İSTANBUL BİLGİ ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
BİLİŞİM VE TEKNOLOJİ HUKUKU YÜKSEK LİSANS PROGRAMI

AN EXAMINATION OF ADEQUACY OF THE EU-U.S. PRIVACY SHIELD UNDER THE EU LAW

Onur Cem ALTUN
113691001

TEZ DANIŞMANI:
Yrd. Doç. Dr. Mehmet Bedii KAYA

İSTANBUL
2017

An Examination of Adequacy of the EU-U.S. Privacy Shield under the EU Law

AB-ABD Privacy Shield Anlaşmasının AB Hukuku Kapsamında Yeterliliği Üzerine Bir İnceleme

Onur Cem ALTUN

113691001

Tez Danışmanı : **Yrd. Doç. Dr. Mehmet Bedii KAYA** (İmza) .....

Yıldırım Beyazıt Üniversitesi

Jüri Üyeleri : **Prof. Dr. Ahmet DENKER** (İmza) .....

İstanbul Bilgi Üniversitesi

Doç. Dr. Leyla KESER BERBER (İmza) .....

İstanbul Bilgi Üniversitesi

Tezin Onaylandığı Tarih : 26 Ocak 2018

Toplam Sayfa Sayısı : 158

Anahtar Kelimeler (Türkçe)

1) Güvenlik Kalkanı
2) Güvenli Liman
3) Veri Koruma Hukuku
4) Avrupa Birliği
5) Amerika Birleşik Devletleri

Anahtar Kelimeler (İngilizce)

1) Privacy Shield
2) Safe Harbour
3) Data Protection Law
4) European Union
5) The United States of America

Table of Contents

List of Abbreviations

ADR	: Alternative Dispute Resolution
BCR	: Binding Corporate Rules
CAN-SPAM Act	: The Controlling the Assault of Non-Solicited Pornography and Marketing Act
CFAA	: Computer Fraud and Abuse Ac
CFREU	: Charter of Fundamental Rights of the European Union
CJEU	: Court of Justice of the European Union
CoE	: Council of Europe
Convention 108	: Council of Europe Data Protection Convention
COPRA	: Children's Online Privacy Protection Act
Data	: Personal Data
DoC	: Department of Commerce
DPA	: Data Protection Authority
DPD	: Data Protection Directive
DRD	: Data Retention Directive
DECS	: Directive for the Electronic Communications Sector
ECHR	: European Convention on Human Rights
ECtHR	: European Court of Human Rights
ECPA	: The Electronic Communications Privacy Act
EDPS	: European Data Protection Supervisor
EU	: European Union
EU Members	: Member States of the European Union
FAQ	: Frequently Asked Questions
FBI	: Federal Bureau of Investigation
FCRA	: The Fair Credit Reporting Act
FISA	: Foreign Intelligence Surveillance Act
FISC	: Foreign Intelligence Surveillance Court
FOIA	: Freedom of Information Act
FSM	: Financial Services Modernization Act
FTC	: Federal Trade Commission
FTC Act	: Federal Trade Commission Act
GDPR	: General Data Protection Regulation
HIPAA	: The Health Insurance Portability and Accountability Act
IRM	: Independent Dispute Resolution Body
JRA	: Judicial Redress Act

NSA	: National Security Authority
ODNI	: Office of the Director of National Intelligence
PIPPD	: Regulation (EC) No. 45/2001 on the protection of individuals with regard to the processing of personal data by the institutions and bodies of the Community and on the free movement of such data
Privacy Shield	: EU:U.S. Privacy Shield
Roskomnadzor	: Russian Federal Service for Supervision of Communications, Information Technology and Mass Media
PPD:28	: Presidential Policy Directive 28
Safe Harbour	: Safe Harbour Privacy Principles and Frequently Asked Questions issued by the Department of Commerce
Safe Harbour Decision	: Commission Decision 520/2000/EC
Schrems Decision	: C: 362/14, Maximillian Schrems v. Data Protection Commissioner
TCPA	: Telephone Consumer Protection Act
TEU	: Treaty on the European Union
TFEU	: Treaty on the Functioning of the European Union US - United States
WP29	: Working Party on the Protection of Individuals with regard to the Processing of Personal Data

List of Tables

Özet

Bu tez, Avrupa Birliği ile Amerika Birleşik Devletleri arasındaki müzakerelerin bir sonucu olan Privacy Shield (Güvenlik Kalkanı) çerçeve anlaşmasını, Avrupa Birliği Veri Koruma Direktifi, AB Veri Koruması Genel Regülasyonu ve Avrupa Birliği'nin ilgili içtihadı çerçevesinde incelemektedir. Privacy Shield, Avrupa Birliği Komisyonu ile müzakere edildikten sonra Amerika Birleşik Devletleri Ticaret Bakanlığı tarafından, Avrupa Birliği'nden Amerika Birleşik Devletleri yönüne yapılan veri transferini düzenlemek amacıyla yayınlanmış bir hukuki çerçeve anlaşmadır.

Bu tez Amerika Birleşik Devletleri'nin sağladığı veri koruma seviyesinin Avrupa Birliği'nin sağladığı veri koruma seviyesine eş değer olup olmadığı sorusuna cevap aramaktadır. Bununla birlikte, Safe Harbour'dan (Güvenli Liman), Privacy Shield'a geçiş sebeplerini araştırmak, eğer varsa, Privacy Shield'ın Avrupa Birliği hukuku kapsamında yeterli bir veri koruma seviyesi sağlama amacını gerçekleştirirken eksik kaldığı noktaları tespit etmek ve bunun sonucunda bu eksiklikleri ortadan kaldıracak değişiklikleri ortaya koymak bu çalışmanın amaçlarıdır.

Bu tez Amerika Birleşik Devletleri'nin Avrupa Birliği'nin sağladığı veri koruma seviyesine eş değer seviyede bir veri koruması sağlamadığını savunmaktadır. Bu bağlamda, bu tez Amerika Birleşik Devletleri'nin veri koruma seviyesini Avrupa Birliği'nin veri koruma seviyesine yaklaştıracak değişiklikler önermektedir. Bu amacı gerçekleştirmek için sunulan öneriler, ana hatlarıyla: daha güçlü kriptolama tekniklerinin kullanılması; Amerika Birleşik Devletleri'nde bağımsız bir veri koruma otoritesinin kurulması; Privacy Shield ile öngörülen uyuşmazlık çözüm yollarının sadeleştirilmesi ve geliştirilmesi olacaktır.

Abstract

This thesis examines the EU-U.S. Privacy Shield taking into consideration the EU Data Protection Directive, General Data Protection Regulation and relevant case law of the EU. The EU-U.S. Privacy Shield is a framework drafted by the U.S. Department of Commerce with the contributions of the European Commission, to regulate the data transfer from the European Union to the United States.

The thesis aims to answer the question whether the U.S. provides a level of data protection, which is equivalent to that of the EU. Furthermore, it aims to investigate the reasons for the transition from the EU-U.S. Safe Harbour to the EU-U.S. Privacy Shield, identify the shortcomings of the Privacy Shield, if any, that might undermine the level of adequacy of the framework with reference to the EU law, and subsequently suggest amendments that can eliminate those shortcomings. The thesis utilizes black letter and doctrinal legal analysis methods to achieve its objectives.

This thesis argues that the U.S. does not provide a level of data protection that is equivalent to that of the EU. In that regard, the thesis provides suggestions which might bring the data protection level of the U.S. closer to that of the EU. Accordingly, it is argued that certain amendments to the Privacy Shield Principles can be made, strong encryption techniques can be adopted, an independent data protection authority in the U.S. can be established, redress options under the framework can be simplified and improved to achieve for that purpose.

INTRODUCTION

BACKGROUND

Right to Data Protection

Personal Data can be defined as "any information relating to an identified or identifiable natural person[1]." In that regard, any information that might be utilized to identify a person whether it is directly or indirectly can be regarded as personal data[2]. To exemplify, identification number of the person, or "factors specific to his physical, physiological, mental, economic, cultural or social identity" might be used as references to identify a person[3].

Under the European Union Law, the right to data protection[4] is considered as a fundamental human right that is even close to negotiations[5]. Charter of Fundamental Rights of the European Union (hereafter the CFREU), under the article 8, lays down the general rules and limitations for processing of the personal data, as well as the right of access to and rectify the personal data by the data subjects[6]. Similarly, Article 16 of The Treaty on the Functioning of the European Union (hereafter the TFEU) recognizes the right to data protection, and brings about certain obligations for the Union institutions and Members in this context[7].

---

[1] Directive 95/46/EC, of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, art. 2(a), 1995 O.J. (L 281) 31–32 [hereinafter DPD].

[2] Ibid.

[3] Ibid.

[4] Also known as Right to Protection of Personal Data.

[5] Ionna Tourkochuriti, *The Snowden Revelations, the Transatlantic Trade and Investment Partnership and the Divide between U.S.-EU in Data Privacy Protection*, 36 UALR L. REV. 161 (2014), at 163.

See also, Joel R. Reidenberg, *Resolving Conflicting International Data Privacy Rules in Cyberspace Resolving Conflicting International Data Privacy Rules in Cyberspace*, 1315 STAN. L. REV (1999), at 1347.

For a related discussion see also, Paul M. Schwartz, *The EU-U.S. Privacy Collision: A Turn to Institutions and Procedures*, 126 HARV. LAW REV. 1966 (2013), at 1989.

[6] Charter of Fundamental Rights of the European Union, Dec. 7, 2000, O.J. (C 364) 1 [hereinafter CFEU].

[7] Consolidated version of the Treaty on the Functioning of the European Union art. 63 OJ c 326/71, art. 107 OJ c 326/91, art. 108 OJ c 326/92, Dec. 13, 2007, O.J. (C 71) [hereinafter TFEU].

In addition to those, the right to data protection is governed by the EU Directives[8]. The Directive 95/46/EC on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (hereafter the DPD or EU Data Protection Directive) comprises comprehensive provisions regarding the protection of the personal data[9].

Under the U.S. Law, the right to data protection takes its roots from the fourth Amendment to the Constitution: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, should not be violated[10]..." The fourth amendment prohibits arbitrary interference of the government to the reasonable expectation of the privacy of a person, and brings about the obligation to obtain warrant for the searches. The Supreme Court also evaluates search and seizure of electronic devices, electronic surveillance and wiretapping in this context[11]. However, the fourth amendment does not provide a comprehensive protection for personal data[12].

The term personal data is referred as "personal information" in the U.S. Law, and there is no uniform definition for the personal data[13]. One of the most substantial regulations regarding the data protection in the U.S. Law is the Privacy Act of 1974[14]. The Act prohibits disclosure of the personal data maintained by the government agencies, grants data subjects' access to and rectification of the personal data, also brings about certain rules for the "collection, maintenance, and dissemination of records[15]." However, the Act only applies to the citizens of the

---

[8] Schwartz, *supra* note 5, at 1972.
[9] DPD, *supra* note 1.
[10] U.S. CONST. amend. IV.
[11] Ryan Strasser, FOURTH AMENDMENT: AN OVERVIEW, https://www.law.cornell.edu/wex/fourth_amendment (last visited Dec 14, 2017).
See also, Francesca Bignami, THE US LEGAL SYSTEM ON DATA PROTECTION IN THE FIELD OF LAW ENFORCEMENT. SAFEGUARDS, RIGHTS AND REMEDIES FOR EU CITIZENS EUROPEAN PARLIAMENT 2015–54 (2015), at 8.
[12] Bignami, *supra* note 11, at 8.
[13] However, the term "personal data" will be used throughout this study to eliminate inconsistency.
For a discussion on definition of the personal data under the U.S. law, see Paul M. Schwartz, Daniel J. Solove, *Defining "Personal Data" in the European Union and United States*, 13 PVLR 1581 (Sept. 15, 2014), reprinted at 14 World Data Protection Report 4 (Sept. 2014), at 1.
[14] Bignami, *supra* note 11, at 10.
[15] Id. at 11.

U.S. and permanent residents[16]. The Judicial Redress Act of 2015 gives similar rights to the EU citizens[17]. Furthermore, there are limiting provisions for the public authorities with regards to the access to the personal data in the Foreign Intelligence Surveillance Act (FISA), the Electronic Communications Privacy Act (ECPA) and the USA PATRIOT Act (PATRIOT Act[18]).

Furthermore, the U.S. Law allows retention and processing of data as long as the processing and retention does not cause any harm or the law does not prohibit that[19]. Whereas, the EU Law has a contrasting approach: according to the European Court of Human Rights (hereafter ECtHR), irrespective of the damage, retention of the data can violate the right to data protection[20].

The approach to data protection in the U.S. relies on self-regulation practices rather than regulations issued by the government[21]. That approach is based on the idea that the data privacy is an issue pertaining to the consumer law[22]. On the other hand, the EU approach is based on the idea that data protection is an issue related to the public law[23].

A brief comparison of the two legislations shows that the E.U. Law regards right to data protection as a human right, whereas the U.S. Law regards that right as a consumer right, which exclusively belongs to the U.S. citizens. This fundamental difference in the U.S. and EU legal cultures will be taken into account throughout this study.

See also, OVERVIEW OF THE PRIVACY ACT OF 1974, http://www.justice.gov/opcl/privacyactoverview2012/1974compmatch.htm (last visited Dec 14, 2017).

[16] See, 5 U.S.C. § 552a.
See also, Bignami, *supra* note 11, at 12.

