the general and indiscriminate retention of all traffic data and location data of all subscribers, in the context of the means of electronic communications, cannot be justified, even if its purpose relates to the fight against crime[170]. However, Member – States are able to implement Article 15 (1) of the E – Privacy by adopting measures of targeted and limited retention of traffic and location data for the purpose of fighting against crime and terrorism[171], taking into account specific categories of data and persons. This is the reason why the national legislation must 'lay down clear and precise rules governing the scope and application of such a data retention measure'[172] to what is truly necessary. Finally, another critical point of this decision refers to the access of national authorities to the retained data, establishing that their access must be based on prior judicial review or review of an independent administrative body[173], while the notification of the affected data subjects is necessary for the exercise of the relevant legal remedies, unless there is an imminent danger for the investigations of the public authorities[174].

## B. Specific Regulations on International Data Transfers. The Essence of the European Legal Standards for the Assessment of the Notion of 'Adequacy'.

### 1. The Meaning of International Data Transfers

Starting from the definition of the notion of the transfer of personal data, it can be concluded that, neither Directive 95/46/EC nor any other official European legal instrument contain an interpretation of the content of data transfers, a fact affirmed in the

[170] *Tele2 Sverige AB* (n 169), para 103, in accordance with previous case – law (see e.g. *Digital Rights Ireland*).
[171] *Tele2 Sverige AB* (n 169), para 108.
[172] *Tele2 Sverige AB* (n 169), para 109.
[173] *Tele2 Sverige AB* (n 169), para 120.
[174] *Tele2 Sverige AB* (n 169), para 121.

*Lindqvist* decision[175]. The decision addressed the issue whether the loading of personal data onto an Internet page constitutes or not a data transfer, regulated under the Directive 95/46/EC, and more precisely under Article 25. It acknowledges that information and data on the Internet can be accessed by anyone around the world who possesses the technical means. However, this particular action of the loading of data on a web page cannot automatically send to Internet users information that the latter did not pursue to gain access to. The Court notes that a user, in order to have knowledge of these data, has to take specific technical actions in order to attain their goal. In these cases, there is no direct transfer of data from the data subject, who loads information on a web page, to the recipient of the third country, since the computer infrastructure of the web hosting provider intervenes between them. In an attempt to clarify whether cases like this one fall within the meaning of the data transfer expressed by the Directive and Article 25, the CJEU highlights that the Chapter IV of the Directive regulating the data transfers to third countries sets a complementary regime compared to the general data protection regime set by the general provisions of the Directive, especially by Chapter II. There is no relevant provision in Chapter IV about data transfers particularly on the Internet, therefore the CJEU, taking into account the condition of the Internet use at the time of the adoption of the Directive, as well as the absence of any indexes for cases emerging on the Internet space in the Directive, concluded that it cannot be presumed that the Chapter IV of the Directive encompasses cases like the one at stake, namely the loading of personal data onto an Internet page, making these information accessible to any potential user, otherwise the complementary regime of the data transfers would be considered as a regime of general application.

According to the Position Paper of the European Data Protection Supervisor, on the transfer of personal data to third countries and international organisations by EU institutions and bodies[176], the definition of the notion of data transfers should naturally include the 'movement' of personal data, or the fact that personal data are allowed to

[175] *Lindqvist* (n 40), para 56.
[176] European Data Protection Supervisor (EDPS), Position Paper on the 'Transfer of personal data to third countries and international organisations by EU institutions and bodies', 14 July 2014: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Papers/14-07-14_transfer_third_countries_EN.pdf accessed 01 December 2016.

'move' between different users[177]. It should be noted that the abovementioned Position Paper mostly refers to Regulation 45/2001, which applies to the processing of personal data by the EU institutions and bodies (article 3(1)). The European Data Protection Supervisor, in the light of the *Lindqvist* judgment, advocates that the international data transfers should be composed of the following elements[178]: The action of making the personal data available to the recipient (e.g. communication, disclosure) and the element of the intention or knowledge on behalf of the sender subject in order for the recipient to have access to the data. In order to examine the meaning of the adequacy required for institutions or bodies outside the EU pursuant to article 9 of the Regulation, the EDPS refers to the guidelines pointed out by the WP 29 Working Document on Transfers of Personal Data.

## 2. European Legal Provisions about Transborder Data Flows

Directive 95/46/EC is characterized as one of the most 'influential'[179] legal instruments providing for specific rules in the field of international data transfers. Recitals 56 to 60 of the Directive 95/46/EC refer to the cross – border data transfers and their importance, consisting in their value for the international commerce. The recitals reiterate the content of the Articles 25 and 26, while particularly Recital 60 emphasizes that the lawfulness of data transfers entails the full compliance with the relevant provisions of the Member States' laws and absolutely with the Directive. Generally, the Directive provides a double categorization for data transfers, those realized within the EU and EEA, and the data transfers to third countries, outside the European Union. Article 1, paragraph 2 sets a crucial rule referring to the data transfers within the European Union, stating that '2. Member States shall neither restrict nor prohibit the free flow of personal data between Member States for reasons connected with the protection afforded under paragraph 1.'. It is, thus, evident that under no circumstances can the flow of personal data be restricted. However, this is not the case as far as international data transfers are concerned. Article 25 of the Directive sets the tone regarding the prerequisites:

[177] EDPS (n 176) at 6.
[178] EDPS (n 176) at 7.
[179] Christopher Kuner, *Transborder Data Flows and Data Privacy Law* [1st edn, OUP, 2013] at 40.

‘Article 25

Principles

1. 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 this Directive, the third country in question ensures an adequate level of protection.

2. The adequacy of the level of protection afforded by a third country shall be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations; particular consideration shall be given to 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.

3. The Member States and the Commission shall inform each other of cases where they consider that a third country does not ensure an adequate level of protection within the meaning of paragraph 2.

4. Where the Commission finds, under the procedure provided for in Article 31 (2), that a third country does not ensure an adequate level of protection within the meaning of paragraph 2 of this Article, Member States shall take the measures necessary to prevent any transfer of data of the same type to the third country in question.

5. At the appropriate time, the Commission shall enter into negotiations with a view to remedying the situation resulting from the finding made pursuant to paragraph 4.

6. The Commission may find, in accordance with the procedure referred to in Article 31 (2), that a third country ensures an adequate level of protection

within the meaning of paragraph 2 of this Article, by reason of its domestic law or of the international commitments it has entered into, particularly upon conclusion of the negotiations referred to in paragraph 5, for the protection of the private lives and basic freedoms and rights of individuals.

Member States shall take the measures necessary to comply with the Commission's decision.'

It can be concluded that international data transfers may take place only by fulfilling a major term; the third country is necessary to ensure an adequate level of protection of the fundamental rights, according to Paragraph 1 of the Article 25. Owing to the difficulty of the process of the judgment on the adequacy of a third country's level of protection, Paragraph 3 imposes the obligation of the cooperation of Member – States with the European Commission. The Member States, by virtue of Paragraph 4, are entitled to prevent any transfer of personal data to countries whose level of protection has been deemed as inadequate. Paragraph 2 attempts to enlighten the meaning of this, rather abstract, condition set by the Directive. The assessment of the adequacy of the protection level has to take into account all the circumstances that are closely related to a specific data transfer, particularly the nature of the data, the purpose and duration of the operation, the countries of origin and destination, the legal framework in force in the third country, inter alia.

According to Article 26,

'Derogations

1. 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 which does not ensure an adequate level of protection within the meaning of Article 25 (2) may take place on condition that:

(a) the data subject has given his consent unambiguously to the proposed transfer; or

(b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of precontractual measures taken in response to the data subject's request; or

(c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and a third party; or

(d) the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defence of legal claims; or

(e) the transfer is necessary in order to protect the vital interests of the data subject; or

(f) the transfer is made from a register which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest, to the extent that the conditions laid down in law for consultation are fulfilled in the particular case.

2. 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 the corresponding rights; such safeguards may in particular result from appropriate contractual clauses.

3. The Member State shall inform the Commission and the other Member States of the authorizations it grants pursuant to paragraph 2.

If a Member State or the Commission objects on justified grounds involving the protection of the privacy and fundamental rights and freedoms of individuals, the Commission shall take appropriate measures in accordance with the procedure laid down in Article 31 (2).

Member States shall take the necessary measures to comply with the Commission's decision.

4. Where the Commission decides, in accordance with the procedure referred to in Article 31 (2), that certain standard contractual clauses offer sufficient safeguards as required by paragraph 2, Member States shall take the necessary measures to comply with the Commission's decision.'

Paragraph 1 of Article 26 permits the transfer of personal data to third countries even in the case the prerequisite of the 'adequate protection' is not met, however the derogations prescribed in Article 26 (1) are allowed pursuant to specific, exhaustive reasons. The Article 29 Working Party, in its working document[180] on the meaning of Article 26 (1) of the Directive, notes that the meaning of these reasons is not clear enough, leading to different interpretations and divergences in the national legislations[181]. The evident result stemming from Article 26 (1) is connected with the fact that the data controller is not obliged to ensure that the recipient provides for an adequate level of protection, which could be characterized as inconsistent with the purpose of the standard general rules which require that the transfer to third countries must effectively guarantee an essentially equivalent level of protection of fundamental rights and freedoms in order for the individuals, whose data have been transferred, to enjoy the same protection granted by the Directive[182]. The Article 29 Working Party has tried to address the issue suggesting that the interpretation of Article 26 (1) must be strict. It is important to make clear that the provision of specific derogations from the general requirements of Article 25 does not entail that the activities of the data controller are exempted from the application of the general provisions of the Directive which guarantee the data subjects' rights, such as the data quality principles and impose respective obligations on the data controllers[183]. The

[180] Article 29 Working Party, 'Working Document on a common interpretation of Article 26 (1) of Directive 95/46/EC of 24 October 1995' (WP 114, 25 November 2005).
[181] Article 29 Working Party (n 180), at 3.
[182] Article 29 Working Party (n 180), at 6 – 7.
[183] Article 29 Working Party (n 180), at 8.

analysis of the specific characteristics of the legal grounds for the legitimization of data processing can be valuable for the deeper understanding of the derogations of Article 26 (1).

Paragraph 2 offers an alternative precondition for a successful international data transfer, in case the main prerequisite of the adequate level of protection of the third country is not met. A transfer is yet possible to occur only if the controller provides additional adequate safeguards ensuring the protection of the fundamental rights and freedoms. More precisely, the 'safeguards' which are mentioned in this paragraph could imply the existence of binding contractual commitments agreed between the data exporter and importer. There are two types[184] of clauses that can be used, namely the 'standard contractual clauses' which are approved beforehand by the European Commission, and the 'ad hoc' clauses, which do not have a standard form as they are determined according to each specific case and have to be approved by the national data protection authorities. The standard contractual clauses consist of three sets, two of which refer to transfers to controllers in third countries[185] while the other one refers to transfers to processors in third countries[186]. The use of the 'Binding Corporate Rules'[187] (BCRs) is, also, an alternative legal basis, falling within the meaning of the 'adequate safeguards' under Article 26 (2), on which companies or group of companies in the European Union can export personal data to third countries. The Binding Corporate Rules are legally binding rules which regulate issues related to data processing and express the principle of accountability, meaning that the data controller should ensure that the fundamental principles of security are respected and that he or she are able to fully acknowledge their responsibilities[188]. The existence of the BCRs, thus, allows the transfer of personal data from one corporate member to another based on specific rules which guarantee a high level of

[184] Christopher Kuner (n 179) at 43.
[185] 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.
[186] Commission Decision 2010/87/EU of 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.
[187] Christopher Kuner (n 179) at 43.
[188] Christopher Kuner (n 179) at 43.

protection. It should be noted that the Binding Corporate Rules are not mentioned in the Directive, while only the national data protection authorities are entitled to approve the BCRs.

## 3. Analysis of the *Schrems* Case. Assessment of the 'Adequacy'

The *Schrems* decision reiterated the main prerequisite for international data transfers, which is the necessity for the third country to prove that its level of protection is in practice adequate[189]. The decision, in order to theoretically assess the essence of the adequacy, explicitly refers to the Article 25, paragraph 6 of the Directive, stating that the adequacy may be judged by the domestic law or the international commitments the third country has undertaken for the protection of the fundamental rights of individuals[190]. Furthermore, the Court notes that an 'adequate' level of protection does not necessarily have to mean that the third country is obliged to put into practice an identical, to the European standards, level of protection[191]. More specifically, the third country's level of protection has to be essentially equivalent to the European one, by virtue of the Directive 95/46/EC in the light of the Charter[192]. An essentially equivalent level of protection provides for a high level of protection of fundamental rights, with special reference to the right for respect of privacy and protection of personal data[193]. The requirement of an 'essentially equivalent' level of protection is not a totally new notion. It is reminiscent[194] of the *Solange* decision of 29 May 1974, where the German Bundesverfassungsgericht concluded that legal acts of the European Union can be measured by it against the yardstick of the German fundamental rights, as long as the European Economic Community does not provide for an 'essentially comparable' standard of protection to the one guaranteed by the German Constitutional regime.

---

[189] Case C-362/14, *Maximillian Schrems v Data Protection Commissioner* (Grand Chamber, 6 October 2015), para 48.
[190] *Schrems* (n 189), paras 69, 71.
[191] *Schrems* (n 189), para 73, Opinion of Advocate General Bot in *Schrems* (n 185), para 141.
[192] *Schrems* (n 189), para 73.
[193] *Schrems* (n 189), para 73, Opinion of Advocate General Bot in *Schrems* (n 185), para 142.
[194] Loïc Azoulai and Marijn van der Sluis, 'Institutionalizing personal data protection in times of global institutional distrust: *Schrems*', (2016) 53 Common Market Law Review at 1363.

The assessment of the third country's level of protection involves, inter alia, the examination of the content of the applicable rules, as well as the relevant practice put into effect in order for the compliance with these rules to be ensured[195]. The Directive 95/46/EC creates an updated protection system for the effective exercise of the rights enshrined in it, encompassing a multitude of safeguards, namely regulations on the liabilities, the sanctions, the powers of the supervisory authorities and the means of redress. It has already been pointed out[196] that it is essential for the effective protection of individuals' rights, regarding the issue of the transfer of their personal data to third countries, to set out an appropriate mechanism which will function in practice, satisfying the requirements of law, in order to fully implement the theoretical legal rules. It can be concluded that the adequacy of the level of protection of the third country, not only does it depend on the content of the relevant legal rules, but also on the existing means which will ensure the application of these rules.

According to the WP 29 Working Document on the Transfers to Third Countries, the assessment of the adequacy, as far as this concerns the part of the content of the applicable rules, has to revolve around the following principles:

- The purpose limitation principle[197]. The processing of personal data is allowed only for a specific purpose. Article 6, paragraph 1 (a) and (b) of the Directive lays down the requirements for the data processing to be considered as lawful. The collection is allowed only for 'specified, explicit and legitimate purposes', while the processing must be compatible with these purposes. Article 13 refers to specific, restrictive exemptions from obligations set out in the abovementioned Article.
- The data quality and proportionality principle[198]. The relevant provisions of the Directive are Article 6 (c) and (d), which impose to the Member States the obligation that the data should be 'adequate, relevant and not excessive' and 'accurate and, where necessary, kept up to date'.

[195] *Schrems* (n 189), para 75, Opinion of Advocate General Bot in *Schrems* (n 189), paras 141, 143.
[196] Article 29 Working Party, 'Working Document: Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive' (WP 12, 24 July 1998), at 5.
[197] See also Chapter 2, Section A3 (i).
[198] See also Chapter 2, Section A3 (i).

- The transparency principle[199]. Whether the data have been collected directly from the data subject, or not, in both cases the Directive, in Article 10 (for data collected from the data subject) and Article 11 (for data which have not been obtained from the data subject) provides for the obligation, for the controller or his representative, to provide a minimum of information regarding the identity of the controller, the purposes of the processing and further relevant information, which are necessary for the lawfulness of the information.
- The security principle[200]. Article 17 of the Directive refers to the security of processing, which has to be safeguarded by the implementation of the appropriate technical and organizational measures. Paragraph 2 and 3 of the Article 17 regulate the case of the processing by the processor who acts on behalf of the controller. This person has to 'provide sufficient guarantees' and act on the specific instructions from the controller.
- The rights of access and rectification and the right to object[201]. It is essential that data protection law effectively protect the data subject's fundamental rights of access to his/her data. According to Article 12, the general right of access consists of the right to obtain confirmation about the processing, communication to the controller and knowledge of the logic, if the processing has been carried out via automated means. Furthermore, the data subjects have officially the rights of rectification, erasure or blocking of their personal data, in case of unlawful processing.
- Restrictions on onward transfers. Onward transfers should not result in the violation of the initial obligations. The same obligations that are valid for the first recipient, are valid for the second one as well.

As it has already been emphasized, an effective protection of the rights related to one's personal data are not limited to the abstract prescription of these core principles in law. Parallelly, it is of utmost importance that an independent, external supervision mechanism be created, in order to ensure the compliance with these rules. As the WP

[199] See also Chapter 2, Section A3 (i).
[200] See also Chapter 2, Section A3 (v).
[201] See also Chapter 2, Section A3 (iii).

29 Working Document suggests, this mechanism can be characterized as adequate provided that it keeps the data subjects constantly aware of their lawful rights, and the controllers aware of their obligations. Moreover, it is essential that, as far as the issue of the data transfers is concerned, effective supervision of the processing for the transferred data be put in practice, while in cases where it is certified that violation of the requirements of the law has occurred, it is significant that the necessary measures be taken for the reestablishment of the legal order. The proper functioning of independent supervisory authorities constitutes a major safeguard towards the protection of the rights of the individuals. The existence of mechanisms able to respond promptly to individuals' complaints is required, in order to provide the necessary support to those individuals who claim that their rights have been breached. In addition, redress mechanisms are also a fundamental element of the proper data protection system, in order to provide for the appropriate remedies and compensation to the victims.

The *Schrems* decision, as well as the *Digital Rights Ireland* decision, clarify that the review of the legal standards of the adequacy has to be strict[202]. It is crucial to underline that all decisions make reference to the potential existence of derogation or limitations imposed to the protection of individuals' personal data, stating that these can apply only in exceptional cases insofar as this is strictly necessary[203]. An additional observation, crucial for the assessment of the adequacy of the third country's level of protection, is that both cases cite a characteristic case which, by all means, is contrary to the essence of the European legal standards as far as the protection of privacy and personal data is concerned. It is made clear that the authorization, on a generalized basis, of the storage of all the personal data of all persons whose data have 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 cannot be characterized as strictly necessary. Under this statement, it is implied by the Court that exceptions to the fundamental rights of respect for privacy and protection of personal data are allowed, nevertheless these have to be strictly necessary, taking into account

[202] *Schrems* (n 189), para 78, *Digital Rights Ireland* (n 150), paras 47 – 48.
[203] *Schrems* (n 189), para 92, *Digital Rights Ireland* (n 150), para 52.

the principle of proportionality. According to the opinion of Advocate General Bot, the limitations have to be in compliance with the Article 52 (1) of the Charter, meaning that they have to be prescribed in law, and respect the fundamental essence of the rights at issue. The respect of the principle of proportionality can be obtained only if these derogations are strictly necessary and meet objectives of general interest or the need for the protection of rights or freedoms of others[204]. The definition of specific criteria which would determine the limits of the powers of public authorities with regard to the processing of individuals' personal data constitutes a valuable factor to be taken into consideration as well[205]. Another essential component of the meaning of the adequacy, according to the *Schrems* decision, is the existence and effective function of legal remedies acting as safeguards for fundamental rights of individuals, such as the right for one's access to their personal data, or for the rectification or erasure of them, by virtue of the Article 47 of the Charter about the effective judicial protection[206]. In addition to the abovementioned, the decision stresses the significance of the existence of an external control mechanism, an important trait of which will be its independent form, responsible for the effective protection of individuals' rights and personal data[207].

Taking the aforementioned findings of the CJEU in the *Schrems* case, as well as the Opinion of the Article 29 Working Party[208], four essential elements of the European legal framework should be examined through the assessment of the E.U. – U.S. Privacy Shield, as well as the assessment of the potential interferences which may arise from the legislation of third countries. Firstly, data processing must be based on clear and precise legal rules, while afterwards it has to be examined whether any authorization of access to personal data is necessary and proportionate. Thirdly, the existence and proper functioning of an independent oversight mechanism is crucial for ensuring the compliance with the

[204] Opinion of Advocate General Bot in *Schrems* (n 189), para 176.
[205] *Schrems* (n 189), paras 39, 57 – 61.
[206] *Schrems* (n 189), para 95, Opinion of Advocate General Bot in *Schrems* (n 189), para 165.
[207] Opinion of Advocate General Bot in *Schrems* (n 189), paras 145, 166, 210.
[208] Article 29 Data Protection Working Party, 'Opinion 01/2016 on the E.U. – U.S. Privacy Shield draft adequacy decision' (WP 238, 13 April 2016), at 11, and Hogan Lovells, 'Legal Analysis of the E.U. – US. Privacy Shield, An adequacy assessment by reference to the jurisprudence of the Court of Justice of the European Union.' 4 April 2016, http://www.hoganlovells.com/files/Uploads/Documents/Privacy%20Shield%20Legal%20Analysis%20by%20Hogan%20Lovells%20(2016-03-31).pdf accessed on 10 September 2016, at 14 – 15.

principles of European data protection law, and, finally, effective remedies before an independent body must be available for any person who believes that his or her rights have been infringed.

## C. Data Protection and Social Networking Platforms

According to danah boyd and Nicole Ellison[209], the social network sites[210] constitute web – based services which permit their users to create a public or semi – public profile. Moreover, users are able to search and find other users they know and create a list of them, which can be viewed and traversed by themselves, as well as the other users. It is, of course, natural that these general traits may differentiate to some extent depending on the type and form of the social network site, however their essence remains unchanged. The authors suggest that the existence of social network sites does not derive from the desire to meet new people, but, rather, from the need to sustain and communicate with the existing social network[211]. The social networking platforms have been characterized as a 'semi – public' forum[212], under the meaning that in these sites each and every digital exchange of information remains depicted, while, at the same time, there is a significant risk of exposure, since the amount of the information shared between specific users could potentially be disclosed to other users as well without the consent of the related users. The abovementioned definition of the social networking platforms is really close to the definition given by the European Network and Information Security Agency (ENISA)[213] pointing out the characteristics of the creation of an online profile including personal

[209] danah boyd and Nicole Ellison,' Social Network Sites: Definition, History and Scholarship' (2007), 13 Journal of Computer – Mediated Communication, at 211.
[210] The authors prefer the term 'social network sites' instead of 'social networking sites' since the latter emphasizes the relationship initiation, which, as they note (at 211) is not the primary aim or trait of these sites.
[211] danah boyd and Nicole Ellison (n 209) at 211.
[212] David Haynes, 'Social media, risk and information governance' (2016), 33 Business Information Review at 90-93.
[213] European Network and Information Security Agency, 'Position Paper No1 Security Issues and Recommendations for Online Social Networks', October 2007.

information, the ability of having social interactions with other users and the selection of the users who will have access to one' profile[214].

Opinion 5/2009[215] adopted by the Article 29 Data Protection Working Party on 12 June 2009 refers to the legal context regulating the existence and function of online social networking, more specifically Social Network Services (SNS). The gradual participation of the users in online social networking platforms, the creation of online profiles consisted of personal data voluntarily submitted by the users, leading to the shaping of an online community constitute critical factors inevitably leading to the necessity of legal regulation. This need has been particularly urgent due to the fact that the voluntary disclosure of the users' personal data during their participation in online social networking platforms may pose a serious risk in the case, especially sensitive, personal information happen to be exploited by third parties for commercial purposes, or other reasons as well. Technically, the SNS are legally characterized as information society services[216], in accordance with Article 1, paragraph 2 of Directive 98/34/EC. The Opinion clarifies that in most of the emerging cases, Directive 95/46/EC constitutes the applicable legal instrument applicable. The SNS providers are considered as the data controllers[217], since they are the responsible ones for providing the main services and means to users willing to join the social networking platforms. The Opinion notices that the SNS providers are also involved in the processing of personal data by third parties, made for commercial and advertising purposes. The data subjects are the users who voluntarily decide to join this web community. While Article 3, paragraph 2 of the Directive sets the general rule of the exemption of the applicability of the Directive in the case of the processing by a natural person in the course of a personal or household activity, nevertheless in a few cases users do not fall within this exemption and can be considered as data controllers, particularly when the user acts as a legal representative of a company. The Opinion provides useful guidelines to the SNS providers regarding the appropriate measures that have to be put in practice for the effective

[214] An exhaustive reference to the definition of the social networking platforms can be found in Georgios Yannopoulos, *Η Ευθύνη των Παρόχων Υπηρεσιών στο Internet (The Liability of the Internet Service Providers)* (Nomiki Vivliothiki, 2013) at 19 – 20.
[215] Article 29 Data Protection Working Party, 'Opinion 05/2009 on online social networking' (WP 163, 12 June 2009). See also Georgios Yannopoulos (n 214) at 225 – 228.
[216] Article 29 Data Protection Working Party (n 215) at 4.
[217] Article 29 Data Protection Working Party (n 215) at 5.

protection of the users' privacy. The respect of Article 10 of the Directive is crucial in order for the users to be informed on the purposes of data processing by the SNS providers, including the action of data processing for marketing and advertising purposes[218]. Moreover, the SNS providers have to respond adequately to their obligations as data controllers and take the proper technical and organizational measures to ensure the security of data processing, pursuant to the general provision of Article 17 of the Directive[219].

New challenges have arisen due to significant technological developments, particularly due to the risks posed by the social networking platforms, of which Facebook remains the main and primary online social networking site, for individuals' privacy. In the case of Facebook, users are called to voluntarily submit personal information, among which their full name, date of birth, gender, contact information, personal information regarding their personal and family status, along with photographs of themselves, as well as of their online 'friends'. The profile's main characteristic is the visibility to other users – friends. However, it should be taken into account that users who are not friends, or even people who are not users of Facebook, can have access to personal information of one's Facebook profile, depending on the enabled privacy settings regarding the allowable degree of access. The main concern is that the creation of such a kind of online profile can easily be exploited by advertising companies, which will be able to send to all user tailored advertisements, depending on their preferences based on the personal data of their profile. Moreover, there is a considerable danger that these information could be rendered accessible to public authorities, as well as third parties. Facebook uses the submitted personal data, notably the names and users' pictures, in order to connect them to the users' profiles and to facilitate the communication among users. Facebook is not just another chat – room or forum, where the participants can conceal their true identities, thus its particularity is found in this connection between a user's profile to their real public identity.

Access to social network sites is dependent on the user's agreement to the processing of personal data that relate to him or her. The consent to behavioural advertising is deemed necessary for the access to social networking sites, and the Article 29 Data

[218] Article 29 Data Protection Working Party (n 215) at 7.
[219] Article 29 Data Protection Working Party (n 215) at 7.

Protection Working Party stresses that the users should be put in a position where they will provide specific consent to receiving behavioural advertising, distinguished from the consent which is needed for the access to social networking platforms[220]. Another issue is the fact that users who may want to use external applications, have to provide their consent to the transfer of their personal information to the developer of the application for multiple purposes such as behavioural advertising or reselling to third parties. It is, thus, necessary according to the Article 29 Data Protection WP opinion, that this specific consent be obtained separately from the consent to the use of the application, since the transfer of personal data does not constitute a prerequisite for the proper functioning of the application[221]. It must be stressed that it is possible for the users of Facebook, or other social networking platforms, to protect their personal data by activating the proper privacy settings that will allow for information to be viewed and accessed only by the list of friends, or even by the user exclusively, nevertheless the users cannot monitor the flow of information posted by the rest of users – friends[222]. The Data Policy of Facebook stipulates that personal data of its users are subject to availability upon legal requests, such as search warrants, in the cases where this is required by law or when this is necessary for the detection and prevention of fraud or other illegal activities, crime or abuse[223] or the protection of other users' interests. It is, therefore, reasonable to wonder whether the existence of privacy settings can effectively protect the users' personal data. It should be mentioned that the GDPR seeks to enforce the users' rights regarding their activities in the social networking platforms. Two particularly important changes refer to the introduction of the right to be forgotten pursuant to Article 17, which specifies the cases where the erasure of the personal data is authorised. Notably, the data subject is entitled to request the erasure of personal data that relate to him or her from the data controller provided that the data are no longer necessary for the initial purposes they have been processed. The erasure can be requested in cases where the data subject's consent has been withdrawn, or the data subject exercise their right to object to data processing. Furthermore, Article 20

[220] Article 29 Data Protection Working Party (n 215), at 18.
[221] Article 29 Data protection Working Party (n 215) at 19.
[222] Fereniki Panagopoulou – Koutnatzi, 'Facebook as a challenge to privacy' in Maria Bottis, *Privacy and Surveillance, Current aspects and future perspectives* (1st edn, Nomiki Vivliothiki, 2013) at 224.
[223] See Data Policy of Facebook https://www.facebook.com/about/privacy/ accessed 19 November 2016.

introduces the data subjects' right to data portability, which enables the individuals to receive their personal data provided to one data controller and transmit them to another data controller, provided that the processing is based on the data subject's consent or contract, or the processing is carried out by automated means.