[17] Franziska Boehm, *A Comparison between US and EU Data Protection Legislation for Law Enforcement*, 81 STUDY LIBE COMM. (2015), at 54.

[18] Id. at 56.

[19] Tourkochuriti, *supra* note 5, at 164.
See also, DPD, *supra* note 1, art. 7.

[20] Amann v. Switzerland, App No 27798/95**,** at para. 69 (ECtHR, Feb. 16, 2000).

[21] Reidenberg, *supra* note 5, at 1335.

[22] Ibid.

[23] Id. at 1347.

The EU-U.S. Privacy Shield and the Right to Data Protection

In simplest terms, the EU-U.S. Privacy Shield (hereafter the Privacy Shield) is a framework drafted by the U.S. Department of Commerce with the contributions of the European Commission, to regulate the data transfer from European Union to the United States[24]. As the European Commission, evaluating this framework, found that, in the scope of the Privacy Shield, the data protection level of the United States adequate on July 12, 2016, the Privacy Shield became a valid legal mechanism that requires the certified companies to comply with a certain set of principles[25].

Briefly, the Privacy Shield is designed to ensure that:

i. Certified companies inform the data subjects concerning the right to access to the personal data, the scope of the processing, the contact information of the processor as well as the available recourse mechanisms[26];
ii. The processing of the personal data can only be performed for the original purposes of collection of the data (purpose limitation);
iii. The data to be processed should be minimized in relation to the purposes of limitation (data minimization)[27];
iv. The certified companies secure the data, including the cases where the data is transferred to another company;
v. The data subjects may access to, and rectify their data[28];
vi. The data subjects may obtain a remedy[29];
vii. The data subjects have the right to redress in case that U.S. public authorities access the data exceeding the extent necessary for national security or law enforcement purposes[30].

---

[24] PRIVACY SHIELD PROGRAM OVERVIEW (2017), https://www.privacyshield.gov/Program-Overview (last visited Dec 14, 2017).
[25] Ibid.
[26] EUROPEAN COMMISSION, GUIDE TO EU-U.S. PRIVACY SHIELD (2016), http://ec.europa.eu/justice/data-protection/files/eu-us_privacy_shield_guide_en.pdf (last visited Dec 14, 2017), at 9.
[27] Id. at 10.
[28] Id. at 11.
[29] Id. at 12.
[30] Id. at 13.

Transactions in today's world, in many instances, require the use of personal data such as a name, address, login name, employee number, gender, age, marital status, credit card information, identity number and, these are examples to the personal data. According to the estimations, cross-border data flow accounts for the 10.1 percent increase in the global GDP from 2005 to 2014. What's more, a better data flow could allow a further 13 percent increase in the global GDP[31]. Moreover, digitally delivered services constitutes 72%[32] of the total export from U.S. to EU and trade between the U.S. and EU stands for 31%[33] of the global economy. Those numbers alone make it possible to assert that well being of the data flow between the U.S. and EU hugely affects the global GDP[34].

As the main role of the Privacy Shield is to provide free flow of data from EU to U.S. organizations[35], it is a significant figure in the global economy considering the given statistics. Analysis of effectiveness of this figure therefore, is one of the goals of this study.

THE RESEARCH QUESTION AND THE CONTRIBUTION TO THE LITERATURE

The primary research question posed in this study is whether the Privacy Shield arrangement is effective at ensuring the protection of the transferred data from EU to the U.S. To answer this question, the Privacy Shield along with the safeguards and limitations provided by the U.S. law will be scrutinized with reference to the EU data protection law. If the Privacy Shield fails to be an effective arrangement in that regard, the points of failure will be identified, and

---

[31] *Digital Globalization : The New Era Of Global Flows*, (2016), https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/digital-globalization-the-new-era-of-global-flows (last visited Dec 14, 2017).

[32] RACHEL F FEFER, SHAYERAH I AKHTAR & WAYNE M MORRISON, DIGITAL TRADE AND U.S. TRADE POLICY, 20 (2017).

[33] *United States Of America*, 106 (2000), https://ec.europa.eu/energy/en/topics/international-cooperation/united-states-america (last visited Dec 14, 2017).

[34] See also, Tourkochuriti, *supra* note 5, at 161.

[35] Guide to EU-U.S. Privacy Shield, *supra* note 26, at 7.

suggestions to eliminate those shortcomings will be provided to conclude this study.

In order to contextualize the analysis, the current legal framework of data protection of the EU as well as the planned changes in that framework will be examined. As the EU Commission adequacy decisions, such as the one that made the Privacy Shield a valid legal mechanism, are based on the Article 25 of the DPD[36], and that article states that "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" have particular importance in those decisions[37], the relevant U.S. legal framework is also going to be examined to a certain extent.

As the Privacy Shield is a relatively new arrangement, there are a limited number of studies in the academic literature. Most of the studies focus on certain aspects of the Privacy Shield; therefore a comprehensive analysis of the whole framework along with the suggestions of update, which might better the framework, will be contribution of this study to the academic literature. Moreover, this master's thesis is the first to examine the Privacy Shield in Turkey.

As stated earlier, one of the goals of the Privacy Shield is to ensure that personal data are processed on the basis of the original purposes for which the data are collected. According to Brautigam[38], Mestre[39], Vermeulen[40] and Schrems[41], the Privacy Shield fails to ensure that. The reason of that is the

---

[36] Nora Di Loidean, *The end of Safe Harbor: implications for EU digital privacy and data protection law*, 19 J. INTERNET LAW 7–14 (2016), at 8.

[37] See, Christopher Kuner, *The European Union and the Search for an International Data Protection Framework*, 2 COPYR. GRONINGEN J. INT. LAW 222–228 (2014), at 69.

[38] Tobias Bräutigam, *The Land of Confusion: International Data Transfers between Schrems and the GDPR*, (2016).

[39] Francois Mestre, THE UGLY TRUTH BEHIND THE PRIVACY SHIELD, https://ciolawsdotcom.wordpress.com/2016/08/21/the-ugly-truth-behind-the-privacy-shield/ (last visited Dec 14, 2017).

[40] Gert Vermeulen, *The paper shield: on the degree of protection of the EU-US privacy shield against unnecessary or disproportionate data collection by the US intelligence and law enforcement services, Svantesson*, 4 TRANSATLANTIC DATA PRIVACY RELATIONSHIPS AS A CHALLENGE FOR DEMOCRACY 1–16.

[41] Max Schrems, *The Privacy Shield is a Soft Update of the Safe Harbor*, 2 EUROPEAN DATA PROTECTION LAW REVIEW 148–150 (2016).

wording of the *Notice* and *Choice Principles*[42]. That issue will be investigated in this study in great detail and if necessary, an update to that principle will be suggested.

Another goal of the Privacy Shield is to ensure that data subjects have the right to redress in case that the U.S. authorities exceed the lawful grounds of access to data, and the extent necessary for national security or law enforcement purposes. However, overwhelming number of the writers that examined the Privacy Shield claim that the current U.S. legal framework of data protection allows collection of all the data of all the people (mass surveillance), and that contradicts with the European standards of data protection[43]. Some of the writers assert that this should not necessarily is an evidence that the data protection in the U.S. meets the EU requirements, since mass surveillance is practiced by many countries including the EU members[44]. Some of the writers claim that it is an issue, which cannot be solved by the written law[45]. It is suggested that increased transparency and accountability can overcome this issue[46]. Some argue that strong encryption will restrict the extent of the surveillance practices[47].

As the discussion is concentrated on the U.S. side's interference to the personal data, the extent of that interference, the U.S. legal basis of that interference and the relevant EU law and practices should be scrutinized to be able to conclude whether the surveillance practices of the U.S. side differentiate from that of the EU. The suggestions proposed by the aforementioned writers will also be evaluated, and a novel solution to that issue will be looked for.

---

[42] Commission Implementing Decision of 12.7.2016 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, 2016 O.J. (C 4176) 4. [hereinafter Privacy Shield].

[43] See, O'brien & Reitman, *infra* note 801, Guild, Didier & Carrera, *infra* note 886, Bräutigam, *supra* note 38, Mestre, *infra* note 583, Vermeulen, *supra* note 40, Deckelboim, *infra* note 57, Schrems, *supra* note 41, Loidean, *supra* note 36, Boehm, *supra* note 17.

[44] See, Tracol, *infra* note 854, Bräutigam, supra note 38, Lam, *infra* note 952.

[45] See, Kuner, *infra* note 252, Haufbaer & Jung, *infra* note 152, Burri & Schär, *infra* note 250.

[46] See, EU Organizations, and US Organizations. "EU-US NGO Letter Safe Harbor." Received by Secretary Pritzker and Commissioner Jourová, *The Public Voice*, 13 Nov. 2015, thepublicvoice.org/EU-US-NGO-letter-Safe-Harbor-11-15.pdf.

[47] See, Haufbaer & Jung, *infra* note 152, Hare, *infra* note 251, Deckelboim, *infra* note 57, Gross, *infra* note 967.

Since the Privacy Shield provides legal redress options as mentioned, the means of redress possibilities as well as the complexity of those possibilities are also subject to discussion in the academic literature. Some argue that the legal redress mechanism provided by the Privacy Shield is overly complex[48], and some argue that there are substantial improvements in that matter[49]. The Ombudsperson mechanism, a new redress option, which is introduced by the Privacy Shield[50], is also discussed by the writers. It is widely claimed that the Ombudsperson mechanism lacks the independence and authority to be able to work as worded in the Privacy Shield[51]. Since there are conflicting arguments, the structure, complexity and means of redress possibilities provided by both the Privacy Shield and the U.S. Law will be examined with reference to the EU Law. If that analysis indicates any shortcomings, options of improvement will be looked for.

Some of the writers argue that the mechanisms of oversight provided by the Privacy Shield are inadequate[52]. To overcome this issue, it is argued that an independent Data Protection Authority should be established in the U.S.[53]. As lack of oversight might undermine the effectiveness of the framework[54], special attention will be given to this issue. The oversight mechanisms and practices will be scrutinized with reference to the EU Law.

METHODOLOGY

The methodology of this thesis will be black letter and doctrinal legal analysis.

The objective of this thesis is to investigate the reasons of the transition from the Safe Harbour to the Privacy Shield, identify the shortcomings of the Privacy

[48] See, Salolatva, *infra* note 339.
[49] See, Bräutigam, *supra* note 38, Voss, *infra* note 934.
[50] Privacy Shield, *supra* note 42, ANNEX III, Annex A.
[51] See, Bräutigam, *supra* note 38, Mestre, *infra* note 583, Vermeulen *supra* note 40, Margulies, *infra* note 857.
[52] Estelle Masse & Amie Stepanovich, THREE FACTS ABOUT US SURVEILLANCE THE EUROPEAN COMMISSION GETS WRONG IN PRIVACY SHIELD (2016), https://www.accessnow.org/three-facts-us-surveillance-european-commission-gets-wrong-privacy-shield/ (last visited Oct 27, 2017).
[53] Schrems, *supra* note 41.
[54] ARTICLE 29 DATA PROTECTION WORKING PARTY, EU – U.S. PRIVACY SHIELD – FIRST ANNUAL JOINT REVIEW, WP 255, 9-10 (2017), [hereinafter WP29].

Shield that might undermine the level of adequacy of the arrangement with reference to the EU law, subsequently suggest amendments that can eliminate those shortcomings. In that regard, the black letter approach will be utilized to provide a through analysis of the Privacy Shield arrangement with reference to the EU's data protection law and practices. To be able to contextualize EU's data protection law and practices, along with the other sources, the CFREU, the TFEU, the relevant EU Directives, and case law of the Court of Justice of the European Union (hereafter the CJEU) will be examined.

In a similar manner, the U.S. law and practices that set the legal context of the Privacy Shield, the U.S. Constitution, state constitutions, federal and state statutes, common law, case law, and administrative law will be examined to the extent necessary.

This thesis also utilizes the doctrinal legal analysis method. In that regard, this thesis will compare and analyze the relevant academic works to obtain a better understanding of the current discussions, and identify the problems as well as arguments posed by the scholars. That analysis will provide a road map for further examination of the other sources of law in an attempt to suggest amendments, which will potentially improve the Privacy Shield.

Nevertheless, comparison of legal systems, beyond the legal texts, requires a broad analysis of "constitutional protection, treaty protection, human rights institutions, civil law protection, criminal law, administrative law, and self-regulation[55]." Since this type of analysis in a broad scale cannot be conducted in this thesis, the emphasis will be given to the provisions of the Privacy Shield, which conflict the EU Law. Besides, this thesis will not analyze the economical or financial aspects of the Privacy Shield. Likewise, this thesis will not apply methods of empirical analysis to reach its objectives.

[55] See, Graham Greenleaf, *2014-2017 Update to Graham Greenleaf's Asian Data Privacy Laws - Trade and Human Rights Perspectives*, UNSW LAW RESEARCH SERIES(2017), at 53.

OUTLINE OF THE THESIS

The comparison of the Approaches of the U.S. and EU is critical to the overall evaluation of the thesis. That's why the Section 2 will make that comparison, taking into account the different legal approaches of two sides. To give more depth to that comparison, as it is the primary legal instrument of data protection in the U.S, an overview of the Data Protection Directive is given under the Section 3. As the GDPR will replace the DPD soon, the changes that the GDPR brings to the table are examined under the Section 5.

The Safe Harbour is reviewed in the Section 4 of this study in an attempt to identify the shortcomings of the Safe Harbour as set forth by the CJEU. The results of the Section 4, the shortcomings of the Safe Harbour, are used in the other sections as a point of reference.

In the Section 6 of the thesis, an overview of the Privacy Shield framework and the Commission Decision that made it a valid framework is given. The Commission adequacy decision along with the CJEU's Schrems Decision are critical parts of this study, as they are referred in the following sections where the Privacy Shield is analyzed.

In the Section 7 the focus is put on the commercial aspects, and in the Section 8 on the aspects regarding the access by the U.S. public authorities respectively. A doctrinal legal analysis is made on those aspects of the Privacy Shield with reference to the Safe Harbour, DPD, and the GPDR. At the end of the Section 7 and Section 8, the possible options of improvement are provided.

In the Section 9, alternative options that are not discussed in the Section 7 and Section 8 are evaluated.

The Section 10 brings together all of the results achieved in this study. Subsequent to the results, an evaluation is given on how this study could be improved.

SECTION 1

THE RIGHT TO DATA PROTECTION IN THE EU AND U.S. LAW

1.1. THE HISTORICAL BACKGROUND OF THE RIGHT TO DATA PROTECTION

Following the World War II, a good number of the European countries including Germany, France, and the United Kingdom, made rigorous privacy laws[56]. Perhaps, the most significant result of the legislative efforts of those countries was the European Convention on Human Rights (hereafter ECHR) issued by the Council of Europe (hereafter CoE) in 1950[57]. The Convention aimed to protect the rights and freedoms of all the humans without any kind of discrimination[58]. The Article 8 of the Convention is of great importance in terms of privacy in general and data protection as the article dictates that everyone has right to privacy, and regards that right as a human right[59]. The subject of this privacy is declared as private life, family life, home and correspondence of the person[60]. In the Article 8(2), the limitations to this right is provided, the public authorities may interfere when it is "in accordance with the law and is necessary in a democratic society" for the following purposes[61]:

i. "National security,
ii. Public safety,
iii. Economic well being of the country,

---

[56] Gehrd Steinke, *Data privacy approaches from US and EU perspectives*, 19 TELEMAT. INFORMATICS 193 (2002), at 195.

[57] See, Sherri J. Deckelboim, *Consumer Privacy on an International Scale: Conflicting Viewpoints Underlying the EU-U.S. Privacy Shield Framework and How the Framework Will Impact Privacy Advocates, National Security, and Businesses*, 48 GEO. J. INT'L L. 263 (2016), at 266.
See also, Council of Europe, European Convention on Human Rights, 4 Nov. 1950, (as amended).

[58] ECHR, *supra* note 57, art. 1.

[59] See, Boehm, *supra* note 17, at 41.
On this matter, see also, Dainel Solove, *Understanding Privacy*, 13 HARVARD UNIV. PRESS 515–530 (2008), at 3-4.

[60] ECHR, *supra* note 57, art. 8.

[61] For a discussion on the recent cases before the ECtHR see, Nora Ni Loideain, *EU Law and Mass Internet Metadata Surveillance in the Post-Snowden Era*, 3 MEDIA COMMUN. 53 (2015), at 59.

iv. Prevention of disorder or crime,

v. Protection of health and morals,

vi. Protection of rights and freedoms of others."

Established by the ECHR, European Court of Human Rights (hereafter ECtHR) is the judiciary organ of the CoE[62]. The 47 members of the European Council recognize the judiciary power of the ECtHR[63]. However, the U.S. is not a member of the European Council, therefore the judiciary power of the Court is irrelevant in the U.S. legal context. All of the EU member countries are also members of the European Council, thus the Case Law of the Court is critical understanding many aspects of the data protection law in the EU other than the matters in the area of soveregnity of the EU members[64].

Since, in the Roman Zakharov v. Russia Case, the ECtHR summarized all of its previous judgments, it puts the fundamentals of the Case Law of the Court regarding the safeguards against arbitrary and abusive interference of the public authorities[65]. The principles laid out in the judgement is as following[66]:

i. The domestic law must be accessible and sufficiently clear with regard to the interference[67];

ii. That law must clearly provide the scope and duration of the interference[68];

---

[62] THE COURT IN BRIEF, http://www.echr.coe.int/Documents/Court_in_brief_ENG.pdf (last visited Dec 15, 2017).

[63] PRESS RESOURCES - FACTSHEETS, COUNTRY PROFILES, http://www.echr.coe.int/Pages/home.aspx?p=press%2Ffactsheets&c=#n1347951547702_pointer (last visited Dec 15, 2017).
See also, 47 MEMBER STATES, https://www.coe.int/en/web/portal/47-members-states (last visited Dec 15, 2017).

[64] EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS, SURVEILLANCE BY INTELLIGENCE SERVICES: FUNDAMENTAL RIGHTS SAFEGUARDS AND REMEDIES IN THE EU VOLUME I: MEMBER STATES' LEGAL FRAMEWORKS, 13, (2015).

[65] SURVEILLANCE BY INTELLIGENCE SERVICES: FUNDAMENTAL RIGHTS SAFEGUARDS AND REMEDIES IN THE EU VOLUME II: MEMBER STATES' LEGAL FRAMEWORKS, 20 (2015).

[66] See, Roman Zakharov v. Russia, No. 47143/06, at para. 227-234 (ECtHR, Dec. 4, 2015).

[67] See, Shimovolos v. Russia, No. 30194/09, at para. 68, (ECtHR, June 21, 2011).
See also, Malone v. the United Kingdom, Series A no. 82, at para. 67, (ECtHR, Aug. 2, 1984).
See also, Leander v. Sweden, Series A no. 116, at para. 51, (ECtHR, Mar. 26, 1987).
See also, Huvig v. France, Series A no. 176-B, at para. 29, (ECtHR, Apr. 24, 1990).

[68] Malone, *supra* note 67, at para. 68.
See also, Leander, *supra* note 67, at para. 51.
See also, Huvig, *supra* note 67, at para. 29.

iii. That law must clearly provide the procedures for "storing, accessing, examining, using, communicating and destroying" the data which is subject to interference[69];

iv. The abuse should be prevented by adequate guarantees provided by the "procedures for authorisation, supervision, and review[70];"

v. The authority which is empowered to authorize surveillance must be independent and procedures for review must require that there is reasonable suspicion against the data subject to begin the surveillance, also surveillance "must be proportionate to the legitimate aims[71];"

vi. The authority which is empowered to supervise the surveillance must be independent, must have the powers that will enable sufficient control of the surveillance and public must be informed about the activities of that authority[72];

vii. As soon as the surveillance is ended, the information regarding the measure must be given to the data subject as long as this information will not jeopardize the purpose of the measure[73];

viii. Effective remedies at national level that allow the individuals challenge the legality of the interference are essential safeguards[74].

Council of Europe Data Protection Convention[75] (hereafter the Convention 108) is another tool of the CoE that sets forth the principles for the right to data

---

[69] See, Kennedy, v. the United Kingdom, No. 26839/05, at para. 122-123, (ECtHR, May 18, 2010).

[70] See, Huvig, *supra* note 67, at para. 34.
See also, Amann, *supra* note 20, para. 56-58.
See also, Valenzuela Contreras v. Spain, no. 27671/95, at para. 46, (ECtHR, Jul. 30, 1998).
See also, Prado Bugallo v. Spain, no. 58496/00, at para. 30, (ECtHR, Feb. 18, 2003).

[71] See, Klass and Others v. Germany, Series A no. 28, at para. 49-50 and 59, (ECtHR, Sep. 6, 1978).
See also, Weber and Saravia v. Germany, No. 54934/00, at para. 106, (ECtHR, June 29, 2006).
See also, Kvasnica v. Slovakia, no.72094/01, at para 80, (ECtHR, Jun. 9, 2009).
See also, Kennedy, supra note 69, at para. 153-154.

[72] See, Klass and Others, *supra* note 71, at para. 55-56.

[73] See, Klass and Others, *supra* note 71, at para. 57.
See also, Weber and Saravia, supra note 71, at para. 135.

[74] Kennedy, supra note 69, at para. 167.

[75] See, CETS 108: Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Jan. 1, 1981.

protection[76]. Even though countries other than the members of the CoE may also ratify the CEDPC, the U.S. did not ratify the Convention, hence the Convention is not binding for the U.S.[77]. However, the Convention is of significant importance in understanding the evolution of the data protection legal framework of the EU members[78].

The Article 5 of the CEDPC provides the purpose limitation, data minimization and anonymization principles[79]. Article 6 dictates that processing of the sensitive data is subject to additional safeguards[80], Article 7 dictates that certain precautions should be taken for data protection[81], Article 8 sets forth the data subjects' right to access to and rectify the data as well as have legal remedy[82]. Article 9 sets forth the derogations, parties to the convention may refrain exercising article 5,6 and 8 for the purposes of "protecting state security, public safety, the monetary interests of the State or the suppression of criminal offences; protecting the data subject or the rights and freedoms of others[83]."

Another tool of the CoE is the European Commission for Democracy through Law, also known as Venice Commission. The Venice Commission provides legal advice for the CoE member states, which aim to reach the European Standards of democracy, human rights and the rule of law[84]. The Venice Commission provides the advice regarding the right to privacy as well as the right to data protection[85]. Moreover, the U.S. is also a member state of the Commission[86]. Therefore, the

---

[76] WJ MAXWELL, CAHIER DE PROSPECTIVE THE FUTURES OF PRIVACY FOUNDATION TELECOM, INSTITUT MINES-TELECOM (2014), https://www.fondation-mines-telecom.org/wp-content/uploads/2016/01/2014-The-Futures-of-Privacy-.pdf#page=56 (last visited Dec 10, 2017). at 56.

[77] See the Full List of the countries which ratified the Convention, FULL LIST, https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures?p_auth=wKGN72rz (last visited Nov 7, 2017).

[78] Maxwell, *supra* note, 76, at 59.

[79] CEDPC, *supra* note 75, at art. 5.

[80] Id. at art. 6.

[81] Id. at art. 7.

[82] Id. at art. 8.

[83] Id. at art. 9.

[84] The Venice Commission of the Council of Europe, VENICE COMMISSION, http://www.venice.coe.int/WebForms/pages/?p=01_Presentation&lang=EN (last visited Nov 7, 2017).

[85] Ibid.

[86] Ibid.

advice provided by the Commission is taken into account by both EU members and the U.S.

The advice provided by the Venice Commission on the Democratic Oversight of the Security Services is particularly useful for this study, since it might be in help identifying the steps that must be taken by the U.S. to meet the EU standards. The advice given by the Commission in this context can be summarized as following:

i. Security and intelligence agencies must be independent from the executive governance[87];

ii. The need of operational secrecy is not a justification for not providing control and remedy mechanisms[88];

iii. More than one level of accountability mechanisms must be provided[89];

iv. Minimum standards on privacy protection must be determined by an international agreement, in this way "competing or incompatible obligations" for companies must be eliminated[90];

v. Independent control and oversight mechanisms must be provided[91].

1.2. THE EVOLUTION OF THE RIGHT TO DATA PROTECTION IN THE EU LEGAL CONTEXT

1.2.1. The Evolution of The Right to Data Protection in the EU Treaties

The European countries, with the aim of creating a single market, signed the Treaty of Rome in 1957, establishing the European Economic Community. The European Union was established in accordance with the Maastricht Treaty on European Union in 1993[92]. In 2007, the Maastricht Treaty, and Treaty of Rome

[87] EUROPEAN COMMISSION FOR DEMOCRACY THROUGH LAW (VENICE COMMISSION), REPORT ON THE DEMOCRATIC OVERSIGHT OF THE SECURITY SERVICES ADOPTED, para. 252 (2007).
[88] Id. at para. 258.
[89] Id. at para. 259.
[90] EUROPEAN COMMISSION FOR DEMOCRACY THROUGH LAW (VENICE COMMISSION), UPDATE OF THE 2007 REPORT ON THE DEMOCRATIC OVERSIGHT OF THE SECURITY SERVICES AND REPORT ON THE DEMOCRATIC OVERSIGHT OF SIGNALS INTELLIGENCE AGENCIES, para. 139 (2015).
[91] Id. at para. 140.
[92] European Union, THE HISTORY OF THE EUROPEAN UNION (2017), https://europa.eu/european-union/about-eu/history_en (last visited Nov 6, 2017).

are amended and they are renamed as the Treaty on European Union (hereafter TEU) and The Treaty on Functioning of the European Union (hereafter TFEU)[93]. Today, these treaties along with the Charter of Fundamental Rights of the European Union (The CFREU) are regarded as primary sources of the EU Law[94].

On 7 December 2000, the European Council issued the CFREU. The Charter, in addition to the rights provided by the ECHR, sets forth the third generation fundamental rights[95]. Treaty of Lisbon (2009) ensures that the Charter is binding for the institutions and bodies of the EU as well as for the national authorities implementing the EU Law[96]. The Article 7 and 8 are of great importance in terms of data privacy and protection[97]. The Article 7 protects the privacy of private and family life, home and communications of all humans[98]. The Article 8 protects the right to data protection, and according to the Article, personal data should be processed based on consent and specified purposes[99]. The Article defines right to access and right to have the data rectified, moreover imposes that compliance must be monitored by an independent authority[100].