# 3 ADEQUACY OF THE NEW EU – U.S. PRIVACY SHIELD. REALITY or MYTH?

After a long period of negotiations between the European Union and the United States and in view of the impact of the CJEU decision regarding the *Schrems* case, on 2 February 2016 the European Commission and the U.S. Department of Commerce reached a political agreement for the replacement of the invalidated Safe Harbour with the EU – U.S. Privacy Shield Agreement with regard to the establishment of a new framework for the transatlantic data flows between the EU and the U.S.[224]. On 29 February 2016 the European Commission issued a Draft Adequacy Decision and the Annexes attached to it which constituted the basis of the Privacy Shield Agreement, and a Communication[225] about the actions taken over the previous years for the enhancement of the security of transatlantic data flows[226]. Finally, the European Commission officially adopted the finalized implementing Decision[227] and the attached Annexes, constituting the EU – U.S. Privacy Shield, on 12 July 2016[228]. The final text of the Decision and the Annexes present insignificant differences from the draft adequacy decision.

The Privacy Shield constitutes the legal instrument which authorizes the transfer of personal data from the European Union to the United States and it is based on the European Commission's main conclusion that the U.S. level of protection is adequate[229]. The assessment of the adequacy of the U.S. legal order and, most of all, the adequacy of the Privacy Shield Framework constitutes the heart of this chapter and it focuses on the following elements: The Privacy Shield Principles, which can be considered as the main

[224] European Commission, 'EU Commission and United States agree on new framework for transatlantic data flows: EU – U.S. Privacy Shield, 2 February 2016, IP – 16 – 216: http://europa.eu/rapid/press-release_IP-16-216_en.htm accessed 20 January 2017.
[225] European Commission, 'Communication from the Commission to the European Parliament and the Council, Transatlantic Data Flows: Restoring Trust through Strong Safeguards' COM (2016) 117 final.
[226] European Commission, 'Restoring trust in transatlantic data flows through strong safeguards: European Commission presents EU – U.S. Privacy Shield', 29 February 2016, IP – 16 – 433: http://europa.eu/rapid/press-release_IP-16-433_en.htm accessed 20 January 2017.
[227] Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU – U.S. Privacy Shield, OJ 2016 L 207/1.
[228] European Commission, 'European Commission launches EU – U.S. Privacy Shield: stronger protection for transatlantic data flows', 12 July 2016, IP – 16 – 2461: http://europa.eu/rapid/press-release_IP-16-2461_en.htm accessed 20 January 2017.
[229] Commission Implementing Decision (n 227), Recital 136, at 39, Article 1, at 43.

body of the Privacy Shield Agreement, the existence of oversight and recourse mechanisms under the Privacy Shield, and the U.S. legislation regulating the access and use of personal data transferred under the Privacy Shield by U.S. public authorities for national security reasons, mostly elaborated in the commitments from representatives of the U.S. Government, contained in the Annexes attached to the Commission Implementing Decision. The examination of the adequacy will be based, among others, on the guarantees and standards of the EU data protection law, which were scrutinized in the previous chapter. It should be emphasized that the functioning of the Privacy Shield scheme is based on a self – certification system[230], similar to the one established within the Safe Harbour scheme, however it appears to have been improved and strengthened with the aid of crucial guarantees which have been introduced with the Privacy Shield Agreement. Only these U.S. organisations which will self – certify their adherence to the Privacy Shield Principles, analysed in Annex II attached to the Decision, will be able to process personal data transferred from the European Union to the United States. It should be noted that the Privacy Shield concerns not only controllers, but also processors[231] who have entered into contract with an EU controller in order to act on the instructions of the latter and according to the Privacy Shield Principles. The administration and monitoring of the Privacy Shield belong to the Department of Commerce, while the Federal Trade Commission and the Department of Transportation are responsible for the enforcement of the Principles[232].

## A. The Core of the EU – U.S. Privacy Shield: The Privacy Shield Principles

The main body of the Privacy Shield Agreement consists of seven Main Principles and sixteen Supplemental Principles whose existence aims to ensure the adequacy of the Privacy Shield with regard to the effective protection of the processing of personal data. It has to be made clear that the Privacy Shield Principles constitute the evolution of the Safe Harbour Principles, in the wake of the *Schrems* ruling by the CJEU and the GDPR.

[230] Commission Implementing Decision (n 227), Recital 14, at 4.
[231] Commission Implementing Decision (n 227), Recital 14, at 5.
[232] Commission Implementing Decision (n 227), Recital 18, at 6.

The Principle of Notice[233] defines the amount of information an organization has to provide to individuals regarding the transfer of their personal data. The Privacy Shield agreement analyses more deeply, compared to the Safe Harbour Agreement, the exact obligations of the organisations. It reiterates the obligations set out in the Safe Harbour regarding the need for the organization to inform, in an explicit way, the individuals on the purposes of the collection and processing of personal data, the possible ways of contact with the organization, the information on the third parties the personal data are disclosed to, as well as the means that the organization puts into practice for the limitation of the use and disclosure of personal data. The Privacy Shield Agreement adds that the organization must clarify in advance its participation in the Privacy Shield scheme, providing, at the same time, a link or a web address for the Privacy Shield list and explicitly state its commitment to abide by the Principles of the Privacy Shield agreement. Furthermore, the organization must from now on describe with great details the independent dispute resolution body for the case of complaints, provide free of charge recourse to individuals, as well as refer to the possibility of the binding arbitration as a last resort solution. Moreover, the organization is obliged to acknowledge its liability in the case of the disclosure of personal data in the case of onward transfers to third parties and to inform individuals on the requirement to respond to lawful requests by U.S. authorities for national security or law enforcement reasons. The new binding rules are, undoubtedly, considered to promote the transparency of the new framework and safeguard the personal data of EU citizens.

The Principle of Choice[234] reiterates, to a great extent, the content of the Principle of Choice of the Safe Harbour Agreement, without considerable changes. An organization must provide individuals with the ability to decide whether they wish their personal data to be disclosed to third parties, or be used for purposes materially different from the initial purposes the personal data have been collected for. The Privacy Shield clarifies that the principle of choice is not applicable in the case the third party is in fact an agent the organization has entered into contract with. Finally, the Privacy Shield reiterates the

[233] Commission Implementing Decision (n 227), Recital 20, at 6, and, Annex II attached to the Commission Implementing Decision, Section II.1., at 19 – 20.
[234] Commission Implementing Decision (n 227), Recital 22, at 6 – 7, and, Annex II attached to the Commission Implementing Decision, Section II.2., at 20.

obligation for an explicit affirmative consent of individuals in the case of sensitive personal data for the abovementioned cases. The Decision, referring to the Principle of Choice, states that individuals have to right to object[235] (opt – out) whenever a new purpose is materially different from the original purpose, but still compatible with the Principles, whereas in the field of direct marketing the opt – out is allowed at any time. Undoubtedly, the reference to the right to object, in the particular case of the modification of the original purpose and in the general field of direct marketing, can be characterized as encouraging for the protection of data subjects, however, the right to object at any time should not be limited solely in direct marketing, neither this right should depend on the change of the purpose of the processing. The enshrinement of a general right to object based on any compelling legitimate grounds, taking into account the particular situation, is considered as necessary in order to meet the standards of the respective right enshrined in the EU Data Protection Directive and the GDPR[236]. Generally, the Principle of Choice, in conjunction with the Principle of Notice, gives the impression that the processing of personal data is not based on specific criteria, relevant to the standards set by Article 7 of the EU Data Protection Directive[237].

The Principle of Accountability for onward transfer[238] regulates two types of onward transfers of personal data to third parties, depending on whether the latter act as a controller or an agent of the organization. In both cases, the transfer and processing of personal data, on behalf of both types of third parties, must occur according to specified and limited purposes, with respect to the Privacy Shield Principles and the contract they have entered into with the organisation. In case the third party makes a determination stating that it cannot abide by these obligations, the organization must be notified.

[235] Commission Implementing Decision (n 227), Recital 22, at 6.
[236] See also Article 29 Working Party, 'Opinion 01/2016 on the EU – U.S. Privacy Shield draft adequacy decision' (WP 238, 13 April 2016) at 20.
[237] Franziska Boehm, 'Assessing the New Instruments in EU – US Data Protection Law for Law Enforcement and Surveillance Purposes' (2016) 2 European Data Protection Law Review at 189.
[238] Commission Implementing Decision (n 227), Recital 28, at 8, and, Annex II attached to the Commission Implementing Decision, Section II.3., at 21.

According to the Principle of Security[239], the organisations are obliged to undertake the appropriate measures in order to ensure the security of personal data against potential risks of loss, exploitation for unlawful purposes or unauthorized access, disclosure, dissemination or destruction of the personal data at issue, with respect to the different types of these personal data. The Privacy Shield bears almost no difference to this particular point in relation to the Safe Harbour.

The next principle constitutes the lynchpin of the data protection framework generally and this is the Principle of Data Integrity and Purpose Limitation[240]. In comparison to the respective principle of the Safe Harbour, the Privacy Shield principle is more explanatory and detailed, taking into account the fact that the purpose limitation principle is now explicitly stated in the title. The Privacy Shield sets out that personal information 'must be limited to the information that is relevant for the purposes of processing', adding that is prohibited for the organization to process personal information in an incompatible manner with the initial purposes for which the data have been collected, or the purposes authorized by the data subjects. It is interesting, though, to mention the opinion of the Working Party of Article 29, according to which the exact phrase of the Annex II, regarding the limitation of personal data to the information that is relevant for the purposes of the processing, cannot be considered to fully respond to the EU standard of necessity and proportionality, since the wording should clearly state that personal data should be limited to the information that is necessary (not simply relevant) for the purposes of processing[241]. The EDPS does not agree with the abovementioned phrase as well, recommending that the principle should state that personal information should be adequate and not excessive or limited to the information that is necessary for the purposes of the collection and processing[242]. Furthermore, the organizations must safeguard the safety and accuracy of the personal data during the period of processing. The abovementioned have also been mentioned in the Safe Harbour Decision, however the main difference is that the Privacy Shield refers to the

[239] Commission Implementing Decision (n 227), Recital 24, at. 7, and, Annex II attached to the Commission Implementing Decision, Section II.4., at 21.
[240] Commission Implementing Decision (n 227), Recital 21 and 23, at 6 – 7, and, Annex II attached to the Commission Implementing Decision, Section II.5., at 21 – 22.
[241] Article 29 Working Party (n 236), at 23.
[242] European Data Protection Supervisor (EDPS), 'Opinion 4/2016: Opinion on the EU – U.S. Privacy Shield draft adequacy decision', 30 May 2016, at 9.

retention of personal data as well, stipulating that the duration of the retention period is determined by the purpose of processing. According to the wording of the principle, personal information can be retained 'for as long as it serves a purpose of processing', while it is possible for the processing period to be extended if this is deemed as necessary for the purposes of public interest, journalism, literature and art, scientific or historical research and statistical analysis. Nevertheless, taking into account the observations of the Working Party of Article 29[243] and the EDPS[244], it has to be mentioned that this Principle does not set out an explicit rule of the erasure of personal data after the termination of the period during which the processing of the personal data has been carried out for specific purposes. The erasure of the personal data that are no longer needed for the purposes for which have been collected and processed constitutes an important standard of the EU data protection framework based on the right to be forgotten and Articles 12 of the Directive 95/46/EC and Article 17 of the GDPR, hence the absence of a clear reference of the Privacy Shield to this issue implies the absence of a time limit for the retained data[245], in breach of the respective EU principle.

The Principle of Access[246] reiterates the content of the respective Safe Harbour Principle. Personal data have to be accessible for each and every data subject, which, according to the Supplemental Principles referring to the right of access[247], has the meaning that the individuals have the right to obtain confirmation of whether an organization is processing their personal information, to gain knowledge of the content, to be able to verify the accuracy and lawfulness of the processing and to be able to correct, amend or delete the data which are inaccurate or processed in an incompatible manner regarding the Privacy Shield Principles. Nevertheless, pursuant to the principle it may be possible that the right of access could be considered as disproportionate to the risks to individuals' privacy or the violation of rights of others than the owner of personal data.

[243] Article 29 Working Party (n 236), at 17.
[244] European Data Protection Supervisor (n 242), at 9.
[245] Article 29 Working Party (n 236), at 17.
[246] Commission Implementing Decision (n 227), Recital 25, at 7, and, Annex II attached to the Commission Implementing Decision, Section II.6., at 22.
[247] Annex II attached to the Commission Implementing Decision, Section III.8., at 31.

The last principle is referred as the Recourse, Enforcement and Liability Principle[248]. The Privacy Shield stresses the need for the existence of effective, independent recourse mechanisms which will investigate and address individuals' complaints and award damages pursuant to the applicable law. What is more, it is emphasized that the organisations' privacy policies and practices ought to be verified through follow – up procedures, and cases of non – compliance must be addressed through sufficient sanctions imposed to the organisations at issue. The Privacy Shield, compared to the Safe Harbour, puts the emphasis on the importance of the prompt response of the recourse mechanisms, set by the organisations, to individuals' complaints and inquiries on behalf of the Department of Commerce. In the case of the invocation of binding arbitration, the organisations must abide by the specific rules set out in the Privacy Shield Agreement regarding this issue. With reference to onward transfers, it is clearly stated that the organizations which receive transferred data from the EU and subsequently transfer third parties acting as agents on their behalf are liable for the action of the processing, even if this is carried out in an inconsistent way to the Principles by the agent, unless it is proven otherwise. Finally, there is mention to some details of the investigative powers of the FTC regarding referrals of non – compliance.

Section III of Annex II[249] attached to the Decision of the Privacy Shield Agreement refers to supplemental principles, many of which preexisted in the Safe Harbour. There are specific provisions which introduce particular regulations regarding different categories of personal data, such as sensitive data, data related to journalism, human recources data, travel information and medical data, as well as provisions which refer to specific issues, such as the role of the DPAs, the procedure of self – certification and verification under the Privacy Shield, and issues related to the role of recourse mechanisms and the enforcement of the Privacy Shield.

[248] Commission Implementing Decision (n 227), Recital 26, at 8, and, Annex II attached to the Commission Implementing Decision, Section II.7., at 22 – 23.
[249] Annex II attached to the Commission Implementing Decision, Section III, at 24 – 46.

## B. Supervision and Enforcement of the EU – U.S. Privacy Shield: The Role of the Department of Commerce and the Federal Trade Commission

### 1. The Department of Commerce

The details of the role of the Department of Commerce (DoC) are included in Annex I, attached to the Commission Implementing Decision. Annex I is composed of Annex 1, namely the Letter from Acting Under Secretary for International Trade which contains the commitments of the Department of Commerce as far as the monitoring of the Privacy Shield is concerned, and Annex 2 which presents the new arbitral model in the framework of the Privacy Shield mechanism. An important development, in comparison with the previous regime of the Safe Harbour, is the obligation of the Department of Commerce to make publicly available the list of the U.S. organisations[250] that have decided to self – certify to the Department and acknowledge their adherence to the Privacy Shield Principles, as well as update this list whenever any changes, such as an addition or removal of a U.S. organization, emerges. At the same time, all organisations under the Privacy Shield are obliged to provide a hyperlink to the Privacy Shield website and the available complaint submission form[251], a step which promotes transparency. The DoC shall verify if the publicly available privacy policies of the certified organisations are compatible with the Privacy Shield Principles[252]. Despite these positive changes, it should be taken into consideration that there is no explicit legal basis for the authorization of the abovementioned actions, other than the commitments of the DoC in the context of the Privacy Shield Agreement. Consequently, there is no explicit legal obligation which would bind the Department of Commerce to uphold these changes.

Regarding the Privacy Shield List, it is evident that for each organization certified and included in the List there is a reference to the category of 'covered data' at issue. The List has created two categories, HR data which refer to personal data about the organization's

[250] This list can be found here: https://www.privacyshield.gov/list accessed 2 February 2017.
[251] Commission Implementing Decision (n 227), Recital 32, at 10.
[252] Commission Implementing Decision (n 227), Recital 32, at 10.

own employees collected in the context of the employment relationship, and non – HR regarding all the rest of personal data. By clicking on the name of each organization, one can find a short description of the type of personal data transferred from the EU and the purpose of this transfer. In addition to the list of the active organisations self – certified under the Privacy Shield, the Department of Commerce is also responsible for drawing up the list of the organisations which have been removed from the Privacy Shield list stating that they are no longer bound by the Principles, except for cases of personal data acquired during the period of their participation in the Privacy Shield[253]. Furthermore, the Department of Commerce is competent to verify if the organization wishing to self – certify under the Privacy Shield satisfies all the necessary requirements relevant to the adoption of the appropriate privacy policy in accordance with the Privacy Shield Principles[254]. As far as the removed from the Privacy Shield list organisations are concerned, the Department of Commerce must review on a periodic basis the privacy policies of these organisations and certify that their privacy policies do not imply that they are still participating in the Privacy Shield[255].

A major responsibility of the Department of Commerce is related to the monitoring of the effective operation of the Privacy Shield mechanism. Therefore, the DoC is obliged to conduct periodic ex officio compliance reviews through detailed questionnaires sent to the participating organizations in order to constantly address any arising critical issues[256]. It should be emphasized that the DoC, through the dedicated website to the operation of the Privacy Shield, has been able to provide essential information depending on the different audiences, namely the U.S. businesses, the EU businesses, the EU individuals and the DPAs. Regarding the EU individuals[257], it is, undoubtedly, quite positive the fact that the DoC, through the website of the Privacy Shield, informs the EU individuals on the different rights they are entitled to under the Privacy Shield Agreement, the proper manner of

[253] Annex I attached to the Commission Implementing Decision, Annex 1, at 6. These organisations are considered as 'inactive organisations' and the list is included in this link: https://www.privacyshield.gov/inactive. So far, this list does not contain any organisations.
[254] The exact self – certification requirements are analysed in Annex I attached to the Commission Implementing Decision, Annex 1, at 6 – 7.
[255] Annex I attached to the Commission Implementing Decision, Annex 1 at 7 – 8.
[256] Annex I attached to the Commission Implementing Decision, Annex 1 at 9.
[257] https://www.privacyshield.gov/Individuals-in-Europe accessed 2 February 2017.

submitting a complaint, the multitude of recourse mechanisms existing for the handling of the complaints, and the process of submitting a request to the Ombudsperson for issues of access to personal data by the U.S. authorities for the purpose of national security. The DoC focuses on improving the cooperation with the DPAs, through the establishment of a dedicated contact acting as a liaison with the DPAs[258] for the receipt of a referral of an organization for further review. In case of complaints from the DPAs regarding organisations which do not comply with the Principles, the DoC is committed to provide an answer to these complaints within 90 days[259]. Finally, the DoC, along with other agencies, will participate with the European Commission, the DPAs and representatives of the Working Party of Article 29 in the meetings during the period of the annual review of the Privacy Shield. The DoC has been criticized for its limited role, due to the fact that it is responsible for the verification of the formal requirements for the self – certification of the organisations, rather than proceed to the assessment of the substantial compatibility of the organisations' privacy policies with the Privacy Shield Principles[260].

### 2. The Federal Trade Commission

The main mission of the Federal Trade Commission is pertinent to the enforcement of the new Privacy Shield mechanism. The Letter from Federal Trade Commission Chairwoman, included in Annex IV, stipulates that the protection of consumer privacy and competition has been the highest priority for the FTC, as this is evident in the FTC Act which constitutes the legal instrument which prohibits unfair methods of competition and unfair or deceptive commercial practices. The main, though, characteristic of the FTC action remains its strong enforcement powers when it comes to the protection of consumer privacy and security[261]. The Letter certifies that the FTC Act yields benefits not exclusively to U.S. consumers, but to EU consumers as well[262], stating that Section 5 of the FTC Act, related to the prohibition of unfair or deceptive commercial acts or practices, applies to U.S. and foreign consumers and persons who are generally engaged in commerce. The FTC

[258] More information can be found here: https://www.privacyshield.gov/article?id=DPA-Liaison-at-Department-of-Commerce accessed 2 February 2017.
[259] Annex I attached to the Commission Implementing Decision, Annex 1 at 10.
[260] Article 29 Working Party (n 236), at 28.
[261] Annex IV attached to the Commission Implementing Decision, Section I.A., at 61 – 62.
[262] Annex IV attached to the Commission Implementing Decision, Section I.B., at 62.

has brought enforcement actions, during the period of the operation of the Safe Harbour, in multiple cases. Three of these cases[263] concerned Google, Facebook and MySpace, which were required, pursuant to the consent orders, to adopt effective privacy policies ensuring the protection of the confidentiality of personal data and to refrain from any attempt of misinterpretation of their privacy policies. These obligations, as it is noted in the Letter, are still valid under the Privacy Shield Agreement.

The main commitment of the FTC, with regard to the implementation of the new Privacy Shield Framework, is focused on the prioritization of referrals from EU Member Stated regarding issues of non – compliance through a standardized referral process which is being created by the FTC and aims to provide aid to EU Member States and facilitate the referral process, while a special agency point of contact will be designated. The FTC is committed to proceed into a wide range of actions to solve the issues, including, among others, the review of the privacy policy of the organisations, the assessment of the potential violations and the exchange of information with the DPAs and the referring enforcement authorities[264]. However, these statements remain, so far, solely the commitment of the Federal Trade Commission and they have not still been put into practice, since the official website of FTC simply reiterates the content of the Letter of Annex IV, without providing any additional information.

Apart from the abovementioned, the FTC is committed to address cases of deceptive behavior of organization and monitor enforcement orders with the purpose to safeguard the effective operation of the Privacy Shield mechanism and the compliance with the Privacy Shield Principles. For this reason, the FTC will also participate in periodic meetings with the DPAs and representatives of the Working Party of Article 29 for the improvement of the enforcement process, as well as in the annual review of the Privacy Shield Framework, along with the DoC, the European Commission and representatives of the Working Party of Article 29.

The Working Party of Article 29 generally approves the enhanced role of the DoC and FTC especially regarding the compliance reviews, the enforcement of the Privacy

[263] Annex IV attached to the Commission Implementing Decision, Section I.C., at 63.
[264] Annex IV attached to the Commission Implementing Decision, Section II, at 64 – 65.

Shield Framework and additional investigatory powers, implying that these advancements have certainly addressed a lot of shortcomings faced under the Safe Harbour. However, the Article 29 Working Party expresses doubts about the practical implementation of the commitments undertaken by the FTC and the DoC, particularly about the issue of the on – site inspections on the premises of the organisations. Regarding this specific issue, the European Data Protection Supervisor has also expressed the need for clarification taking into account paragraph 81 of the *Schrems* ruling which considers that a well – established self – certification system must be able to possess effective oversight mechanisms which will be able to detect and address any cases of infringements of the data protection rules at any time[265]. Other problematic issues refer to the effective enforcement of EU authority decisions on US territory, and the degree of deterrence of the Privacy Shield sanctions[266].

## C. Recourse Mechanisms under the EU – U.S. Privacy Shield

One of the greatest differences of the Privacy Shield Framework from the precious regime of the Safe Harbour is related to the significant enhancement of the recourse mechanisms for the effective response to EU data subjects' complaints with reference to cases of non – compliance and violations of the Privacy Shield Principles. The main characteristic is that the Privacy Shield sets out a multi – layered redress system[267] in order to satisfy the standards of the Recourse, Enforcement and Liability Principle.

The first layer consists in direct contacts with the U.S. self – certified organization at issue. It is absolutely mandatory that the organisations should put into practice effective recourse mechanisms and the response period to the complaints of EU data subjects is set to 45 days. The EU data subjects are able to choose, instead of the first layer, the second one which is comprised of the independent dispute resolution body, either in the United States or the European Union, designated by the organization at issue. The Decision clarifies that these mechanisms must be able to investigate the individuals' complaints and undertake the appropriate measures to remedy the situation, by ordering, for instance, the

[265] See European Data Protection Supervisor (n 242), at 10.
[266] Article 29 Working (n 236), at 30.
[267] Commission Implementing Decision (n 227), Recitals 41 – 63, at 12 – 16.

termination of the processing carried out in breach of the Privacy Shield Principles, or the deletion of the personal data at issue. The registration of the U.S. organizations to independent resolution bodies is subject to investigation and verification on behalf of the DoC, while the constant refusal of the organization to comply with the decisions of the independent recourse bodies may lead to its removal from the Privacy Shield List by the Department of Commerce. The Privacy Shield provides to data subjects the ability, if they wish, to bring their complaints before the EU National Data Protection Authorities (DPAs). Throughout the Privacy Shield[268], it is evident that U.S. organisations are advised to cooperate on good terms with the EU DPAs for the stronger implementation of the Privacy Shield and its safeguarding against cases of non – compliance, responding to their inquiries and taking into consideration the DPAs' advice on the proposed actions. This advice is provided by the panel of the DPAs, whose details are provided in Section III, 5c of Annex II, attached to the Decision. The fourth layer of the recourse system is relevant to the significant role of the Department of Commerce, which is also competent to receive and address individuals' complaints for cases of non – compliance. There has already been made reference to the commitment of the DoC regarding the establishment of a contact point as a liaison with the DPAs and its power to strike an organization from the Privacy Shield List in the case of persistent failure for the organization to comply with the Principles. In addition to the abovementioned, another layer refers to the Federal Trade Commission and its enforcement powers, which has also been mentioned. On behalf of the FTC, the compliance is enforced through the consent orders, which technically constitute administrative orders, and, additionally, it may refer the case to the competent court which will be responsible for ordering the appropriate remedies for the individuals.

One of the most important institutional changes is the introduction of the 'Privacy Shield Panel' which constitutes a recourse mechanism of last resort, in case all the previous existent redress mechanisms fail to succeed. According to the Privacy Shield Agreement[269] it is the obligation of the organisations to inform the individuals regarding the possibility of invoking binding arbitration under the Privacy Shield Panel, pursuant to the Principle of

[268] A representative example is of Annex II attached to the Implementing Decision, Section III.5., at 25 where it is stated that 'Organisations will implement their commitment to cooperate with European Union data protection authorities (DPAs)'.
[269] Commission Implementing Decision (n 227), Recitals 56 – 57, at 15.

Notice. The Agreement stipulates that this panel shall be designated by the Department of Commerce and the Commission and will be composed of, at least, 20 arbitrators renowned for their independence, as well as their professionalism. It is clarified that the parties involved in an individual dispute will be responsible for the selection of one or three arbitrators, as the final composition of the panel. Individuals who invoke arbitration are not entitled to claim damages, since the role of the arbitration panel is to impose 'individual – specific, non – monetary equitable relief'[270], which may result into the correction or even the deletion of the personal data processed in breach of the Principles. In Annex I regarding the Arbitral Model, it is stated that the set of U.S. arbitral procedures between the Department of Commerce and the European Commission is to be adopted within a period of six (6) months from the adoption of the Commission Implementing Decision of the Privacy Shield, however this has not happened so far, undermining, thus, the role of the Privacy Shield Panel. Also, the persistence that the arbitrators who will comprise the Privacy Shield Panel, according to Annex I regarding the Arbitral Model, must be admitted to practice law in the U.S. and be experts in U.S. privacy law, with expertise in EU data protection law, could be interpreted as a general preference for the U.S. law over the EU legal system[271].

As a general comment on the multi – layered structure of the Privacy Shield recourse mechanism, the Article 29 Working Party welcomes these improvements, however it notes that there is a possibility that the operation of these mechanisms may not be successful as planned due to the complexity of the multiple layers which comprise the redress system, resulting into the supremacy of the quantity over the quality[272].

[270] Commission Implementing Decision (n 227), Recital 58, at 15.
[271] Christopher Kuner, Paper No 14 'Reality and Illusion in EU Data Transfer Regulation Post Schrems', March 2016, Legal Studies Research Paper Series, University of Cambridge, at 21.
[272] Article 29 Working Party 29 (n 236), at 26. Also, Franziska Boehm (n 237), at 189.