Another relevant article of the Charter is the Article 47[101]. Even though the article 47 has effects on all of the rights mentioned in the Charter, it is of particular importance for the right to privacy[102]. The Article 47 sets forth provisions regarding the right to effective remedy and to a fair trial. The individuals in the EU should be able to have effective remedy, when their rights

---

[93] See, TFEU, *supra* note 7.

[94] See, European Parliament, FACT SHEETS ON THE EUROPEAN UNION, SOURCES AND SCOPE OF EUROPEAN
http://www.europarl.europa.eu/atyourservice/en/displayFtu.html?ftuId=FTU_1.2.1.html (last visited Nov 10, 2017).
See also, Boehm, *supra* note 17, at 11.

[95] In that regard, right to data protection is regarded as a third generation fundamental right. See, Richard J Peltz-Steele, *The pond betwixt: Differences in the US-EU data protection/safe harbor negotiation*, 19 J. INTERNET LAW 1–30 (2015), at 15.

[96] Boehm, *supra* note 17, at 25.

[97] Id, at 11.

[98] CFEU, supra note 6, at art. 7.

[99] Id. at art. 8.

[100] Ibid.

[101] Id. at art. 47.

[102] Ibid.
See, Maximillian Schrems v. Data Protection Commissioner, C-362/14, at para. 95, (CJEU, Oct. 6, 2015).

are violated[103]. The court should be independent, established by law, provide judicial review within a reasonable time, and the hearing should be open to public and fair[104].

The Article 39 of the TEU authorizes the Council of Europe for adopting a decision that imposes the principles regarding the data processing by the EU Members and establishment of a common policy on security matters as well as the free movement of personal data[105].

1.2.2. The Right to Data Protection in the EU Secondary Legislations and Policies

The secondary legislation of the EU is mainly comprised of Regulations and Directives[106]. In addition to that, Decisions, recommendations and opinions are also considered as secondasry legislation[107]. For the EU members, regulations hava a binding nature, and they are directly applicable meaning; EU members do not need to transpose regulations to the national law[108]. If Regulations conflict with the national laws, the national laws supersede[109].

Directives are binding upon the EU members as well[110]. However, directives are firstly transposed into national laws to bind the members[111]. According to the CJEU, there is an exception to that: if the provisions of the directive are related to the rights of the individuals, imperative and sufficiently clear, and the directive is not transposed to the national law as intended, the directive is applicable[112].

---

[103] Ibid.
[104] Ibid.
[105] As a consequence, TEU empowers the Council of Europe to adopt legislation regarding the cyber space as well. See, Patrick G. Crago, *Fundamental Rights on the Infobahn : Regulating the Delivery of Internet Related Services Within the European*, 20 HAST. INT'L COMP. L. REV. 467 (1997), at 498.
[106] SOURCES AND SCOPE OF EUROPEAN UNION LAW, http://www.europarl.europa.eu/atyourservice/en/displayFtu.html?ftuId=FTU_1.2.1.html (last visited Nov 10, 2017).
[107] Ibid.
[108] Ibid.
[109] Ibid.
[110] Ibid.
[111] Ibid.
[112] Ibid.

Decisions are binding upon the members. The decisions are applied in a way comparable to the Directives. The EU members transpose the Decisions into the national laws. On the other hand, Recommendations and Opinions are not binding in nature. They provide guidance for the EU members[113].

The EU Parliament approved the GDPR on 14 April 2016[114]. The Regulation will enter into effect on 25 May 2018, and by that time the Regulation will replace the current Directive, DPD[115]. As the GDPR will be enforced soon, a special attention will be given to the GDPR throughout this study.

The main Directive related to the data protection law is, as mentioned before DPD, which is adopted by the EU Parliament in 1995[116]. The aim of the DPD is to enable free flow of data by ensuring that the data protection legal frameworks of the EU members do not undermine the uniform level of data protection[117].
Directive for the Electronic Communications Sector (hereafter DECS) is a Directive that sets forth exclusive provisions for the electronic communications sector[118].

In addition to the data protection, Regulation (EC) No. 45/2001 on the protection of individuals with regard to the processing operations of the institutions and bodies of the Community and on the free movement of such data (hereafter PIPPD) has provisions regarding the processing operations of the EU Institutions[119].

1.3. THE EVOLUTION OF THE RIGHT TO DATA PROTECTION IN THE US LEGAL CONTEXT

The article "The Right to Privacy" written by Samuel Warren and Louis Brandeis, published in the 1890 is acknowledged as the first publication on the

[113] Ibid.
[114] See, HOME PAGE OF EU GDPR, http://www.eugdpr.org/ (last visited Nov 11, 2017).
[115] Ibid.
[116] EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS AND THE COUNCIL OF EUROPE, HANDBOOK ON EUROPEAN DATA PROTECTION LAW, 17 (2014).
[117] Id. at 18.
[118] Id. at 19.
[119] Ibid.

right to privacy in the United States[120]. In that article the definition of the right to privacy is given as "a right to be let alone[121]." Eventually, that definition is adopted by the U.S. Case Law, and U.S. Supreme Court Justice Louis Brandeis in 1928 gave the same definition "a right to be let alone" and he added it is "the most comprehensive of rights and the right most valued by civilized men[122]." Today, it is argued that the American Common Law Method by its nature, is not capable of creating a legal framework that can address all of the data protection and privacy issues as is possible by the civil law[123]. Nevertheless, throughout the years Federal Laws and Regulations set forth provisions on the matter, and several amendments to the Constitution have been made. Despite all those legislation efforts, critics point out the lack of consensus on conceptualizing privacy[124].

In addition to the lack of a common privacy concept in the U.S., the lack of a comprehensive national law regarding the data processing adds complexity to the issue[125]. Instead of a common legal framework, there are a number of multilevel federal and state level regulations, which are inconsistent at times[126]. Because of this situation, there are self-regulatory guidelines and frameworks regarding the data protection. Consequently, the regulators as well utilize those self-regulatory guidelines and frameworks to ensure the enforcement[127]. As there are a huge number of state laws in the U.S., and each state law is enforced only within the borders of that state, the state laws are out of the scope of this study.

---

[120] İKBAL GÜR, KIŞISEL VERILERIN KORUNMASI HUSUSUNDA AB ILE ABD ARASINDA ÇIKAN UYUŞMAZLIKLAR VE ÇÖZÜM YOLLARI, 138 (2010).
[121] Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. LAW REV. 193–220 (1890), at 193.
[122] Olmstead v. United States 277 U.S. 438 (1928).
[123] İkbal Gür, supra note 120, at 140.
[124] Daniel J. Solove, *Understanding Privacy*, 13 HARVARD UNIV. PRESS 515–530 (2008), at195.
[125] Bignami, *supra* note 11, at 5.
[126] Id. at 8.
[127] Ieuan Jolly, DATA PROTECTION IN THE UNITED STATES: OVERVIEW, https://uk.practicallaw.thomsonreuters.com/6-502-0467?transitionType=Default&contextData=(sc.Default)&firstPage=true&bhcp=1, (last visited Nov 11, 2017).

1.3.1.The Constitutional Background of the Right to Data Protection in the U.S. Legal Context

The provision related to the right to privacy and data protection can be found in the fourth amendment of the U.S. Constitution[128]. It is criticized that the there is no significant protection provided by the Constitution in those ares, therefore, the main protection provided by the U.S. law is by the virtue of other type of regulations[129]. However, there are provisions in the fourth amendment, which seek to protect the U.S. data subjects from the arbitrary surveillance activities of the public authorities[130]. That protection is provided by the fourth amendment given that searches and seizures must be reasonable and rely on probable cause[131].

Furthermore, case law of the U.S. puts additional burden on the data subjects which seek to have legal remedy relying on the fourth amendment: according to the Supreme Court, the claimant must show that he has a justifiable expectation of privacy to be able to claim that his rights are violated[132]. In addition to that, the protection provided by the Constitution is only for the U.S. citizens[133]. Therefore, it can be concluded that neither the right to privacy nor the right to data protection are endowed to the foreign citizens, including the EU subjects under the U.S. Constitution.

1.3.2. The Right to Data Protection in the Federal Laws (National Laws) of the U.S.

The Federal Trade Commission Act[134] (hereafter the FTC Act) is evaluated under the consumer law[135]. The section 5 of the Act prohibits the unfair or

---

[128] U.S. CONST. amend. IV.
[129] Bignami, *supra* note 11, at 8.
[130] Sherri J. Deckelbolm, *Consumer Privacy on an International Scale: Conflicting Viewpoints Underlying the EU-U.S. Privacy Shield Framework and How the Framework Will Impact Privacy Advocates, National Security, and Businesses*, 48 GEO. J. INT'L L. 263 (2016), at 272.
[131] U.S. CONST. amend. IV.
[132] Ryan Strasser, *supra* note 11.
[133] Bignami, *supra* note 11, at 8.
[134] 15 U.S.C. §§41-58
[135] Activities of the intelligence agencies are out of the scope of the FTC Act. See, Boehm, *supra* note 17, at 37.

deceptive commercial practices[136]. As the unfair or deceptive practices can be conducted by any means, whether it is in a digital medium, online or offline, the FTC Act covers practices by all those means[137]. In that regard, The Federal Trade Commission (hereafter FTC) is established according to the Section 5 of the FTC Act, and the FTC is the enforcement organ of the FTC Act[138]. In addition, the FTC enforces Children's Online Privacy Protection Act[139] (hereafter COPRA).

The Financial Services Modernization Act[140] (hereafter the FSM) is a federal act regulating the finance sector. The scope of the act is collection, use and disclosure of the finance related information by all of the financial institutions that offer finance related services and products[141]. Though, some commentators argue that the Act does not provide data protection related rights as the DPD does[142]. However, to a degree, the disclosure of the finance sector related personal data is limited by that act, and FTC has enforcement on financial institutions regarding the personal data, as the Section 5 of the FTC Act does not exclude that sector[143].

The Health Insurance Portability and Accountability Act (hereafter the HIPAA) is a federal act regulating the medical sector[144]. The institutions and persons that collect the health-related personal data are all enforced by the HIPAA[145]. There are provisions in the HIPAA regulating the processing of the health-related personal data[146].

The Fair Credit Reporting Act (hereafter FCRA) is a federal act regulating the activities of consumer reporting agencies. Some institutions need consumer

---

[136] Ibid.
[137] To see the guidelines issued by the FTC regarding the big data, internet of things, mobile privacy, and privacy technologies see, CAMERON F. KERRY ET AL., ESSENTIALLY EQUIVALENT: A COMPARISON OF THE LEGAL ORDERS FOR PRIVACY AND DATA PROTECTION IN THE EUROPEAN UNION AND UNITED STATES, 149, (2016).
[138] Id. at 146.
[139] 15 U.S.C. §§6501-6506
[140] 15 U.S.C. §§6801-6827
[141] Michelle Frasher, *Adequacy versus equivalency: Financial data protection and the U.S.-EU divide*, 56 BUS. HORIZ. 787–795 (2013), at 790.
[142] Id. at 790.
[143] See, 15 U.S.C. § 57a(f)(3), 15 U.S.C. § 57a(f)(4) and 15 U.S.C. § 45(a)(2).
[144] Stephen Hinde, *Privacy legislation: A comparison of the US and European approaches*, 22 COMPUT. SECUR. 378–387 (2003), at 379.
[145] Ibid.
[146] Kerry et al., *supra* note 137, at 141.

reports regarding certain products or services, and the consumer reporting agencies provide those reports. Those consumer reports might include the information regarding the financial status, credit history and similar information that is utilized in determining the credibility of an individual. As information involved in those reports require the use of personal data, the FCRA is one of the acts that regulate the protection of personal data.

The Controlling the Assault of Non-Solicited Pornography and Marketing Act[147] (hereafter CAN-SPAM Act) and the Telephone Consumer Protection Act[148] (hereafter TCPA) are federal laws that regulate the protection of personal data regarding the electronic mails and telephone numbers[149].

The Electronic Communications Privacy Act[150] (hereafter the ECPA) and the Computer Fraud and Abuse Act[151] (hereafter the CFAA) are federal laws that regulate the interference to the electronic communications and computers.

Judicial Redress Act (hereafter the JRA) is a federal law enacted by the Congress in 2016. The aim of the JRA is to provide the right to redress for a number of U.S. allies including the EU members[152]. The redress act under the JRA enables the EU subjects seek redress in the U.S. courts when they believe their personal data is unlawfully disclosed to the U.S. public authorities for the purpose of law enforcement[153].

The Foreign Intelligence Surveillance Act (hereafter FISA), issued in 1978 is a federal law regulating the surveillance activities, which aim to obtain intelligence information from the foreign sources[154]. There is also the Foreign Intelligence Surveillance Court (hereafter FISC), which is created by the FISA[155].

---

147 15 U.S.C. §§7701-7713 and 18 U.S.C. §§1037
See, Kerry et al., *supra* note 137, at 144.
148 47 U.S.C. §227 et seq
149 See, Kerry et al., *supra* note 137, at 144.
150 18 U.S.C. §2510
151 18 U.S.C. §1030
152 To see the conditions for the foreign countries to be regarded as U.S. allies under the Judicial Redress Act, GARY CLYDE HUFBAUER & EUIJIN JUNG, PB 16-12 THE US-EU PRIVACY SHIELD PACT : A WORK IN PROGRESS, 3 (2016).
153 SHARA MONTELEONE & LAURA PUCCIO, FROM SAFE HARBOUR TO PRIVACY SHIELD, 10 (2017).
154 Venice Commission, *supra* note 90, at para. 127.
155 Ibid.