## D. Social Networking Platforms and EU – U.S. Privacy Shield: The Case of Facebook

Before examining the U.S. legal order with reference to the Privacy Shield and the use of personal data by U.S. authorities, it is important to underline the role of social networking platforms, notably of Facebook, within the framework of Privacy Shield. The greatest company in the field of social networking platforms, Facebook Inc., decided to self – certify under the EU – U.S. Privacy Shield on 30 September 2016[273] regarding the collection and processing of personal data from the advertisers, customers or business partners in the European Union. According to the Facebook Privacy Shield Notice[274], the participation of Facebook Inc. in the EU – U.S. Privacy Shield does not include the whole of the activities of Facebook Inc. for it is limited solely to two specific areas. More specifically, the first area refers to the Workplace, a service which allows the collaboration and sharing of data at work. The organisations or employers are considered as the data controllers, since they submit to Facebook personal data of their members, while Facebook Ireland is the processor and Facebook Inc. the sub – processor. The second area which falls within the Privacy Shield relates to the advertising services provided by Facebook, for which personal data are provided by Facebook's advertisers and business partners in the European Union and they refer to individuals' preferences and experiences about specific products or advertisements. In this case, as well, Facebook Ireland remains the processor and Facebook Inc. the sub – processor. The Facebook Privacy Shield Notice states that the transfer of the aforementioned categories of personal data is carried out with respect to the Privacy Shield Principles and aims to advance the services provided by Facebook regarding these areas. Facebook Inc. underlines that it will take the appropriate measures to ensure the individuals' right of access to their personal data, as well as their right to correct, amend or delete inaccurate data. Furthermore, it is affirmed that the personal data at issue can be further transferred to Facebook's family of companies (including Instagram and WhatsApp) and to third parties, according to the Privacy Shield rules. One important issue is that Facebook Inc. directly states that personal data may be disclosed in cases of legal

[273] The profile of Facebook Inc. in the Privacy Shield List can be found here: https://www.privacyshield.gov/participant?id=a2zt0000000GnywAAC accessed 2 February 2017.
[274] https://www.facebook.com/about/privacyshield accessed 2 February 2017.

requests and judicial orders. Finally, Facebook Inc. refers to TRUSTe which constitutes the alternative dispute resolution body, based in the United States, pursuant to the requirements set out in the Privacy Shield Agreement. Generally, the adequacy of the Privacy Shield especially in the field of the social networking platforms will still be based on the general provision of the Privacy Shield and the relevant provisions of the U.S. legislation.

It is important to note that only a small part of Facebook's activities is regulated under the Privacy Shield. However, this does not mean that the transfer of personal data of EU citizens is limited only to the abovementioned categories. Facebook Ireland Ltd. is able to transfer EU citizens' personal data to Facebook Inc. pursuant to other legal means. One of these refers to the Standard Contractual Clauses (SCCs)[275], pursuant to the Data Transfer and Processing Agreement, made between Facebook Ireland Ltd. and Facebook Inc. and entered into force on 13 November 2015. However, Maximilian Schrems submitted a reformulated complaint against the validity of the SCCs within the Data Protection Commissioner, who initiated proceedings before the Irish High Court against Facebook Ireland Ltd. and Schrems, asking from the Irish High Court to make a reference to the CJEU regarding the validity of the SCCs[276].

## E. U.S. Legislation on the Access and Use of Personal Data by the U.S. Authorities

As it has already been elaborated, the EU regime regulating the processing of personal data is characterized as an omnibus regime with the specific traits analysed in the previous chapter. On the other hand, the US regime has been characterized as 'sectoral' or 'sectional'[277], lacking the horizontal character of the EU legislation. The main deficiencies of the U.S. data protection system are related to the limited protection of the rights of the

[275] The text can be found here: http://www.europe-v-facebook.org/comp_fb_scc.pdf accessed 10 February 2017.
[276] The progress of "Data Protection Commissioner v. Facebook Ireland Ltd and Maximilian Schrems" can be found here: http://www.europe-v-facebook.org/MU_HC.pdf accessed 2 February 2017.
[277] Orla Lynskey, *The Foundations of EU Data Protection Law* (1st edn, OUP, 2015) at 15.

private sector, since the U.S. perspective treats privacy mostly as a right which has to be protected against the governmental interferences[278]. The Privacy Act of 1974[279] is focused on the public sector, particularly on the activities of federal agencies concerning the processing of personal data. The comprehension of the data protection legal system of the United States cannot be considered as an easy task due to the existence of different legislations among the states. The private sector is regulated by specialized legislative initiatives and self – regulation rules[280], unlike the horizontal character of the EU data protection framework. Generally, the role of the government is rather limited in practice, since markets and industries set the rules regarding the regulation of data privacy law.

The Privacy Shield Agreement refers in an extensive way to the boundaries of the US public authorities regarding the access and processing of personal data of European citizens and the relevant provisions of the US legislation, as these have been shaped by the recent amendments in the wake of the revelations of Edward Snowden, the *Schrems* ruling and the subsequent collapse of the Safe Harbour. The Commission Implementing Decision, as well as Annex II attached to the Commission Implementing Decision, Section I.5, emphasize that adherence to the Privacy Shield Principles can be limited to the extent this is deemed necessary in order to meet national security, public interest or law enforcement requirements[281]. Section I.5 adds that such limitations can, also, occur in the case of conflicting obligations or explicit authorisations created by statute, government regulation of case law, provided that the non – compliance of the organization is justified by certain legitimate interests considered of utmost importance. What is more, the Privacy Shield Agreement acknowledges the legal value of exceptions or derogations which are provided for by the Directive or by the Member States' national legislation. It is important to trace that, in case there is certain derogation permitted under the Principles of the Privacy Shield Agreement and/or the U.S. law, then the organisations must comply with the solution offering the highest, as much as possible, protection. The abovementioned rules enshrined in the Section I.5 of the Privacy Shield constitute a mere reiteration of the 4th paragraph of

[278] Lee A. Bygrave, *Data Privacy Law: An International Perspective* (1st edn, OUP, 2014) at 112.
[279] Privacy Act of 1974, 5 United States Code §552a, Pub. L. 93 – 579, 88 Stat. 1896.
[280] Orla Lynskey (n 277) at 17.
[281] Commission Implementing Decision (n 227), Recital 64, at 16, and, Annex II attached to the Commission Implementing Decision, Section I.5, at 17 – 18.

the Safe Harbour. However, the Safe Harbour, in Annex IV, Part B, provided for specific clarifications regarding the role and meaning of the conflicting obligations and explicit legal authorization under the U.S. law, which can, under circumstances, permit the emergence of derogations from the Principles. The CJEU criticized the statement of the Safe Harbour, according to which in cases where the U.S. legislation creates conflicting obligations for the U.S. organisations, the latter must comply with the U.S. law whatsoever, irrespective of whether they are certified under the Safe Harbour or not. More specifically, in *Schrems*[282], the CJEU found that this particular statement implies the primacy of the U.S. law over the rules and principles set out in the Safe Harbour, allowing, thus, to the U.S. organisations to derogate from the principles in a generalized manner and comply with the U.S. law. The Privacy Shield Agreement has maintained the exact content of the fourth paragraph of Annex I of the Safe Harbour, located, now, at Section I.5 of Annex II. However, the Privacy Shield does not make any particular reference to the conflicting obligations or explicit authorisations under the U.S. law, omitting, thus, the criticized by the CJEU statement regarding the preferred compliance with the U.S. law in the case of conflicting obligations. Despite this positive change, the reiteration of the wording of Safe Harbour has provoked criticism, for the mentioned derogations from the Principles can be considered as broad[283] and not precise enough[284], while the fact that, according to Section I.7, the U.S. law will generally apply in cases of interpretation and compliance with the Principles, can be seen as a statement in favour of the supremacy of the U.S. law over the autonomous EU data protection legal framework in spite of the observation of the CJEU in *Schrems* case over this particular issue[285].

## 1. The Presidential Policy Directive No 28 (PPD – 28)

A significant improvement of the Privacy Shield can be found within the particularly detailed reference to the U.S. law and the recent amendments that have taken place, especially after the revelations of Edward Snowden, for the safeguarding of the rights of

[282] *Schrems* (n 189) paras 84 – 86.
[283] Christopher Kuner (n 271), at 21.
[284] European Data Protection Supervisor (n 242), at 8.
[285] Christopher Kuner (n 271), at 21.

U.S. and E.U. citizens over their personal data. Annex VI attached to the Commission Implementing Decision includes the letter from Robert Litt, the General Councel of the Office of the Director of National Intelligence which refers to the critical issue of the limitations imposed on the U.S. public authorities regarding the collection and access of personal data for national security reasons.

The Presidential Policy Directive No 28[286] ('PPD – 28'), issued by the former U.S. president Barack Obama on 14 January 2014, constitutes a different, compared to other U.S. surveillance laws, such as the Foreign Intelligence Surveillance Act, legal instrument which introduces several reforms and sets out specific guidelines related to signals intelligence activities and the collection of foreign intelligence. However, it should be clarified that PPD – 28 does not constitute a per se legal basis for the authorization of signal intelligence activities, since its main role consists in the adoption of these guidelines and principles whenever any kind of signals intelligence activities take place[287].

Generally, it is emphasized throughout the PPD – 28 that signal intelligence activities have to be consistent with the essence of individuals' fundamental right to the protection of their privacy, irrespective of their nationality and residence. The directive sets out four basic principles with regard to signal intelligence activities[288]. Firstly, each and every signals intelligence activity which involves the collection of individuals' personal data can only be initiated provided there is an explicit and clear legal basis, such as statutes, Executive Orders, proclamations or any kind of Presidential Directive, whose content must be respected by the intelligence agencies. Secondly, it is reiterated that the notion of privacy and, generally, the essence of civil liberties have to be taken into account and constantly be borne in mind by the intelligence agencies, whose activities must serve specific foreign intelligence purposes for the protection of national security. Thirdly, the collection of commercial information and trade secrets can only be justified under the need of the protection of national security, while it is explicitly forbidden for the U.S. government to exploit these data for the financial support of U.S. businesses and companies

[286] https://www.whitehouse.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities accessed 10 January 2017.
[287] Article 29 Working Party (n 236), at 35.
[288] Presidential Policy Directive No 28 (PPD – 28), Section 1.

at the expense of the rest companies. Finally, the last principle clarifies that the activities of signal intelligence agencies must be 'tailored as feasible', which means that they ought to examine whether the desired information can be collected from diplomatic or public sources, leaving the signal intelligence activities as a last resort for the gathering of signal intelligence. Nevertheless, the Working Party of Article 29 observes that the meaning of the wording of 'tailored as feasible' is not concrete since it not made clear whether the collection of data is necessary and proportionate according to the standards of EU data protection law[289].

Moreover, it is crucial to underline that the PPD – 28 provides for the collection of signals intelligence in a bulk scale. According to the definition[290] given by the PPD – 28, the 'bulk' collection of signals intelligence refers to an authorized collection of 'large quantities of signals intelligence data' without the use of discriminants, such as selection terms or identifiers. More specifically, the directive urges that this bulk collection may be deemed as inevitable, however it serves the purpose of the protection of national security and the proper addressing of present or future threats, which entails a great number of difficulties in the era of modern technologies and digital communication. The directive acknowledges the potential dangers of this action regarding the great possibility of collecting individuals' personal data irrelevant to foreign intelligence, hence the directive sets out six principal limitations during the bulk collection of personal data in order to safeguard, as much as possible, the fundamental right of privacy of individuals. The bulk collection and use of personal data can only occur for the detection and elimination of (i) espionage, (ii) threats related to terrorism, (iii) threats related to the development, possession, proliferation or use of weapons of mass destruction, (iv) cybersecurity threats, (v) military threats to U.S. or allied Armed Forces or other U.S. or allied personnel, and (vi) transnational criminal threats. In addition, it is important to note that the Assistant to the President and National Security Advisor and the Director of National Intelligence are responsible for the annual review of the allowed uses of the signals intelligence gathered in a bulk manner, while these uses will be concentrated in a specific list which will be publicly disclosed, to the extent this is compatible with the purpose of the protection of

[289] Article 29 Working Party (n 236), at 38.
[290] PPD – 28, Section 2, Footnote 5.

national security. Despite the existence of these limitations on the bulk collection of signals intelligence, according to the assessment of the Working Party of Article 29, the purpose limitation cannot be characterized as targeted as the six purposes are quite wide[291]. The main, though, issue is that, despite the existence of limitations, the PPD – 28 explicitly allows the bulk collection of signal intelligence. The *Schrems* decision has emphasized that access on a generalized manner to the content of electronic communications is not consistent with the true meaning of Article 7 of the EU Charter, therefore the authorization of the bulk collection of signals intelligence, even if it is subject to specific purposes, gives rise to doubts about the issue of the essentially equivalent level of protection of the U.S. data protection framework[292].

Section 4 of the PPD – 28 sets out particular principles aiming to ensure a high level of protection in the data protection field with regard to the collected personal data during the signals intelligence activities. The primal principle is the minimization principle, according to which the collected personal data must be retained only for the absolutely necessary time period for the purpose of the protection of national security to be served. The authorization of the dissemination and retention of such personal data are based on the comparable regime set by Executive Order 12333, section 2.3 and applying only to U.S. persons. Moreover, the directive refers to the data security and access principles and stresses the need for the existence of the appropriate safeguards for the security of personal data and the authorization of the access of specific persons to these data for the purpose of the fulfilment of their tasks, in consistence with relevant U.S. legal instruments, such as directives and Executive Orders. Another pillar acknowledged as crucial by the PPD – 28 refers to the need for effective oversight, which will be carried out by the Intelligence Community elements, as well as departments and agencies containing IC elements in cooperation with the Inspectors General of IC elements, responsible for the implementation of the proper measures, including periodic auditing. Furthermore, whenever a case of non

[291] Article 29 Working Party (n 236), at 38.

[292] Christopher Kuner (n 271), at 21. At the same point, he notes that the Commission Implementing Decision in Recital 123 states that 'the United States ensures effective legal protection against interferences by its intelligence authorities with the fundamental rights of the persons whose data are transferred from the Union to the United States under the EU – U.S. Privacy Shield', however the selection of the word 'effective' bears testament to the fact that even the European Commission, deep inside, does not believe that the U.S. level of protection is 'essentially equivalent' to the EU data protection level.