The Section 702 of the FISA allows US authorities to conduct surveillance activities on foreign elements without a court warrant[156].

USA Freedom Act, issued on June 2015, is a federal law that amended a number of intelligence surveillance related acts. The Act regulates the bulk collection of data setting forth the restrictions for bulk collection[157].

1.3.3. The Right to Data Protection in the Secondary Legislations of the U.S.

Presidential Policy Directive 28[158] (hereafter PPD-28) regulates the signal intelligence activities of the U.S. The importance of the PPD-28 in the context of this study is that the PPD-28 provides guideline on the further use of the personal data obtained through signal intelligence activities. The dissemination and anonymization requirements of the personal data is set forth. Along with that, the standards of training for the intelligence agency employees and compliance reviews are provided. It must be noted that, the PPD-28 is a mere guidance and not enforceable by the law[159].

Executive Order 12333[160] sets forth the provisions for the techniques and procedures of collection of personal data and the oversight mechanisms[161].

1.4. THE EVALUATION OF THE U.S. APPROACH OF THE RIGHT TO DATA PROTECTION WITH REFERENCE TO THE EU LAW

Firstly, as mentioned earlier, under the U.S. Law, the right to data protection is treated as if it is a consumer right[162]. Because of that, and because of the fact

---

[156] To see how the surveillance activities are conducted under the Section 702 see, Id. at para. 128.
[157] Haufbaer & Jung, *supra* note 152, at 6.
[158] See, PRESIDENTIAL POLICY DIRECTIVE - SIGNALS INTELLIGENCE ACTIVITIES (2014), https://obamawhitehouse.archives.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities (last visited Dec 17, 2017).
[159] PPD-28, §6(d) and PPD-28, §6(b).
[160] EXECUTIVE ORDERS, https://www.archives.gov/federal-register/codification/executive-order/12333.html (last visited Dec 17, 2017).
[161] MARK BRENNAN, BRET COHEN & VICTORIA HORDERN, LEGAL ANALYSIS OF THE EU-U.S. PRIVACY SHIELD, 39 (2016).
[162] Reidenberg, *supra* note 5, at 1335.

that foreign elements[163] do not have those rights[164], the transactions between the foreign and the U.S. elements pose a controversy in the context of right to data protection[165]. The U.S. corporations and public authorities have the power which allows them to abuse the personal data of the foreign elements[166]. That's why a number of governments which aimed to protect the personal data of their subjects made agreements with the U.S.[167].

Secondly, compared to the legal system of the EU, the U.S. has a very complex legal system where the federal laws and state laws sometimes conflict, and there is no comprehensive data protection law[168]. Therefore, even there are provisions that protect the interests and rights of a foreign element, it might be challenging for him to identify the appropriate avenue in that complexity[169]. In that regard, the agreements between the U.S. and the other governments on data protection should simplify this mechanism, and provide easily reachable avenues for the subjects of that government.

Since the scope of this study is limited to the EU-U.S. Privacy Shield, how other frameworks provide simplified redress options and enhanced rights for people other than EU subjects will not be evaluated. However, the question whether the EU-U.S. Privacy Shield is able to provide that is one of the main concerns of this study, and will be answered to the extent possible.

See also, Paul M. Schwartz & Danie J. Solove, *Reconciling Personal Information in the United States and European Union*, 102 SSRN ELECTRON. J. 877–916 (2013), at 880.

[163] Individuals, public and private organizations.

[164] Reidenberg, *supra* note 5, at 1335.

[165] Haufbaer & Jung, *supra* note 152, at 2.

[166] Ibid.

[167] The EU-U.S. Privacy Shield and the Swiss-U.S. Privacy Shield frameworks can be showed as examples to that.

[168] For an example of "loopholes" in the data protection law of the U.S. federal law, see the California example, Frasher, *supra* note 141, at 791.

[169] See, ARTICLE 29 DATA PROTECTION WORKING PARTY, EU – U.S. PRIVACY SHIELD – FIRST ANNUAL JOINT REVIEW, 8-9 (2017).

SECTION 2

THE KEY FEATURES OF THE EU DATA PROTECTION DIRECTIVE

2.1. INTRODUCTION

DPD, adopted in 1995, is regarded as the principal legal document on data protection in the EU[170]. According to the CJEU, DPD is a legal instrument that provides a standard level of data protection for all of the EU members[171]. All of the EU members must provide a level of data protection that is set forth in the DPD, and a complete harmonization is intended for the EU members rather than meeting minimal level of requirements[172].

As mentioned earlier, before the DPD, the data protection in the EU members were ensured according to the Convention 108[173]. As expected, the provisions of the DPD are similar to those of the Convention 108[174]. Moreover, there are a number of new instruments brought about by the DPD. One of the most important improvements is an independent supervisory mechanism to provide compliance monitoring[175]. The judicial authority that inspects the compliance of the EU members to the DPD is CJEU[176].

Since DPD is regarded as the principal legal document on the data protection, and it provides the standards to the data protection, to evaluate the data protection level of a country with respect to the EU, one must scrutinize the DPD. As in the following sections, the DPD will be regarded as a point of reference in the context of data protection; this section will introduce the key features of the DPD.

---

[170] Handbook on European Data Protection Law, *supra* note 116, at 17.
[171] Id. at 18.
[172] Ibid.
[173] Deckelboim, *supra* note 57, at 267.
See, CEDPC, *supra* note 75.
[174] Handbook on European Data Protection Law, *supra* note 116, at 18.
[175] Ibid.
[176] Ibid.

2.2. THE TERMINOLOGY USED IN THE EU DATA PROTECTION DIRECTIVE

According to the Article 2(a) of the DPD, personal data is "any information relating to an identified or identifiable natural person[177]." Any information which identifies a person whether it be directly or indirectly, can be regarded as personal data[178]. Identification number of the person, or "factors specific to his physical, physiological, mental, economic, cultural or social identity" are the examples of references to identify a person[179].

Article 2(b) of the DPD defines the processing as operation(s) performed on personal data such as "collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction[180]."

Article 2(c) of the DPD defines the personal data filing system as a structured set of personal data that can be accessed by certain criteria[181].

Article 2(d) of the DPD defines the controller as a person or a body, which "determines the purposes and means of the processing[182]."

Article 2(e) of the DPD defines the processor as a person or a body that "processes the personal data on behalf of the controller[183]."

Article 2(f) of the DPD defines the third party as a person or a body "other than the data subject, the controller, the processor and the persons who, under the direct authority of the controller or the processor, are authorized to process the data[184]."

---

[177] See, DPD, *supra* note 1, art. 2(a).
[178] Ibid.
[179] Ibid.
[180] Id. art. 2(b).
[181] Id. art. 2(c).
[182] Id. art. 2(d).
[183] Id. art. 2(e).
[184] Id. art. 2(f).

Article 2(g) of the DPD defines the recipient as a person or a body "whom the data is disclosed. Nevertheless, authorities, to which the data is disclosed, are not regarded as recipients, if they receive the data on the grounds of an inquiry[185].

Article 2(h) of the DPD defines the data subject's consent as "freely given specific and informed" agreement of the data subject for the processing of his personal data[186].

2.3. THE GENERAL PRINCIPLES PROVIDED BY THE EU DATA PROTECTION DIRECTIVE

The principle of lawful processing is provided under the Article 6(1)(a) and 6(1)(b) of the DPD[187]. In that regard, the EU members should provide that processing is performed "lawfully"[188]. The collection of the personal data should be on the grounds of "legitimate purposes[189]." The further processing should be on the grounds of those purposes[190]. In the same manner, *the principle of purpose specification and limitation* requires that the collection and processing should be limited to "specified and explicit" purposes[191].

Under *the data quality principles*, *relevancy of data* is described by the Article 6(1)(c) of the DPD[192]. In that regard, EU members should ensure that the personal data is "adequate, relevant and not excessive" with reference to the original purposes for which the data is collected. That is required for the further processing as well[193].

Under *the data quality principles, accuracy of data* is described by the Article 6(1)(d) of the DPD[194]. In that regard, EU members should ensure that the personal

[185] Id. art. 2(g).
[186] Id. art. 2(h).
[187] Id. art. 6(1)(a) and 6(1)(b).
[188] Ibid.
[189] Ibid.
[190] Ibid.
[191] Ibid.
[192] Id. art. 6(1)(c).
[193] Ibid.
[194] Id. art. 6(1)(d).

data is "accurate and, where necessary, kept up to date"[195]. That article also requires that the personal data should be "erased or rectified" where they are "inaccurate or incomplete[196]."

Under *the data quality principles, limited retention of data* is described by the Article 6(1)(e) of the DPD[197]. In that regard, EU members should ensure that the personal data is "kept in a form which permits identification of data subjects for no longer than is necessary[198]". Necessary time period here is determined according to the requirements of the purposes for which data are collected or further processed[199].

Under *the data quality principles, exemption for scientific research and statistics* is described by the Article 6(1)(e) of the DPD[200]. In that regard, EU members should ensure that there are safeguards to keep the data longer than necessary for the purposes of "historical, statistical or scientific use[201]".

Under *the data quality principles, the principle of fair processing* is provided by the Article 6(1)(a) of the DPD[202]. In that regard, EU members should ensure that the data is "processed fairly[203]".

Under *the data quality principles, the principle of accountability* is provided by the Article 6(2) of the DPD[204]. In that regard, EU members must ensure that the controller complies with the principles mentioned here[205].

---

[195] Ibid.
[196] Ibid.
[197] Id. art. 6(1)(e).
[198] Ibid.
[199] Ibid.
[200] Ibid.
[201] Ibid.
[202] Id. art. 6(1)(a).
[203] Ibid.
[204] Id. art. 6(2).
[205] Ibid.
For a guide on Principles mentioned here with respect to the articles of the DPD see, Handbook on European Data Protection Law, *supra* note 116, at 61-62.

2.4. JUDICIAL REMEDIES, LIABILITY AND SANCTIONS PROVIDED BY THE EU DATA PROTECTION DIRECTIVE

According to the Article 22 of the DPD, EU members must ensure that judicial remedy, regarding the processing, is provided to every person[206]. The article states that the fact a member state provides an administrative remedy does not imply that judicial remedy is not required[207].

According to the Article 23 of the DPD, EU members must ensure that if a person suffers "damage as a result of unlawful processing" the controller compensates his damages[208]. The article further states that the controller is not liable if he can show that he does not have any responsibility for the event causing the damage[209].

According to the Article 24 of the DPD, EU members are responsible for the "full implementation of the provisions" set forth by the DPD[210]. The article further requires EU members to impose sanctions for the persons and bodies that infringe the provisions of the DPD[211].

2.5. TRANSFER OF PERSONAL DATA TO THIRD COUNTRIES UNDER THE EU DATA PROTECTION DIRECTIVE

Transfer of personal data to third countries is subject to the Article 25 of the DPD[212]. Article 25(1) states that such a transfer can be performed with the condition that the third country "ensures an adequate level of protection[213]". Article 25(2) states that the evaluation of that adequacy is subject to the

[206] DPD, *supra* note 1, art. 22.
[207] Ibid.
[208] Id. art. 23.
[209] Ibid.
[210] Id. art. 24.
[211] Ibid.
[212] Id. art. 25.
[213] Id. art. 25(1).

assessment of " all the circumstances surrounding" the transfer[214]. The following factors have particular importance:

i. "The nature of the data,
ii. The purpose and duration of the processing,
iii. The country of origin and country of final destination,
iv. The rules of law, both general and sectoral, in the third country,
v. The professional rules and security measures in the third country[215]."

According to the Article 25(1), the Commission has the authority to declare that the data protection level in a third country is adequate[216]. In such a case, the EU members are free to perform such a transfer to that third country[217]. On the other hand, the Commission has the authority to declare that the data protection level in a third country is not adequate[218]. In such a case, member countries should avoid such a transfer to that third country[219]. However, according to the Article 26, in the presence of appropriate contractual clauses EU members may allow such a transfer to a third country with which those contractual clauses are agreed, or there are other lawful grounds for the transfer[220].

2.6. THE STANDARDS OF THE SUPERVISORY AUTHORITY PROVIDED BY THE EU DATA PROTECTION DIRECTIVE

Article 28 of the DPD sets forth the standards for the supervisory authority, which must be established by each of the EU members to monitor the compliance of its subjects to the provisions adopted adhering to the DPD[221]. The supervisory authorities in that context must be given the following powers:

i. "investigative powers:" the authorities should be able to access the data relevant to the investigation,

---

214 Id. art. 25(2).
215 Ibid.
216 Id. art. 25(1).
217 Ibid.
218 Id. art. 25(3).
219 Id. art. 25(4).
220 Id. art. 26.
221 Id. art. 28.

ii. "effective powers of intervention:" the authorities should be able to provide opinions and publications for the processors,

iii. "the power to engage in legal proceedings:" the ability to refer to the judicial authorities when a violation to the DPD is identified[222].

The Article 28 along with the powers to be endowed provides the responsibilities of the supervisory authorities. In that regard, each supervisory authority:

i. must assess the complaints lodged[223],

ii. must issue regular public reports of its activities[224],

iii. must exert its powers when requested by the national law[225].