– compliance emerges, the Director of National Intelligence (DNI) shall be necessarily informed as promptly as possible, while if the case concerns personal data of non – U.S. individuals, the DNI and the competent agencies will cooperate with the relevant foreign government for the further handling of the case.

Footnote five (5), which contains the definition of the bulk collection of signals intelligence, contains one significant limitation of the scope of PPD – 28. According to the footnote, the limitations which are contained in Section 2 of PPD – 28 and are reflected on the six principles, which have already been mentioned, do not refer to the temporary acquisition of signals intelligence data aiming to facilitate targeted collection. The meaning of this exception remains obscure since there is no further explanation of it in the text of PPD – 28, however it triggers suspicion and concern especially among the EU data subjects since the bulk collection of signals intelligence data can be exempted from the limitations imposed by PPD – 28 provided that its purpose is to facilitate the adoption of the proper procedures for the detection of the target, and the period of the acquisition remains temporary, without any further reference to the exact time length of this period[293].

## 2. The USA FREEDOM Act

USA FREEDOM Act[294] has been enacted on 2 June 2015 amending several provisions of the Patriot Act and FISA. There are three Sections[295], Sections 103, 201 and 501, which refer to the prohibition of bulk collection of specific types of personal data and the obligatory use of specific selection terms. Section 103 sets as mandatory the use of specific selection terms for the collection of tangible things ordered by FISA court orders. Section 201 sets as mandatory the use of specific selection terms as a basis for the use of the pen register or trap and trace devices, while Section 501 imposes the use of specific selection terms in the cases of the collection of personal information for counterintelligence access to telephone toll and transactional records, financial records and consumer records. As the

[293] See also Daniel Severson, 'American Surveillance of Non – U.S. Persons: Why New Privacy Protections Offer Only Cosmetic Change', Summer 2015, 56 Harvard International Law Journal at 483.
[294] Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline over Monitoring Act of 2015, Public Law 114 – 23.
[295] See also Annex IV attached to the Commission Implementing Decision, Section III, at 89.

Sections elaborate[296], this 'specific selection term' relates to a term that identifies a person, account, address or personal device and its purpose is to limit the collection only to these data which are relevant to this term, 'to the greatest extent reasonably practicable' limiting, thus, the consequences of the bulk collection.

Another critical point of the Act concerns the enhancement of transparency. According to Section 602, the Director of the Administrative Office of United States Courts is responsible for submitting to the House of Representatives and the Senate a complete report, among others, on the number of applications and certifications for orders under FISA, as well as the number of appointments of amici curiae, while the Director of National Intelligence must annually carry out a report on the number of certain types of orders and the number of targets of orders. In both cases, these reports are to be made publicly available on the Internet.

Furthermore, regarding the case of the investigation to obtain foreign intelligence information about non – U.S. persons or cases of international terrorism and clandestine intelligence activities, the Director of the Federal Bureau of Investigation (FBI) is competent to make an application for an order for the production of tangible things. One of the necessary conditions for the issuance of this order by the judge is for the FBI to apply specific minimization procedures for the retention and dissemination of any tangible things[297]. According to 50 U.S.C. § 1861(g), as this has been amended by the USA FREEDOM Act, Section 104.a.2, the minimization procedures are initially adopted and updated by the Attorney General. Their purpose is to minimize the retention and prohibit the dissemination of non – publicly available information which concerns solely U.S. persons. Moreover, information which does not constitute foreign intelligence information cannot be disseminated in a manner which identifies a U.S. person without that person's consent, unless this is deemed necessary for the assessment of foreign intelligence information. The USA FREEDOM Act refers at this point to the power of the Foreign Intelligence Surveillance Court (FISC) to impose additional, particularized minimization procedures for the production, retention and dissemination of non – publicly available

[296] USA FREEDOM Act, Section 107 and Section 201.b.
[297] USA FREEDOM Act, Section 104.a.1.

information concerning U.S. persons who do not offer their consent. However, as it has already been suggested and as Franziska Boehm underlines in her article[298], it is implied that this definition of the meaning of the minimization procedures and the amendments of the USA FREEDOM Act refer only to collected tangible things and personal data existing therein, whose data subjects are solely U.S. persons. In this case, the EU data subjects are put at a serious disadvantage regarding the safety of their own personal data, whereas the EU data protection framework, as it has already been established in the Chapter 2, requires that the collection and processing of personal data should respect the data quality principles and the data minimization principle.

The USA FREEDOM Act refers in an exhaustive manner to the issue of the exception from the rule according to which the access to the requested information presupposes the issuance of judicial order[299]. The production of tangible things can occur even without a judicial order due to the emergency authority of the Attorney General, however the latter must notify and make an application for approval to a judge not later than seven (7) days after the request for the production of tangible things under the emergency clause. It is interesting to notice that, in case the application for approval is denied or it is not issued after the termination of the period of seven (7) days, the received information and the evidence that stems from the tangible things cannot be used during any trial or any kind of proceeding before a court, agency or any other authority of the United States and cannot be used or disclosed in any manner from Federal employees or officers in the case a U.S. person, to whom the information refers to, does not provide his or her consent, unless the information indicates a threat of death[300]. It is important to underline that this measure aiming to secure individuals' personal data is applied only to U.S. persons[301], creating potential dangers for the course of the data of EU citizens which have been transferred to the United States.

In the case of an application for the production of call details records, it is important to note that the USA FREEDOM Act refers to the erasure of these data[302], according to which

[298] Franziska Boehm (n 237), at 184.
[299] USA FREEDOM Act, Section 102.
[300] USA FREEDOM Act, Section 102.i.5.
[301] Franziska Boehm (n 237), at 185.
[302] USA FREEDOM Act, Section 101.b.3.F.vii.

the judicial order may demand from the U.S. Government to implement the proper minimization procedures with the purpose of the destruction of the call details records at issue that do not constitute foreign intelligence information and proceed at their destruction if the minimization procedures require this. However, the main drawback of this regulation refers to its limited scope[303], since only U.S. persons can benefit from this as their call details records do not constitute, under normal circumstances, foreign intelligence information and, hence, can be erased, while this may not be the case for call details records of EU data subjects transferred to the U.S., since they can be considered as foreign intelligence information and, thus, may not be deleted. At this point, it should be underlined that the definition of 'foreign intelligence information', given by 50 U.S.C. Section 1801(e), can be characterized as broad, since it encompasses, among others, information related to a foreign power or territory which affects the national defense or security of the United States, or, also, the conduct of foreign affairs of the United States, without any other reference to the limits of this notion.

With regard to the crucial issue of the interception of metadata through the use of pen registers and trap – and – trace devices and the limitation of their bulk collection, the USA FREEDOM Act has added[304] a new subparagraph in 50 U.S.C § 1842 imposing the obligation for the adoption of privacy procedures under the supervision of the Attorney General for the protection of non – publicly available information collected through the use of pen registers or trap – and – trace registers. However, this information concerns only U.S. persons, leaving, once more, the EU data subjects unprotected[305].

## 3. Section 702 of the Foreign Intelligence Surveillance Act (FISA 702)

Section 702 of the Foreign Intelligence Surveillance Act (FISA) is included in the FISA Amendments Act (FAA) of 2008. It was first signed by George W. Bush on 10 July 2008 and it was due to expire at the end of 2012, and afterwards, on 30 December 2012, the former U.S. President Barack Obama extended its validity until 31 December 2017, having

[303] Franziska Boehm (n 237), at 185.
[304] USA FREEDOM Act, Section 202.
[305] Franziska Boehm (n 237), at 186.

ensured the vote of the House of Representatives and the Senate. The FISA Amendments Act of 2008 amended the FISA and, more specifically, 50 U.S.C. Section 1881. Section 702[306] refers to the targeting of non – U.S. persons and the relevant procedures, authorizing the Attorney General and the Director of National Intelligence to collect foreign intelligence information by targeting non – U.S. persons for a period up to 1 year from the date of the authorization. Section 702 has been the legal basis for the operation of two programs of mass surveillance, PRISM and Upstream. The main deficiency of Section 702 is that it permits the monitoring of non – U.S. persons, even without the issuance of a judicial order, since 50 U.S.C. Section 1881a(c)(2) authorizes the targeting of non – U.S. persons for the acquisition of foreign intelligence information on the basis of a determination by the Attorney General and the Director of National Intelligence stating that, due to the existence of 'exigent circumstances' affecting the national security of the United States, the issuance of the order will have to be skipped.

However, the acquisition of foreign intelligence is subject to certain limitations, which, nevertheless, aim to protect mostly the interests of U.S. persons. More specifically, the targeting cannot refer to persons located in the United States directly or indirectly and it has to be consistent with the Fourth Amendment of the Constitution. As Annex IV attached to the Commission Implementing Decision clarifies, the collection of signal intelligence pursuant to Section 702 of FISA must be consistent with the PPD – 28 and the specific requirements it sets. Furthermore, the Attorney General and the DNI must certify that the targeting of non U.S. persons and the collection of foreign intelligence must be carried out with respect to certain targeting procedures[307] and minimization procedures[308]. The definition of the meaning of minimization procedures is given in Section 1801(h), where it is stated that the acquisition and retention of the information must be minimized and be consistent with the need of collection of foreign intelligence, while the collected information which does not constitute foreign intelligence cannot be disseminated in a manner which could lead to the identification of a U.S. person without their consent. The targeting procedures are necessary in order to certify that the target has no relation to a

[306] 50 U.S.C. Section 1881a.
[307] 50 U.S.C. Section 1881a.(d).
[308] 50 U.S.C. Section 1881a.(e).

U.S. person. Once again, the minimization and targeting procedures seem to protect the U.S. persons, not the non – U.S. citizens.

According to the provision of 50 U.S.C. Section 1881a(h)(1), the Attorney General and the Director of National Intelligence may direct the electronic communications service providers, which include, among others, the commonly known as the Internet Service Providers (ISPs), to help the U.S. Government by providing the necessary information for the accomplishment of the authorized acquisition of foreign intelligence information at issue. In exchange, these electronic communications service providers will be compensated by the Government for their assistance. This provision could well be considered as a double – edged sword, since the danger entailed by the domination of the financial gain could lead to the expansion of the surveillance of EU citizens by the ISPs and other electronic communications service providers for the acquisition of as much foreign intelligence information as possible. This danger has been underlined by Craig Timberg and Barton Gellman who in their article[309] allege that this financial motive could turn surveillance into a 'revenue stream' for many U.S. companies involved in the telecommunication sector. It is interesting to notice that the authors claim that big companies such as Google, Facebook and Apple could also offer their services. Besides, the contribution of these companies to PRISM program and the surveillance of both U.S. and EU citizens is well known.

The Privacy and Civil Liberties Oversight Board (PCLOB) in 2014 issued a report[310] regarding the implementation of Section 702 of FISA. As the ODNI Letter, in Annex IV attached to the Commission Implementing Decision suggests, the main conclusion of this report was that the collection of personal data pursuant to Section 702 of FISA is not carried out in a bulk or indiscriminate manner. In fact, it is advocated that the existing limitations prevent an 'unrestricted collection of information about foreigners'. The PCLOB has found that the operation of Section 702 has efficiently contributed to the

[309] Craig Timberg and Barton Gellman, 'NSA paying U.S. companies for access to communications network', *Wall Street Journal* (London, 29 August 2013): https://www.washingtonpost.com/world/national-security/nsa-paying-us-companies-for-access-to-communications-networks/2013/08/29/5641a4b6-10c2-11e3-bdf6-e4fc677d94a1_story.html?utm_term=.6f5db82dd962 accessed 2 February 2017.

[310] Privacy and Civil Liberties Oversight Board (PCLOB) 'Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act', 2 July 2014, https://www.pclob.gov/library/702-Report.pdf accessed 15 January 2017.

fight against international terrorism and has led to the identification of individuals involved in terrorism[311].

Despite the heavy criticism against Section 702, the USA FREEDOM has not amended any significant part of the subchapter 1881(a). One important change[312] refers to the limitation of the use of unlawfully obtained information. In case a part of the certification or certain procedures are declared as deficient by the FISC, then the information which has been obtained pursuant to this part or these procedures and concerns only U.S. persons cannot be used or disclosed in a trial or any other proceeding in or before any court, agency, department or any other U.S. authority, or be used and disclosed by Federal officers or employees without their consent. Once more, the weakness of this provision lies within the fact that the prohibition of the use and disclosure of illegally obtained information is valid for the U.S persons who are the owners of this information, leaving the EU data subjects at a disadvantage.

## 4. Supervision Mechanisms

Civil liberties or privacy officers constitute one of the multiple oversight mechanisms over the implementation of the intelligence activities carried out by the U.S. authorities. Further details can be found within the Section 803 of Implementing Recommendations of the 9/11 Commission Act of 2007 according to which U.S. departments and agencies, including the Attorney General, the Secretary of State, the Director of National Intelligence and the Director of the Central Intelligence Agency, are to designate at least one (1) officer as principal advisor whose role, among others, is the periodic investigation and review of the respective department or agency regarding the proper implementation of policies and guidelines ensuring the safeguarding of privacy and civil liberties. Subsequently, they are obliged to submit a report to the Congress, the head of the respective department or agency and the PCLOB regarding the accomplishment of their tasks, while it is mandatory that the report become publicly available. Nevertheless, the Article 29 Working Party expresses

[311] Privacy and Civil Liberties Oversight Board (n 310), at 10 and 104.
[312] USA FREEDOM Act, Section 301.

doubts whether the requirement of total independence is satisfied by the existing provisions about the various privacy and civil liberties officers[313].

Another layer of internal oversight is comprised of the mechanism of Inspectors General[314]. According to the amended Inspector General Act of 1978, the Office of Inspector General, established in various departments and agencies, including the Office of the Director of National Intelligence and other intelligence agencies, constitute an independent and objective unit whose mission is to conduct periodic audits and supervise the activities of the departments and agencies, recommending, at the same time, the adoption of the optimal policies for the enhancement of the efficiency of the administrative functioning. The Inspector General, who is considered to be the head of the Office of the Inspector General, is appointed by the U.S. President with the consent of the Senate taking into account factors such as the professional experience and the qualities of the nominee, while, at the same time, the U.S. President remains the only power able to remove the Inspector General. It is emphasized that the appointment of the Inspector General must not rely upon any kind of political affiliation for the safeguarding of the independence of the mechanism revolving around the Inspectors General. The Article 29 Working Party estimates that the abovementioned provisions are likely to satisfy the requirement of the organizational independence of the oversight mechanism[315]. With special reference to the Inspector General of the Intelligence Community, Section 405 of Intelligence Authorisation Act of Fiscal Year 2010 stipulates that the Office of the Inspector General of the Intelligence Community is established within the Office of the Director of National Intelligence and its main role is to conduct independent investigations and audits of programs and activities that fall within the responsibilities of the Director of National Intelligence, as well as to promote the best policies and inform the Director of National Intelligence and the congressional intelligence committees of any arising difficulties or the necessity for corrective measures. The Inspector General of the Intelligence Community, the head of the Office of the Inspector General of the Intelligence Community, is appointed by the U.S. President with the consent of the Senate on the basis of the criteria set out in

[313] Article 29 Working Party (n 236), at 41.
[314] See also Annex VI attached to the Commission Implementing Decision, Section I.d., at 83.
[315] Article 29 Working Party (n 236), at 40.

the general provisions about the Inspectors General. It should be noted that according to Section 405(f)(1) the Director of National Intelligence is capable of prohibiting the Inspector General of Intelligence Community from conducting investigations, audits or reviews if this is deemed necessary for the protection of vital national security interests according to the judgement of the Director, who is obliged to submit to the Congress a statement of the reasons for this prohibition. However there is no other mention in the text which would elaborate the meaning of the 'vital national security interests' and clarify the exact cases where the Director is exceptionally allowed to interfere with the mission of the Inspector General of the Intelligence Community.

Moreover, oversight powers are assigned to the Privacy and Civil Liberties Oversight Board (PCLOB) which constitutes an independent agency within the executive branch pursuant to Section 1061 of the Implementing Recommendations of the 9/11 Commission Act of 2007. It is composed of five member appointed by the U.S. President, with the consent of the Senate, and its main role is to supervise the implementation of the legislation and the pertinent practices of the respective departments and agencies relevant to the fight against terrorism and the protection of the national interests, ensuring, at the same time, that privacy and civil liberties are adequately protected. As far as the degree of independence is concerned, the Working Party of Article 29 acknowledges that the PCLOB 'has demonstrated its independent powers'[316], referring to previous disagreements of the PCLOB with the U.S. President on legal issues such as the telephone metadata program which was declared as inefficient and illegally authorized by the PCLOB.

According to the Rules of Procedure of the Foreign Intelligence Surveillance Court (FISC)[317] in conjunction with 50 U.S.C. Section 1803(a), the FISC is composed of eleven (11) judges designated by the Chief Justice of the United States on the basis of specific criteria, while its jurisdiction extends over applications filed by the Government for a Court order pursuant to relevant statute, and certifications filed by the Government for the targeting of non U.S. persons reasonably believed to be located outside of the United States. It is crucial to mention that the hearings before the FISC are ex parte, meaning that the

[316] Article 29 Working Party (n 236), at 42.
[317] http://www.fisc.uscourts.gov/sites/default/files/FISC%20Rules%20of%20Procedure.pdf accessed 2 February 2017.

concerned persons cannot take part in them. USA FREEDOM Act may have introduced the mechanism of the amici curiae, however they are not supposed to act on behalf of a certain person[318].

## 5. Redress and Available Remedies

The U.S. Supreme Court has elaborated the content of the standing requirement in the case *Lujan v. Defenders of Wildlife*[319]. More specifically, the plaintiff must establish that he has suffered an interference with a legally protected interest, in other words 'an injury in fact' which necessarily must satisfy three conditions. The plaintiff must effectively prove that this injury is (a) concrete and (b) actual, and not hypothetical. Moreover, there must be a causal connection between the injury and the actions that provoked it, meaning that the injury can be attributed to the particular action at issue, and, finally, the injury has to be likely to be redressed by a favorable decision. Generally, it can be said that EU citizens may find difficult to prove in practice that all aspects of the aforementioned standing requirement are met, especially in the cases where individuals are not even aware of the fact that they are surveillance targets.

At this point it would be useful to bear in mind that the Umbrella Agreement was signed on 2 June 2016 and its main content refers to the protection of personal data transferred by law – enforcement authorities as far as the issues of the prevention, investigation, detection and prosecution of criminal offences are concerned. The Judicial Redress Act (JRA) was signed on 24 February 2016 and it is considered as a significant legal instrument for the EU citizens. Its significance lies within the fact that it grants remedies to EU data subjects who are now able to exercise their data protection rights in US courts. It has already been mentioned that a great aspect of the high level of protection offered by the EU data protection framework refers to the judicial review which all data subjects should be able to seek at any moment their rights have been violated. It is crucial to underline that the JRA affects only the sharing of personal data in the field of criminal offences and terrorism and

[318] Article 29 Working Party (n 236), at 41.
[319] (90-1424), 504 U.S. 555 (1992).

its main role is to extend the protection of the Privacy Act of 1974 to EU citizens. Traditionally, the Privacy Act of 1974[320] grants US citizens to ability to bring a civil action before the district courts of the United States against an agency for reasons referring to unlawful disclosure or access to records. Furthermore, depending on the agency's exact type of violation of individuals' personal data, the latter may request the amendment of the records, or the production of the illegally stored records to them, as well as the actual damages owing to their suffering, and the financial costs of the action together with the attorney fees. The enactment of the Judicial Redress Act has been an important prerequisite for the ratification of the Umbrella Agreement between the US and the EU, especially after the *Schrems* ruling and the revelations of Edward Snowden.

However, the Judicial Redress Act contains several limitations. The Attorney General, along with the Secretary of State, the Secretary of the Treasury and the Secretary of Homeland Security, is entitled to designate the 'covered' countries that will benefit from the JRA, provided that they satisfy certain requirements[321]. The 'covered' countries must have reached an agreement with the United States regarding the adoption of specific privacy policies about the sharing of personal data for the prevention, investigation, detection or prosecution of criminal offences, alternatively the Attorney General may determine that the country has shared information with the U.S. and has strong privacy protections for the abovementioned purposes. Moreover, the country must allow for the transfer of personal data to the U.S. through an agreement with the U.S, and the Attorney General must certify that the adopted privacy policies do not hamper the national security interests of the United States. Moreover, the JRA has been criticized[322] for its limited scope which includes only EU citizens and is connected to the citizenship, while the EU data protection framework recognizes the right to the protection of personal data as a universal human right. The limitation is also obvious in the case of the covered records, which refer only to these records which are transferred by public authorities or private entities of a covered country to a designated Federal agency for the purposes that have been mentioned earlier. Finally, the JRA may extend the same rights of the US persons to the EU citizens

[320] 5 U.S.C. Section 552a.
[321] Judicial Redress Act, Section 2(d).
[322] Franziska Boehm (n 237), at 183.

with regard to the civil remedies, however it is explicitly stated that a covered person may pursue civil remedies under 5 U.S.C. Section 552a.(g)(1)(D) only for cases of 'disclosures intentionally or willfully made in violation of section 552a(b)', excluding, thus, any other types of violation. Finally, the European Data Protection Supervisor states that the JRA applies to records transferred from public or private entities of the covered countries to U.S. authorities, excluding, hence, the transfer of personal data between private entities under the Privacy Shield which would be accessed by the U.S. authorities afterwards[323]. The disadvantages of the JRA have been pointed out by the Article 29 Working Party as well[324], concluding that the JRA does not meet the EU standard of the effective redress mechanism.

Furthermore, 50 U.S.C. Section 1810, under FISA, provides for civil remedies in the case of electronic surveillance and unlawful disclosure or use of personal data, however it is explicitly stated that 'foreign power or an agent of a foreign power' are excluded from the authorized subjects entitled to invoke this right. The Freedom of Information Act (FOIA) enhances the transparency and openness in governmental level allowing the availability of government documents to the citizens. Both U.S. and EU citizens are entitled to file a request regarding their access to records that refers to them. However, the relevant provisions allow for a list of exemptions from the implementation of the FOIA, namely records which are kept secret in the interest of national defense or foreign policy, as well as classified records and records which are involved in law enforcement purposes. Due to the broad range of the exemptions, the Article 29 Working Party has concluded that FOIA does not provide effective remedies in case of a violation of the data protection rules[325].

## 6. Redress Avenue: The Case of the Ombudsperson Mechanism

A significant change introduced by the Privacy Shield Agreement is the creation of the Privacy Shield Ombudsperson mechanism whose main role is to accept requests from the EU authorities concerning issues of U.S. signals intelligence activities. The details of this

[323] European Data Protection Supervisor (n 242), at 11.
[324] Article 29 Working Party (n 236), at 43.
[325] Article 29 Working Party (n 236), at 44.

new mechanism are elaborated in Recitals 116 – 122 of the Commission Implementing Decision and in the Letter from the U.S. Secretary of State John Kerry, included in Annex III attached to the Commission Implementing Decision. Firstly, it is decided that the Privacy Shield Ombudsperson shall be the Senior Coordinator for International Information Technology Diplomacy, who according to PPD – 28[326] is designated by the Secretary of State as a means of contact for the foreign governments regarding the signals intelligence activities by U.S. authorities. It is stated that the Under Secretary of State for Economic Growth, Energy and the Environment has taken up this role, with additional State Department officials as assistants. Until 20 January 2017, C. Novelli had served as the Under Secretary of State for Economic Growth, Energy and the Environment, however the position is currently vacant, pending a nomination by the recently elected U.S. President Donald Trump.

The Decision[327] and Annex III underline that the mechanism of the Privacy Shield Ombudsperson is characterized by complete independence from the Intelligence Community[328] and each and every potential influence that could undermine the objective fulfillment of its role, with the aid of the Secretary of State who will ensure the independent character of the Ombudsperson. The main role of the Ombudsperson mechanism is to respond in an adequate manner to the EU individuals' complaints, which are likely to be delivered by the DPAs, which constitute the EU independent oversight bodies with investigatory powers. Due to the inherent difficulty of this particular task, the Privacy Shield Ombudsperson will have to cooperate with United States Government officials, particularly with the Office of the Director of National Intelligence, the Department of Justice and Inspectors Generals. The procedure which is set by the Privacy Shield Agreement is described as follows: Firstly, the EU citizens are expected to submit their requests to the competent national data protection authorities. These requests will be subsequently passed on a EU centralized body whose mission is the efficient management of the complaints of EU citizens. This EU individual complaint handling body will be responsible for assessing specific details of the requests in order to be examined whether

[326] Presidential Policy Directive (PPD – 28), Section 4.d.
[327] Commission Implementing Decision, Recital 121 at 34.
[328] Annex III attached to the Commission Implementing Decision, Section III.1 at 53.

they can be characterized as complete. It is crucial to emphasise that the requests' main subject must be related the issue of the transfer of individuals' personal data from the EU to the U.S. pursuant to the Privacy Shield Agreement or other potential means of transfer, for example BCRs, however it is stated that a general and abstract claim that the Privacy Shield is inconsistent with the EU data protection standards is not sufficient. The EU individual complaint handing body is competent to certify whether this is the case, as well as examine whether the request contains all the necessary details, such as the information which will constitute the basis of the request, the nature of information of relief sought, the U.S. Government agencies which are involved and the measures that have been used for obtaining these data and the relevant response to them. Should the request be made in bad faith or be frivolous or vexatious, then it is bound to be rejected by the EU handing body. Furthermore, Annex III[329] clarifies that it is not necessary for the request to prove that the personal data at issue have been actually accessed by the U.S. government agencies through their signals intelligence activities. This is quite important for the further processing of the requests by the Privacy Shield Ombudsperson, otherwise a great number of requests which would fail to do so would be rejected by the EU handing body. The Privacy Shield Ombudsperson receives the requests by the EU handing body and reviews if the abovementioned conditions of Section 3(b) are met and, in case of the need for further information on the subject, the Ombudsperson will inform the EU handing body to further investigate the matter. Subsequently, the Privacy Shield Ombudsperson will have to submit an adequate and timely response to the EU individual complaint handling body, elaborating whether it has been proved that there has been a breach of the U.S. law, consisting of statutes, Executive Orders, presidential directives and agency policies, and, if this is the case, whether any remedies have been offered to the victim. From this point onward, the EU individual complaint handling body is responsible for contacting the requester. The deficiency of the Ombudsperson mechanism lies within the fact that Annex III attached to the Commission Implementing Decision, Section 4.e. explicitly states that the Ombudsperson will not be able to inform individuals on whether they have been the target of surveillance, nor on the exact remedial action applied.

[329] Annex III attached to the Commission Implementing Decision, Section 3.c. at 54.

The fact that the role of the Ombudsperson is bestowed on the Under Secretary of State for Economic Growth, Energy and the Environment may trigger uncertainty about the degree of the independence of the new redress mechanism. The Under Secretary of State for Economic Growth, Energy and the Environment constitutes an undersecretary position existing within the Department of State and the person who serves as an Under Secretary of State is appointed by the U.S. President, with the consent of the Senate[330]. The Under Secretary of the State ranks below the Deputy Secretary and the Secretary of State. Taking all these into account, it could be implied that there are no solid guarantees ensuring the total and absolute independence of the Ombudsperson, due to the potential influence of the Deputy Secretary of State and the Secretary of State[331]. The other serious concern relates to the authority and the nature of the investigatory powers of the Ombudsperson. The main criticism is focused on the abstract and vague reference of the Privacy Shield Agreement to the specific range of the powers of the Ombudsperson, since there is no statement as to what extent the Ombudsperson mechanism may acquire access to records and personnel of the intelligence agencies[332] and can rely on its own investigation on the issue at stake . The lack of specificity of the Ombudsperson's investigative powers is underlined by the Working Party of Article 29 as well[333], adding that it remains unclear in which way the Ombudsperson will provide for specific remedies in a case of non – compliance, while there is no mention to the existence of any kind of remedies regarding the Ombudsperson's decision itself[334].

[330] 22 U.S.C. Section 2651a.(b).(1).
[331] Peter Margulies, 'Global Cybersecurity, Surveillance and Privacy: The Obama Administration's Conflicted Legacy', Legal Studies Research Paper Series, Roger Williams University, at 24. The Working Party of Article 29 is also reluctant to certify that the Ombudsperson can be characterized as a formally and fully independent redress mechanism, see Article 29 Working Party (n 13), at 49 and 51, also Christopher Kuner,(n 267), at 22.
[332] Peter Margulies (n 331), at 24.
[333] Article 29 Working Party (n 236), at 50.
[334] Article 29 Working Party (n 236), at 51.