2.7. WORKING PARTY ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA

The article 29 of the DPD creates an independent body under the title of Working Party on the Protection of Individuals with regard to the Processing of Personal Data (hereafter WP29) with advisory status[226] that will:

i. Assess the application of the Directive in EU members[227],

ii. Assess the protection level of the third countries to inform the Commission[228],

iii. Propose improvements to the DPD[229],

iv. Assess the codes of conduct at Community Level and give opinion[230].

2.8. EXEMPTIONS TO THE EU DATA PROTECTION DIRECTIVE

The Article 13 of the DPD provides the exemptions to the DPD. Data quality principles set forth by the Article 6(1), the task of informing data subjects set forth

[222] Id. art. 28(3).
[223] Id. art. 28(4).
[224] Id. art. 28(5).
[225] Id. art. 28(6).
[226] Id. art. 29(1).
[227] Id. art. 30(1)(a).
[228] Id. art. 30(1)(b).
[229] Id. art. 30(1)(c).
[230] Id. art. 30(1)(d).

by the Article 10 and Article 11(1), right of access provided by the Article 12, and the obligation regarding the publicizing of processing operations provided by the Article 21 may be dismissed by the EU members adopting legislative measures for safeguarding:

i. "national security[231];
ii. defence[232];
iii. public security[233];
iv. the prevention, investigation, detection and prosecution of criminal offences, or of breaches of ethics for regulated professions[234];
v. an important economic or financial interest of a Member State or of the European Union, including monetary, budgetary and taxation matters[235];
vi. a monitoring, inspection or regulatory function connected, even occasionally, with the exercise of the aforementioned supervisory authority[236],
vii. the protection of the data subject or of the rights and freedoms of others[237]."

2.9. EVALUATION OF THE IMPORTANCE OF THE EU DATA PROTECTION DIRECTIVE IN THE CONTEXT OF THIS STUDY

As the focus of this study is Privacy Shield, and the data protection level of the U.S. compared to that of the EU, the DPD plays a significant role identifying the data protection level of the EU. The reason is that the DPD is the principal legal instrument of the EU regarding the data protection[238].

In that regard, it is essential to, in a comprehensive way, analyze the general principles, the options of legal remedy, the standards for the supervisory authority provided by the DPD, to be able to assert that the U.S. provides EU level data

[231] Id. art. 13(1)(a).
[232] Id. art. 13(1)(b).
[233] Id. art. 13(1)(c).
[234] Id. art. 13(1)(d).
[235] Id. art. 13(1)(e).
[236] Id. art. 13(1)(f).
[237] Id. art. 13(1)(g).
[238] Handbook on European Data Protection Law, *supra* note 116, at 17.

protection, or contrarily, U.S. does not provide a data protection in that level because of certain shortcomings. This section of the study however, only provided an introduction to the DPD. Therefore, in the following sections of this study, the key concepts of the DPD will be reviewed, and where necessary, a depth will be added to the DPD utilizing the case law of the EU.

The Article 25 of the DPD, as it comprises principles for the data transfers to the third countries, is significant identifying the legal grounds of such a transfer. The preliminary findings show that "all the circumstances surrounding" the transfer has significance to be able to conclude that a third country provides an adequate level of data protection. In addition to that, the methods used by the Commission[239] in such an evaluation will be taken into account also, though in a critical way.

SECTION 3

THE EMERGENCE AND INVALIDATION OF THE EU-U.S. SAFE HARBOUR

3.1. INTRODUCTION

The DPD, regarding the cross-border personal data transfers require an adequate level of data protection from third countries[240]. As mentioned earlier, the evaluation of adequacy is performed pursuant to the principles worded in the Article 25 of the DPD[241]. As the cross-border data transfers between the EU and the U.S. comprises a very large percentage of the global cross-border data transfers[242], the evaluation of adequacy of data protection in the U.S. is a

[239] The Commission evaluates the adequacy of the data protection in the U.S. in its adequacy decision. See, Privacy Shield, *supra* note 42.
[240] See Loidean, *supra* note 36, at 8.
[241] DPD, *supra* note 1, art. 25.
[242] See, RACHEL F FEFER, SHAYERAH I AKHTAR & WAYNE M MORRISON, DIGITAL TRADE AND U.S. TRADE POLICY, 20 (2017).

significant issue. Particularly, the lack of a comprehensive data protection legal framework in the U.S. entangles the issue[243].

To provide a solution for this issue, the EU and the U.S. conducted negotiations a number of times[244]. As stated earlier, under the DPD, the Commission has the authority to declare that data proteciton level of a third country is adequate[245]. These decisions are called "adequacy decisions".

On 26 July 2000, the Commission adopted the Decision 520/2000/EC[246] (hereafter the Safe Harbour Decision). The Decision declared that the data protection level of the U.S. is adequate, in the scope of the Safe Harbour Privacy Principles and Frequently Asked Questions issued by the Department of Commerce[247] (hereafter the Safe Harbour). Accordingly, the Safe Harbour Decision enabled the free flow of the data from the EU to the organizations in the US, which were self-certified to the Safe Harbour[248].

On 26 September 2013, the number of certified organizations was 3246, and those organizations were mainly the US companies including a good number of Fortune 500[249] companies. Considering the number of the certified US organizations and the trade volume they create, it is reasonable to assert that the overall impact of the Safe Harbour Decision on the data transfer practices was significant.

Nevertheless, the Safe Harbour Decision was declared invalid by the CJEU on 6 October 2015 as Maximillian Schrems, a EU citizen, lodged a complaint with the Data Protection Authority of Ireland, regarding the intelligence activities

---

[243] Gerhard Steinke, *Data privacy approaches from US and EU perspectives*, 19 TELEMAT. INFORMATICS 193 (2002), at 198.

[244] Among others, the Privacy Shield and Safe Harbour arrangements are of particular importance of this study.

[245] DPD, *supra* note 1, art. 25(1).

[246] 2000/520/EC: Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council 2441) on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions, O.J. (L 215), (2000), [hereinafter Safe Harbour].

[247] Id. art. 1.

[248] EUROPEAN COMMISSION, COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL ON THE FUNCTIONING OF THE SAFE HARBOUR FROM THE PERSPECTIVE OF EU CITIZENS AND COMPANIES ESTABLISHED IN THE EU, 2 (2013).

[249] FORTUNE 500 TECHNOLOGY COMPANIES | FORTUNE, http://fortune.com/2016/06/07/fortune-500-technology-companies/ (last visited Dec 18, 2017).

of the US government[250] (hereafter the Schrems Decision). As the Privacy Shield is the updated version of the Safe Harbour[251], and the CJEU has judicial power on the Privacy Shield similar to the Safe Harbour[252], understanding the Safe Harbour and the following invalidity decision is essential understanding the Privacy Shield and how CJEU can exert its judicial power on the Privacy Shield. Therefore, this section provides an introduction to the Safe Harbour and the Schrems Decision.

3.2. THE KEY FEATURES OF THE SAFE HARBOUR

3.2.1. The Principles Provided By The Safe Harbour

The Notice Principle requires from the organizations to inform the individuals about the purposes of the collection and use of the personal data[253]. In that regard, Annex I of the Safe Harbor requires that, as soon as practicable and before usage of the data or transfer of the data to the third parties, information must be given on:

i. The contact information for inquiries and complaints,

ii. The types of third parties to which the organization discloses personal information,

iii. The rights of the data subjects to limit the use and disclosure of their data[254].

The Choice Principle provides that the organizations should provide the individuals the right to determine whether their data will be disclosed to a third party or processed for a purpose that is "different from" the legitimate purposes[255].

---

[250] Mira Burri & Rahel Schär, *The Reform of the EU Data Protection Framework: Outlining Key Changes and Assessing Their Fitness for a Data-Driven Economy*, 6 J. INF. POLICY 479 (2016), at 485.

[251] See, Schrems, *supra* note 41.
See also, Stephanie Hare, *For your eyes only: U.S. technology companies, sovereign states, and the battle over data protection*, 59 BUS. HORIZ. 549–561 (2016), at 554.

[252] See, Christopher Kuner, *Reality and Illusion in EU Data Transfer Regulation Post Schrems*, 18 GER. L.J. 881 (2017), at 884.

[253] Safe Harbour, *supra* note 246, ANNEX I.

[254] Ibid.

[255] Legitimate purposes are the purposes which are compatible with the purposes for which the data was originally collected or subsequently authorized by the individual.
See, Safe Harbour, *supra* note 246, ANNEX I, Choice.

In such a case, if the personal data is considered as sensitive[256], the data subject must give "affirmative or explicit (opt in) choice[257]".

The Safe Harbour sets forth the provisions regarding the accountability for the Onward Transfers[258]. To be able to transfer data to third parties (or agents[259]), organizations may free themselves from responsibility, in case that the third parties process the data unlawfully[260], if the organization does not know and should not know that the third party agent will process the data in such a way or necessary measures had been taken by the organizations to prevent the incident[261].

Security Principle comprises the provisions regarding the precautions that the organizations must take[262]. These precautions are against the "loss, misuse and unauthorized access, disclosure, alteration and destruction" of the personal data[263]. Organizations must comply with this principle "creating, maintaining, using or disseminating" the personal data. However, neither under the Security Principle nor under other provisions of the Safe Harbour, there are details regarding those precautions[264].

Data Integrity Principle requires that the personal data must be accurate, complete, and current compatible to the legitimate purposes[265]. A similar language with the DPD is used in relation to the *principles relating to data quality*[266]. An organization should not process the data for the purposes "different from" the legitimate purposes.

---

[256] The examples to the sensitive data are personal data specifying medical or health conditions, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership or information specifying the sex life of the individual. See the Choice Principle, Safe Harbour, *supra* note 246, ANNEX I.

[257] Ibid.

[258] Id. ANNEX I, Onward Transfers.

[259] An agent is a third party which perform task(s) on behalf of and under the instructions of the organization. See, Ibid.

[260] Contrary to restrictions or representations.

[261] Safe Harbour, *supra* note 246, ANNEX I, Onward Transfers.

[262] Safe Harbour, *supra* note 246, ANNEX I, Security.

[263] Ibid.

[264] Whereas in the EU, DPD lays forward the details of the security measures to be taken. See, DPD, *supra* note 1, recital 46.

[265] The purposes which are compatible with the purposes for which the data was originally collected or subsequently authorized by the individual.
See, Safe Harbour, *supra* note 246, ANNEX I, Data Integrity.

[266] See, DPD, *supra* note 1, art. 6.

The Access Principle enables data subjects to access their data to "correct, amend, or delete" where their data is inaccurate[267].

3.2.2. The Enforcement of the Safe Harbour

According to the provisions of the Safe Harbour related to the enforcement, there must be independent recourse mechanisms to handle the complaints and disputes, and award compensations in case of violation of the data protection rights of individuals[268]. In relation to the compliance, the attestations and assertions of the organizations must be assessed[269]. Sanctions are used to secure the compliance with the principles[270].

The Annex VII provides that The Federal Trade Commission and The US Department of Transportation are the authorized governmental bodies to "investigate complaints and obtain relief against unfair or deceptive practices[271]."

3.2.3 Legal Remedies in the Safe Harbour

Under the Frequently Asked Questions (hereafter the FAQs) Section of the Safe Harbour, the FAQ No 11 describes the independent recourse mechanisms[272]. According to that, these mechanisms might be in any form as soon as they meet the Enforcement Principle's requirements[273].

Under the section Recourse Mechanisms, organizations must provide individuals information regarding the application to the recourse mechanisms[274]. Furthermore, the recourse mechanisms must be independent, "readily available and affordable[275]". According to the section Remedies and Sanctions, the dispute resolution body provides remedy "reversing the effects of non-compliance[276]".

---

[267] Safe Harbour, *supra* note 246, ANNEX I, Access.
[268] Id. ANNEX I, Enforcement.
[269] Ibid.
[270] Ibid.
[271] Id. ANNEX VII,
[272] Id. ANNEX II, FAQ No 11.
[273] Ibid.
[274] Ibid.
[275] Ibid.
[276] Ibid.

3.2.4 The Certification Mechanism for the Safe Harbour

Under the FAQ 6 of the Safe Harbour, the self-certification process is explained[277]. According to that, a corporate officer of the organization must sign a letter including:

i. the contact information of the organization,
ii. the activities on the personal data transferred from the Union,
iii. the privacy policy of the organization[278].

As the corporate officer of the organization signs that letter, the organization is immediately recognized as a certified organization under the Safe Harbour[279].

3.2.5. Exemptions to the Safe Harbour

The Annex I of the Safe Harbour provides limitations for the application of the Principles[280]. In that regard, "national security, public interest, or law enforcement requirements" might limit the application of the Safe Harbour[281]. Furthermore, "statute, government regulation, or case law" might also limit the application of the Safe Harbour[282].

3.3. THE COMMISSION ADEQUACY DECISION

On 26 July 2000, the European Commission, relying on the DPD, particularly the Article 25, in the scope of the Safe Harbor, declared that data protection level of the U.S. is adequate[283].

[277] Id. ANNEX II, FAQ 6.
[278] Ibid.
[279] Ibid.
[280] Id. ANNEX I.
[281] Ibid.
[282] Ibid.
[283] Id. art. 1.

3.4. THE CJEU DECISION THAT MADE THE SAFE HARBOUR INVALID

3.4.1. The Legal Status of the CJEU

The CJEU, established in 1952, is an organ of the EU, which interprets EU law to assure that all of the member countries apply the Union law in harmony[284]. Among other things, the CJEU settles legal disputes between the EU members and EU institutions[285]. Moreover it protects the rights of individuals and organizations against infringements by the EU institutions, and EU members[286].

There are five main functions of the CJEU: when a national court is in doubt regarding the application of EU law, the CJEU can provide clarification; when a national government fails to comply with EU law, CJEU can identify the non-compliance, and can penalize that government; when an EU Act violates an EU Treaty, or a fundamental right, the Court has the authority to invalidate the act; when EU governments and other EU institutions lodge a complaint with the Court on the grounds that the Parliament, Council or Commission does not function as intended under the EU law, the Court takes on to solve the issue; when an individual or a company is harmed by the action or inaction of an EU institution or EU staff, the Court can decide to compensate the damages[287].

3.4.2. Reasoning and the Implications of the CJEU Decision that made the Safe Harbour Invalid

As stated earlier, the Safe Harbour Decision was declared invalid by the CJEU on 6 October 2015, as Maximillian Schrems, a EU citizen, lodged a complaint with the Data Protection Authority of Ireland, regarding the intelligence activities of the US government[288].

---

[284] Handbook on European Data Protection Law, *supra* note 116, at 17-18.

[285] EUROPA - COURT OF JUSTICE OF THE EUROPEAN UNION (2014), Https://Europa.Eu/European-Union/About-Eu/Institutions-Bodies/Court-Justice_En (Last Visited Dec 18, 2017).

[286] Ibid.

[287] Ibid.

For the functions of the CJEU see also, TFEU, *supra* note 7, art. 17.

[288] SHARA MONTELEONE & LAURA PUCCIO, FROM SAFE HARBOUR TO PRIVACY SHIELD, 6 (2017).

Referring to the Safe Harbor Decision, the Irish authority rejected the complaint[289]. Thereupon, the case was brought before the High Court of Ireland, and the Court preferred to have opinion of the the Court of Justice whether it is possible for the national authorities to investigate the data protection level provided by a third country despite the presence of an adequacy decision[290]. The Court of the Justice ruled that the existence of an adequacy decision does not prevent the national authorities from investigating the level of protection[291].

Not limited with the issue of investigation of the adequacy of data protection of third countries by the national authorities, the Court evaluated the Safe Harbour Decision comprehensively[292]. According to the Court, the Commission is obliged to assess the domestic law and international commitments of the country in question to find that the third country provides "essentially equivalent" level of protection in relation to the EU Law[293].

The Court finds that the Commission merely examined the safe harbor scheme, and did not evaluate the required elements of the U.S. Law[294]. The Safe Harbor is only applicable to the United States undertakings, not to the public authorities[295]. Therefore, The Court found that the data protection and privacy legislations and practices of the U.S. do not provide effective safeguards to protect personal data against arbitrary interference of the public authorities[296]. The Court also finds that the Safe Harbor does not provide the legal remedies to individuals to access the personal data, have the data rectified, and erased[297]. Thus the Safe Harbour violates the right to effective judicial protection[298]. The rule of law mandates the presence of this possibility[299].

---

[289] Maximillian Schrems, *supra* note 102, para. 29.
[290] Id. at para. 36.
[291] Id. at art. 1.
[292] Id. at para. 79-106.
[293] Id. at para. 96.
[294] Id. at para. 97.
[295] Id. at para. 89.
[296] Id. at para. 93.
[297] Id. at para. 95.
[298] CFEU, *supra* note 6, art. 7.
See also, Kuner, supra note 252, at 891.
[299] See, Burri & Schär, *supra* note 250, at 496.

The decision of the CJEU is significant in the sense that the Court empowered the national supervisory authorities to evaluate the adequacy of a third country, even if there is a Commission Decision manifesting that the third country has an adequate level of protection[300]. Consequently, the third countries pursuant to the DPD should provide robust Data Protection mechanisms eliminating the infringements to the rights of the data subjects to provide legal stability for the data transfers from the Union.

The decision of the CJEU is noteworthy in terms of its reasoning. The term adequate protection is redefined by the Court: "the third country ... to ensure, by reason of its domestic law or its international commitments, a level of protection... essentially equivalent to that... of the EU provided by the DPD and the Charter[301]." By that account, pursuant to the Schrems Decision, to determine whether the data protection level of a third country is adequate, Commission should examine:

i. "the applicable rules in that country resulting from its domestic law or international commitments and,

ii. the practice designed to ensure compliance with those rules[302]..."

However, the Schrems Case showed that, interference for the purposes of "national security, public interest, or law enforcement" are not subject to limitations by the Safe Harbour[303]. The public authorities interfering for those purposes may disregard the Safe Harbour completely, even if the interference will result in adverse consequences, such as infringement to the right to privacy, or right to data protection[304]. Besides, the CJEU finds that the Commission in the Safe Harbour Decision does not evaluate any safeguards in the U.S., which protect the fundamental rights against interference of the public authorities[305].

---

[300] Maximillian Schrems, *supra* note 102, at art. 1.
[301] Id. para. 96.
[302] Id. para. 75.
[303] See, Id. para. 87.
[304] Ibid.
[305] Id. para. 88.

To provide evidence for the lack of safeguards in the U.S. Law, the Court refers to the Commission's own assessment COM(2013) 846[306]: the Commission finds that "the United States authorities were able to access the personal data transferred from the Member States to the United States and process it in a way incompatible, in particular, with the purposes for which it was transferred, beyond what was strictly necessary and proportionate to the protection of national security[307]." The Commission further notes that, there are no effective redress mechanisms enabling the data subjects to access, rectify or erase their data[308]. The Court finds that the absence of effective recourse mechanisms for the data subjects infringes the fundamental right to effective judicial protection[309].

3.4.3 The Legal Status of Data Transfers from the EU to US in the Transition Period

As the Safe Harbor Decision was declared invalid by the CJEU, more than 4000 US companies had to use other tools to continue performing transfers from the EU[310]. To remove the legal uncertainty and guide the companies, which perform transatlantic data transfers, the WP29, a group of EU DPAs and the Commission prepared guiding publications[311]. In its statement on 16 October 2015, the Article 29 Working Party stated that the transfers performed under the Safe Harbor are unlawful after the invalidity decision[312]. Nonetheless, the

---

[306] Id. para. 90.
See also, EUROPEAN COMMISSION, COM(2013) 846: COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL ON THE FUNCTIONING OF THE SAFE HARBOUR FROM THE PERSPECTIVE OF EU CITIZENS AND COMPANIES ESTABLISHED IN THE EU, (Nov. 27, 2013)
[307] Id. §7.1, §7.2 and §8.
[308] Maximillian Schrems, *supra* note 102, para. 90.
See also, Com(2013) 846, *supra* note 306, §7.2.
[309] Maximillian Schrems, *supra* note 102, para. 95.
[310] SAFE HARBOR DATA PRIVACY BRIEFING: YOUR QUESTIONS ANSWERED BY GIOVANNI BUTTARELLI | INSIGHTS | SIDLEY AUSTIN LLP, https://www.sidley.com/en/insights/events/2015/10/safe-harbor-briefing-your-questions-answered-10-20 (last visited Dec 19, 2017).
[311] MARTIN A WEISS & KRISTIN ARCHICK, U .S.-EU DATA PRIVACY : FROM SAFE HARBOR TO PRIVACY SHIELD, 12 (2016).
[312] *Press Release Issued by the Article 29 Data Protection Working Party*, (Oct. 6, 2015), http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2015/20151006_wp29_press_release_on_safe_harbor.pdf (last visited Dec 19, 2017).

organizations may utilize the Standard Contractual Clauses[313] and Binding Corporate Rules[314] (hereafter BCRs) to perform the transfers[315]. As an additional method, according to the Article 26(1) of the Directive, if the data subject had given his consent unambiguously for the transfer, transfers of data to the U.S. could take place[316].

3.5. EVALUATION OF THE SAFE HARBOUR AND THE INVALIDITY DECISION

The CJEU in its decision addresses both the deficiencies of the Safe Harbor and the formulation of the Safe Harbour Decision[317]. In this connection, the CJEU, to a great degree, communicated the insufficient aspects of the Safe Harbour that a new legal framework replacing the Safe Harbor should fix, and the points that the Commission should take into account formulating a new adequacy decision regarding that framework[318].

It is clear that the new legal framework replacing the Safe Harbour should, in essence, comply with the DPD and the Charter[319]. The new framework should provide that the interference of the public authorities to the transferred data should be limited, and subject to effective safeguards in the context of "national security, public interest, or law enforcement" purposes. The new framework should also provide effective recourse mechanisms for the data subjects to have legal dress in

---

[313] The Council and the European Parliament have given the Commission the power to formulate certain contractual clauses on the grounds of the Article 26 of the Directive. These clauses provide adequate safeguards on protection of privacy and the fundamental rights of the data subjects. The Commission has so far issued two sets of standard contractual clauses. See, MODEL CONTRACTS FOR THE TRANSFER OF PERSONAL DATA TO THIRD COUNTRIES - EUROPEAN COMMISSION, http://ec.europa.eu/justice/data-protection/international-transfers/transfer/index_en.htm (last visited Dec 19, 2017).

[314] Binding Corporate Rules are internal rules that frame the global data protection and privacy policy of a multinational group of companies. Following the approval, the BCR provides the authorisation by national data protection authorities. This way, the company is not obliged to sign standard contractual clauses for each transfer within the group. See, Ibid.

[315] Press Release of the WP29, *supra* note 312.

[316] ARTICLE 29 WORKING PARTY, WORKING DOCUMENT ON A COMMON INTERPRETATION OF ARTICLE 26(1) OF DIRECTIVE 95/46/EC OF 24 OCTOBER 1995, §2 (2005).

[317] Weiss & Archick, *supra* note 311, at 7.

[318] For criteria laid out by the CJEU, *supra* note 161, at 18.

[319] It is a conclusion drawn out of the Schrems Decision. For Schrems Decision see Maximillian Schrems, *supra* note 102.
See also, THE EUROPEAN DATA PROTECTION SUPERVISOR, OPINION 4/2016: OPINION ON THE EU-U.S. PRIVACY SHIELD DRAFT ADEQUACY DECISION, 3 (2016).

case that their rights are violated by the U.S. organizations. The Commission on the other hand, to eliminate the legal uncertainty in the future, should not only examine the applicable rules of the domestic law and international commitments of the U.S., but also include them in the pertinent adequacy decision to ensure that there are effective safeguards and effective recourse mechanisms for protecting the rights of data subjects.

SECTION 4

A NOVEL APPROACH TO DATA PROTECTION: THE GENERAL DATA PROTECTION REGULATION OF THE EU

4.1. INTRODUCTION

The General Data Protection Regulation (GDPR) will take effect on 25 May 2018[320]. It is not a Directive as in the case of the DPD, but a Regulation, which means that it will directly apply in the EU members without further domestic implementation[321]. Other than the procedures of implementation, directives and regulations serve similar purposes[322]. As the Commission puts, the new Regulation will increase the control of the individuals over their data and simplify the regulations for the organizations[323].

Primarily, the GDPR brings extra-territorial applicability, increased penalties for the infringements, a more clear language for the requests of consents and a simplified process for withdrawals of the consents[324]. Right of the data subjects are also improved by obliging the companies to notify the breaches to the

---

[320] See, Jan P. Albrecht, *How the GDPR Will Change the World*, 2 EUR. DATA PROT. LAW REV. 287–289 (2016), at 287.

[321] See, Bert-Jaap Koops & Ronald Leenes, *International Review of Law, Computers & Technology Privacy regulation cannot be hardcoded. A critical comment on the "privacy by design" provision in data-protection law Privacy regulation cannot be hardcoded. A critical comment on the 'privacy by de*, 28 INT. REV. LAW, COMPUT. TECHNOL. 159 (2017), at 163.

[322] Burri & Schär, *supra* note 250, at 489.

[323] PROTECTION OF PERSONAL DATA, http://ec.europa.eu/justice/data-protection/ (last visited Dec 19, 2017).

[324] KEY CHANGES WITH THE GENERAL DATA PROTECTION REGULATION, http://www.eugdpr.org/key-changes.html (last visited Nov 18, 2017).

data subjects, providing an electronic copy of the personal data to the data subjects moreover, data subjects will have the right to be forgotten[325]. What is more, data subjects will be able to transfer their data to other organizations of their choice (data portability), there will be higher standards in designing of systems and a simplified cooperation mechanism between the local DPAs and union institutions[326].

GDPR brings a good number of improvements and changes, which are out of the scope of this study. In that regard, the scope of the assessment under this section will be limited to the application of the GDPR to the Privacy Shield to identify what extent the framework complies with the new data protection regulations. As the Privacy Shield is based on the DPD, not the GDPR, it is expected that the framework will not completely comply to the Regulation as it is. However, since the Privacy Shield will be reviewed on an annual basis, there might be changes to the framework to provide an increased compliance in the future[327].

The main principles guaranteed in the GDPR are purpose limitation, data quality and proportionality, transparency, security, rights of access, rectification and opposition, data retention and restrictions on onward transfers[328]. Therefore, a comparative approach will be used presenting the changes in the principles. Other changes that might have an effect on the application of the Privacy Shield will also be examined.

---

[325] Ibid.
[326] Ibid.
[327] See, Burri & Schär, *supra* note 250, at 505.
See also, Kuner, *supra* note 252, at 903.
See also, ARTICLE 29 DATA PROTECTION WORKING PARTY, OPINION 01/2016 ON THE EU–U.S. PRIVACY SHIELD DRAFT ADEQUACY DECISION WORKING PARTY OPINIONS, 15 (2016), [hereinafter WP29 Opinion].
[328] Key Changes with the General Data Protection Regulation, supra note 324.