# CONCLUSIONS

There is no doubt about the fact that the CJEU ruling regarding *Schrems* case brought radical changes to the Safe Harbour regime which regulated the data flows from the European Union to the United States. The invalidation of the Safe Harbour pushed the European Commission and the United States to bring within a period of a few months a new pact, the EU – U.S. Privacy Shield Framework in the hope that all legal obstacles, which led to the initial collapse of the Safe Harbour, had been surpassed. Once more, the new Privacy Shield Framework is being challenged[335], since Digital Rights Ireland brought an action in the General Court of the CJEU on 16 September 2016, as well as La Quadrature du Net on 2 November 2016. The CJEU will have to decide on the adequacy of the Privacy Shield, taking into account and assessing the amendments of the U.S. legislation in the light of the EU data protection standards.

The Privacy Shield constitutes a much more robust mechanism in comparison to the Safe Harbour. Indeed, there has been an incontestable progress in crucial pillars, such as the enhancement of the Principles, the extensive role of the Department of Commerce and the Federal Trade Commission and the rebuilding of the recourse system for EU citizens' complaints. Furthermore, the commitments of the U.S. authorities constitute a positive step towards the limitation of the bulk collection of EU data subjects' personal data. Nevertheless, the main conclusion of this dissertation is that the EU – U.S. Privacy Shield is likely, once again, to be found as inadequate, based on the fact that the U.S. level of data protection is not essentially equivalent to the European. The main deficiencies of the Privacy Shield refer to the failure of the Data Integrity and Purpose Limitation Principle to respond to the principles of necessity and proportionality regarding the collection and processing only of the personal data which are necessary, not simply relevant, for the purposes at issue, as well as the absence of a clear statement of the necessity of the erasure of personal data when they are no longer needed for the purposes they have been collected and processed for. Regarding the oversight and enforcement role of the DoC and FTC, the main drawback is that their responsibilities are based, to a great extent, to commitments and assurances given in the letters of the Annexes attached to the Commission

[335] http://datamatters.sidley.com/eu-u-s-privacy-shield-challenged-cjeu/ accessed 2 February 2017.

Implementing Decision, which cannot be considered as adequate insofar as they are not put into practice. As far as the recourse system is concerned, there have been several remarks regarding the complexity of such a multi – layered system, creating even more legal obstacles for the EU citizens to have access to these mechanisms. The main interest lies in the U.S. legislation and its amendments regarding the access and use of EU data subjects' personal data by the U.S. public authorities for national security reasons. Firstly, the Presidential Policy Directive No 28 fails to protect in an effective manner the rights of EU individuals against cases of indiscriminate collection of personal information because of the signals intelligence activities of the U.S. Intelligence agencies. In fact, it has been emphasized that PPD – 28 explicitly provides for the bulk collection of signals intelligence for specific purposes, however the very existence of this phenomenon is against the principles of the EU data protection framework, which do not authorise, under any circumstances, the bulk collection of EU citizens' data. Moreover, the provision which excludes the limitations imposed by the PPD – 28 from the temporary acquisition of signals intelligence constitutes one more shortcoming of the PPD – 28. USA FREEDOM Act introduces various reforms, many of which are encouraging, notably the limitation of the bulk collection with the use of specific selection terms. However, it has already been established that many provisions, with special reference to the adoption of minimization procedures, yield benefits only to U.S. persons, excluding EU citizens from them, even though the EU data protection framework provides for them. Section 702 of FISA has also been faced as an enemy of the rights of EU citizens, since it has been the basis of the surveillance programs which, according to Edward Snowden, permitted the massive collection of EU citizens' personal information. It is also important to note that FISA is due to expire at the end of 2017, therefore it is highly possible that the new U.S. President will introduce several amendments to FISA, which are to change in an unprecedented way its content. As far as oversight, redress mechanisms and remedies are concerned, it is considered difficult for EU citizens to respond to the standing requirement, while the existent remedies, such as those of the JRA or FOIA, cannot be considered as easily accessible for the EU data subjects for the reasons that have been mentioned earlier. As for the oversight mechanisms, such as Inspectors General, and the Privacy Shield Ombudsperson, they both fail to respond to the EU standard of the independence which

must characterize oversight and recourse mechanisms. In due time, the CJEU will decide upon the adequacy of the Privacy Shield Agreement, however the main concern is focused on the changes that will be brought by the new U.S. President, especially after the departure of many U.S. officials who belonged to the Obama Administration. The danger of the destabilization of the EU – U.S. relations regarding data transfers and the weakening of data privacy rights of non – U.S. persons seems imminent and is about to test the power of the EU data protection framework.

# BIBLIOGRAPHY

## Books and Book Chapters


Lee A. Bygrave, *Data Privacy Law: An International Perspective* (1st edn, OUP, 2014)

Alan Dashwood, Derrick Wyatt and others, *European Union Law* (6th edn, Hart Publishing, 2011)

Rob Kitchin, *The Data Revolution: Big Data, Open Data, Data Infrastructures and their Consequences* (1st edn, SAGE Publications, 2014)

Herke Kranenborg, 'Interpretation of Article 8' in Steve Peers, Tamara Hervey and others, *The EU Charter of Fundamental Rights: A Commentary* (1st edn, Hart Publishing, 2014)

Christopher Kuner, *Transborder Data Flows and Data Privacy Law* (1st edn, OUP, 2013)

Orla Lynskey, *The Foundations of EU Data Protection Law* (1st edn, OUP, 2015)

Andrew Murray, *Information Technology Law: The Law and the Society* (3rd edn, OUP, 2016)

Fereniki Panagopoulou – Koutnatzi, 'Facebook as a challenge to privacy' in Maria Bottis, *Privacy and Surveillance, Current aspects and future perspectives* (1st edn, Nomiki Vivliothiki, 2013)

Athanassios Tsevas, *Προσωπικά Δεδομένα και Μέσα Ενημέρωσης (Personal data and media)* (1st edn, Nomiki Vivliothiki, 2010)

Georgios Yannopoulos, *Η Ευθύνη των Παρόχων Υπηρεσιών στο Internet (The Liability of the Internet Service Providers)* (1st edn,Nomiki Vivliothiki, 2013)


## Legal Articles and Reports


Loïc Azoulai and Marijn van der Sluis, 'Institutionalizing personal data protection in times of global institutional distrust: *Schrems*', (2016) 53 Common Market Law Review

Franziska Boehm, 'Assessing the New Instruments in EU – US Data Protection Law for Law Enforcement and Surveillance Purposes' (2016) 2 European Data Protection Law Review

danah boyd and Nicole Ellison,' Social Network Sites: Definition, History and Scholarship' (2007), 13 Journal of Computer – Mediated Communication

European Network and Information Security Agency, 'Position Paper No1 Security Issues and Recommendations for Online Social Networks', October 2007

European Union Agency for Fundamental Rights, 'Handbook on European data protection law', April 2014, http://www.echr.coe.int/documents/handbook_data_protection_eng.pdf

David Haynes, 'Social media, risk and information governance' (2016), 33 Business Information Review at 90-93.

Hogan Lovells, 'Legal Analysis of the E.U. – US. Privacy Shield, An adequacy assessment by reference to the jurisprudence of the Court of Justice of the European Union.' 4 April 2016, http://www.hoganlovells.com/files/Uploads/Documents/Privacy%20Shield%20Legal%20Analysis%20by%20Hogan%20Lovells%20(2016-03-31).pdf

Christopher Kuner, Paper No 14 'Reality and Illusion in EU Data Transfer Regulation Post Schrems', March 2016, Legal Studies Research Paper Series, University of Cambridge

Peter Margulies, 'Global Cybersecurity, Surveillance and Privacy: The Obama Administration's Conflicted Legacy', Legal Studies Research Paper Series, Roger Williams University

Yann Padova, 'The Safe Harbour is invalid: what tools remain for data transfers and what comes next?' (2016), 6 International Data Privacy Law

Privacy and Civil Liberties Oversight Board (PCLOB) 'Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act', 2 July 2014, https://www.pclob.gov/library/702-Report.pdf

Daniel Severson, 'American Surveillance of Non – U.S. Persons: Why New Privacy Protections Offer Only Cosmetic Change', Summer 2015, 56 Harvard International Law Journal

**Official Papers of Data Protection Authorities**

Article 29 Data Protection Working Party, 'Opinion 01/2016 on the E.U. – U.S. Privacy Shield draft adequacy decision' (WP 238, 13 April 2016)

Article 29 Working Party, 'Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC', (WP 217, 9 April 2014)

Article 29 Working Party, 'Opinion 03/2013 on purpose limitation' (WP 203, 2 April 2013)

Article 29 Working Party, 'Opinion 15/2011 on the definition of consent' (WP187, 13 July 2011)

Article 29 Data Protection Working Party, 'Opinion 05/2009 on online social networking' (WP 163, 12 June 2009

Article 29 Working Party, 'Opinion 4/2007 on the concept of personal data' (WP 136, 20 June 2007)

Article 29 Working Party, 'Working Document on a common interpretation of Article 26 (1) of Directive 95/46/EC of 24 October 1995' (WP 114, 25 November 2005)

Article 29 Working Party, Opinion 8/2001 on the processing of personal data in the employment context' (WP 48, 13 September 2001)

Article 29 Working Party, 'Working Document: Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive' (WP 12, 24 July 1998)

European Data Protection Supervisor (EDPS), 'Opinion 4/2016: Opinion on the EU – U.S. Privacy Shield draft adequacy decision', 30 May 2016

European Data Protection Supervisor (EDPS), Position Paper on the 'Transfer of personal data to third countries and international organisations by EU institutions and bodies', 14 July 2014

## Press Articles

Wall Street Journal, 'Facebook Profit Soars, but Growth Concerns Emerge', 2 November 2016, http://www.wsj.com/articles/facebook-profit-jumps-sharply-1478117646 accessed 26 November 2016.

Barton Gellman and Laura Poitras, U.S., 'British intelligence mining data from nine U.S. Internet companies in broad secret program', 7 June 2013, https://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html?utm_term=.907cc3e8f9ee accessed 02 February 2017.

Craig Timberg and Barton Gellman, 'NSA paying U.S. companies for access to communications network', *Wall Street Journal* (London, 29 August 2013): https://www.washingtonpost.com/world/national-security/nsa-paying-us-companies-for-access-to-communications-networks/2013/08/29/5641a4b6-10c2-11e3-bdf6-e4fc677d94a1_story.html?utm_term=.6f5db82dd962 accessed 2 February 2017.

## LIST OF LEGAL INSTRUMENTS

Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU – U.S. Privacy Shield, OJ 2016 L 207/1

Council of Europe, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data ETS No 108, 28.I.1981: http://www.conventions.coe.int/Treaty/EN/Treaties/Html/108.htm accessed on 13 November 2016

Directive 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

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.

Commission Decision 2010/87/EU of 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

Consolidated Version of the Treaty on European Union [2010] OJ C83/13

Consolidated Version of the Treaty on the Functioning of the European Union [2010] OJ C83/47

Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between

national authorities responsible for the enforcement of consumer protection laws [2009] OJ L337/11

Treaty of Lisbon Amending the Treaty on European Union and the Treaty establishing the European Community [2007] OJ C306/01

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 networks and amending Directive 2002/58/EC [2006] OJ L 105/54

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 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

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

Commission Decision 2000/520/EC of 26 July 2000 pursuant to Directive 95/46/EC on the adequacy of the protection provided by the safe harbor privacy principles and related frequently asked questions issued by the US Department of Commerce, OJ 2000 L 215/7

Charter of Fundamental Rights of the European Union [2000] OJ C364/01 and [2010] OJ C83/389

Cologne European Council, 'Conclusions of the Presidency', 3 – 4 June 1999

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

Declaration on the protection of personal data in the field of judicial cooperation in criminal matters and police cooperation annexed to the final act of the intergovernmental conference that adopted the Treaty of Lisbon [2008] OJ C115/3450

## LIST OF CASES

### Court of Justice of European Union


Joined Cases C-203/15 and C-698/15 *Tele2 Sverige AB v Post – och telestyrelsen* and *Secretary of State for Home Department v Tom Watson and Others* (Grand Chamber, 21 December 2016).

Case C-362/14 *Maximillian Schrems v Data Protection Commissioner* (Grand Chamber, 6 October 2015)

Case C-288/12, *European Commission v Hungary* [2014] OJ C175/6

Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others* and *Kärntner Landesregierung and Others* [2014] OJ C175/6

Case C-131/12, *Google Spain SL and Google Inc. v AEPD and Mario Costeja González* [2014] OJ C212/4

Joined Cases C-468/10 and C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) and Federación de Comercio Electrónico y Marketing Directo (FECEMD) v Administración del Estado* [2011] ECR I – 12181

Case C-518/07 *Commission v Germany* [2010] ECR I – 1885

Joined Cases C-92/09 and C-93/09 *Volker und Markus Schecke and Hartmut Eifert* [2010] ECR I – 11063

C-553/07, *College van burgemeester en wethouders van Rotterdam v M.E.E. Rijkeboer* [2009] ECR I – 03889

Case C-524/06, *Heinz Huber v Bundesrepublik Deutschland* [2008] ECR I-09705

Case C-73/07 *Tietosuojavaltuutettu v. Satakunnan Markkinapörssi OY, Satamedia* [2008] ECR I – 09831

Joined Cases C-465/00, C-138/01 and C-139/01, *Österreichischer Rundfunk and Others* [2003] ECR I-4989

Case C-101/01 *Bodil Lindqvist* [2003] ECR I – 12971

Case 7/73, *Nold v Commission* [1974] ECR 491

Case 11/70, *Internationale Handelsgesellshaft mbH v Einfuhr- und Vorratsstelle für Getreide und Futtermittel* [1970] ECR 1125

Case 29/69, *Stauder v City of Ulm* [1969] ECR 419

**European Court of Human Rights**

Roman Zakharov v Russia [2015] ECHR 1065

S. and Marper v United Kingdom (2009) 48 EHRR 50, paras 67, 121.

Coster v the United Kingdom (2001) 33 EHRR 20

Rotaru v Romania (App No 28341/95) (unreported) 4 May 2000

Kopp v Switzerland (1999) 27 EHRR 91, para 55,

Murray v United Kingdom (1996) 23 EHRR 313

Leander v Sweden (1987) 9 EHRR 433

X and Y v The Netherlands (1985) 8 EHRR 235

Malone v United Kingdom (1985) 7 EHRR 14.

Klass v Germany (1979) 2 EHRR 214.