4.2. THE TERRITORIAL SCOPE OF THE GDPR

The Article 3 of the GDPR specifies the territorial scope of the Regulation[329]. The first paragraph of the Article provides that the territorial scope does not depend on the place of processing, as long as the controller or the processor is located in the Union, the Regulation is enforced on the personal data[330]. What's more, if the data subjects are in the Union, not depending on the location of the controller or the processor, the Regulation applies, if the personal data is collected for the activities of offering goods and services to, or monitoring[331] of behavior of data subjects[332]. As a result the territorial scope, and the number of organizations subject to the Regulation will be enormous[333].

A similar provision exists under the Article 4 of the DPD[334]. However, as can be inferred from the wording of the DPD, the territorial scope of the directive does not depend on the location of the data subjects, but that of the controllers[335]. DPD applies when the controller is established in the EU, or the international law dictates that the EU law applies where the controller is established[336]. Furthermore, under the DPD, the difference between data controllers and data processors is critical, since data controllers have limited obligations and responsibilities[337]. Yet,

---

[329] See, Ioanna Tourkochoriti, *The Transatlantic Flow Of Data And The National Security Exception In The European Data Privacy Regulation : In Search For Legal Protection Against Surveillance Europe Regulates Data Privacy Against Violations Coming From The Private Sector More Strictly,* U. Pa. J. Int'l L. 459 (2015), at 509.

[330] 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, O.J. (L 119/1) (2016), art. 3. [hereinafter GDPR].

[331] Monitoring of the data subjects can be done enabling data subjects create online accounts or profiles which can be monitored and tracked. See, Melissa Ryan, *Navigating Privacy In A Sea Of Change*, INTERN. AUDIT. 68–69 (2017), at 62.

[332] GDPR, *supra* note 330, art. 3.

[333] See, ELENI KOSTA, NADEZHDA PURTOVA & COLETTE CUJIPERS, DATA PROTECTION REFORM AND THE INTERNET : THE DRAFT DATA PROTECTION REGULATION TILBURG LAW SCHOOL LEGAL STUDIES RESEARCH PAPER SERIES, No:03/2014, at 3.

[334] See, DPD, *supra* note 1, art. 4.

[335] Kosta et al. *supra* note 333, at 2.

[336] Ibid.

[337] See, Burri & Schär, *supra* note 250, at 493.

GDPR changes that bringing about varying responsibilities for controllers and processors[338].

In terms of the territorial scope of the GDPR, the most significant part is that the Regulation will apply to U.S. organizations irrespective of their location and participation to the Privacy Shield, if they process personal data (originally collected to offer goods and services to, or monitor behavior of data subjects) of the data subjects who are located in the EU[339]. Thus, the GDPR leaves the controllers, which do not process personal data in those contexts, out of the scope[340]. In that regard, the Privacy Shield will still be the primary legislative instrument for those controllers[341].

4.3. THE KEY FEATURES OF THE GDPR IN COMPARISON WITH THE DPD

4.3.1. Article 5 Principles Relating to Processing

The GDPR introduces the principles relating to processing under the article 5[342], whereas the DPD has similar provisions under the Article 6[343]. The improvements under the first paragraph are the newly introduced "transparency[344]" and "integrity and confidentiality[345]" principles.

---

[338] Ibid.
Article 30(2) of the GDPR provides the requirements of the records that the processors should maintain, Article 31 provides the reuirements for the processors regarding cooperation with the supervisory authorities, Article 32(1) provides the obligations for the proessor in terms of the security of processing, Article 33 provides the notification requirements for the processors in tcase of data breach, Article 79 provides the right to have remedy against the processor, Article 82 provides right to have compensation from the processors. See, GDPR, *supra* note 330, art. 30(2), 31, 32(1), 33, 79, 82.

[339] Leena Salolatva, *Privacy Shield Redress Mechanisms Assessment in the Light of the Schrems Case*, 2017.
See, Tourkochoriti, *supra* note 329, at 496.
See also, WHO DOES THE EU GDPR APPLY TO?, https://www.varonis.com/learn/who-does-gdpr-apply-to/ (last visited Nov 18, 2017).

[340] Michael Colesky, Sepideh Ghanavati Digital, *Privacy shielding by design - A strategies case for near-compliance*, *in* PROCEEDINGS - 2016 IEEE 24TH INTERNATIONAL REQUIREMENTS ENGINEERING CONFERENCE WORKSHOPS, REW 2016 271–275 (2017), at 273.

[341] Ibid.

[342] GDPR, *supra* note 330, art. 5.

[343] DPD, *supra* note 1, art. 6.

[344] GDPR, *supra* note 330, art. 12.

[345] Id. art. 25 and 32.

For the principles of fairness, lawfulness, purpose limitation, data minimization, accuracy, storage limitation and accountability principles[346], there is no significant change to the DPD[347].

4.3.2. Article 7 Conditions for Consent

Where the DPD has provisions related to the consent in the Article 7 "Criteria for Making Data Processing Legitimate" and in the Article 8 "The Processing of Special Categories of Data", the GDPR has a specific article which sets forth the provisions regarding the conditions for consent[348]. The Article 7 of the GDPR sets forth that consent should be clearly distinguishable from the other matters[349], the data subject should have a right to withdraw his consent any time[350], in the assessment whether the consent is given freely, the most important factor is the necessity of the collection of the personal data[351].

4.3.3. Article 8 Conditions Applicable to Child's Consent In Relation to Information Society Services

The GDPR provides that for the consent of a child to be lawful, there are additional conditions to the consent in the context of information society services[352]. Information society services, as defined by the Article 1 of the Directive on electronic commerce, any charged service that is offered at a distance by electronic means requiring transfer of data[353]. The Article 8 of the GDPR dictates that the consent of the child in relation to information society services is lawful, if the child is at least 16 years old, though EU members can lower this

---

[346] Id. art. 5.
[347] Ryan, *supra* note 331, at 61.
[348] See, Burri & Schär, *supra* note 250, at 492.
[349] GDPR, *supra* note 330, art. 7(2).
[350] Id. art. 7(3).
[351] Id. art. 7(4).
[352] GDPR, *supra* note 330, art. 8.
[353] Directive 2000/31/EC of The European Parliament and of the Council of 8 June 2000 on Certain Legal Aspects of Information Society Services, in Particular Electronic Commerce, in The Internal Market (Directive on electronic commerce), O.J. (L 178/1) (2000), art. 1.

limit to 13 years[354]. If the child is below that limit, the service provider should obtain consent from the responsible parent[355].

4.3.4. Article 9 Processing of Special Categories of Personal Data

There are several changes under the Article 9 of the GDPR. Firstly, processing of genetic data, and biometric data is recognized as processing of special categories of data[356]. Secondly, new conditions are provided for the EU members to lawfully process the special categories of data for reasons of public interest such as in the area of public health, and for archiving purposes[357].

4.3.5. Section 2 Information and Access to Personal Data

The Article 12 of the GDPR dictates that the for the exercise of the rights related to the data protection, information and communication should be "concise, transparent, intelligible and easily accessible[358]." The language used should be clear and plain[359]. If the data is collected from the children, the language should be further simplified[360]. The information should be provided in a written form, and in electronic form where possible[361]. Article 13, 14 and 15 provides that the data subject must be able to obtain confirmation and communication (where applicable) to identify the controller, the contact details of the data protection officer, the purposes of processing, legal grounds of the processing, the recipients, the legal grounds of the transfer, the period of the storage of the data, the rights of the data subject, the existence of automated-decision making[362].

---

354 GDPR, *supra* note 330, art. 8(1).
355 Ibid.
356 Id. art. 9.
Medical data is considered as sensitive data by the DPD see, Handbook on European Data Protection Law, *supra* note 116, at 174.
Currently there are detailed provisions regarding the genetic data under the Rec(97)5 see, COUNCIL OF EUROPE, COMMITTEE OF MINISTERS, RECOMMENDATION REC(97)5 TO MEMBER STATES ON THE PROTECTION OF MEDICAL DATA (13 February 1997).
357 See, Burri & Schär, *supra* note 250, at 490.
358 GDPR, *supra* note 330, art. 12(1).
359 Ibid.
360 Ibid.
361 Ibid.
362 Id. art. 13, 14 and 15.

4.3.6. Article 17 Right to Erasure ('Right to be Forgotten')

The Article 17(1) of the GDPR provides that data subjects may have the data erased by withdrawing their consent, in case that there are no other legitimate grounds for the processing[363]. Before the GDPR, the right to be forgotten was not recognized by EU Regulations or Directives, instead the right was protected by the case law of the CJEU[364].

4.3.7. Article 20 Right to Data Portability

Right to data portability is introduced by the GDPR, and does not exist under the DPD[365]. According to the Article 20(1) and 20(2) of the GDPR, the data subject may move personal data from the controller and transfer it to a different controller of his choice if the processing is carried out based on his consent and the data is processed by automated means[366].

4.3.8. Article 21 *Right to Object*

If the controller cannot show compelling legal grounds, the data subject has right to object to the processing whenever wishes, even when the grounds of the processing are related to profiling, automated decision-making, direct marketing, scientific or historical research purposes or statistical purposes or in relation to the information society services[367].

---

[363] Id. art. 17.

[364] Deckelboim, *supra* note 57, at 271.
See, Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, Case C-131/12 (May 13, 2014, CJEU).

[365] Kosta et al. *supra* note 333, at 17.

[366] GDPR, *supra* note 330, art. 20(1) and 20(2).

[367] Id. art. 21.
For detailed information on profiling, see Boehm, *supra* note 17, at 40.

4.3.9. Article 25 and 32, "Data Protection by Design and by Default" and "Security of Personal Data"

Reading the Article 25 along with the Article 32, the controller and the processor determining the means of processing should take into account the risks related to the rights and freedoms, related modern technology and the cost of implementation, and take appropriate measures, whether it be technical or organizational[368]. The controller and the processor where applicable should:

i. utilize pseudonymization and encryption of personal data[369];
ii. ensure that the existing processing systems provide "integrity, availability and resilience[370];"
iii. ensure that in case of a physical or technical incident, the data can be restored expeditiously[371];
iv. perform regular testing, assessment, and evaluations of the security of the data[372];
v. eliminate the risks of "accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data transmitted, stored or otherwise processed[373]."
vi. ensure that natural persons working under instruction who have access to the data, do not process the data out of the instructions[374];
vii. by utilizing appropriate technical and organizational measures, ensure that processing is limited to what is necessary for each specific purpose and the data is not accessible by an indefinite number of persons[375].

[368] GDPR, *supra* note 330, art. 25 and 32.
[369] Id. art. 32(1)(a).
[370] Id. art. 32(1)(b).
[371] Id. art. 32(1)(c).
[372] Id. art. 32(1)(d).
[373] Id. art. 32(2).
[374] Id. art. 32(4).
[375] Id. art. 25(2).

4.3.10. Article 27 Representatives of Controllers or Processors not Established in the Union

A controller or a processor, which offers goods or services to, or monitors the behavior of the data subjects located in the EU, should have a representative in one of the Member Countries where its data subjects reside[376]. The representative is authorized by the controller or the processor related to all of the issues regarding the compliance to the Regulation[377].

4.3.11. Article 33 and Article 34 "Notification of a Personal Data Breach to the Supervisory Authority" and "Communication of a Personal Data Breach to the Subject"

Article 33 of the GDPR dictates that in case of a personal data breach, the controller should notice the supervisory authority within the 72 hours unless the personal data breach does not constitute a risk for the rights and freedoms[378]. According to the Article 34, if there are high-level risks to the rights and freedoms of the data subjects, the controller should notify the personal data breach to the data subject as well[379]. According to the Article 33, whenever the processor becomes aware of a personal data breach, it should notify the controller without delay[380].

[376] Id. art. 27(1).
[377] Id. art. 27(4).
[378] Id. art. 33(1).
[379] Id. art. 34(1).
[380] Id. art. 33(2).

4.3.12. Section 3 Data Protection Impact Assessment and Prior Consultation

Under the Article 34 and 36, the GDPR sets forth a new method to assess the risks of the processing of the personal data[381]. According to the Article 35(1), if a type of processing creates the impression that it will have a high level of risk to the rights and freedoms, the controller is obliged to carry out an impact assessment beforehand[382]. According to the Article 35(2), performing the impact assessment, the controller should take advice of the data protection officer[383]. The supervisory authority is responsible for determining the types of processing which are risky and which are not[384]. Furthermore, the authority must list them according to the Article 35(4) and 35(5)[385]. If the impact assessment indicates that the processing will have a high level of risk, the controller should consult the supervisory authority according to the Article 36(1)[386].

4.3.13. Section 4 Data Protection Officer

Article 37 of the GDPR dictates that the controller and the processor should have a data protection officer, if:

i. data are processed by a public authority[387],
ii. the core activities of the controller or the processor requires systematic and large scale monitoring of the data subjects[388] or,
iii. the processor requires large scale processing of the special categories of data[389].

More than one public authority or body may designate a single data protection officer[390]. The tasks of the data protection officer are to inform and

[381] See, Felix Bieker, *Enforcing data protection law - The role of the supervisory authorities in theory and practice*, 498 *in* IFIP ADVANCES IN INFORMATION AND COMMUNICATION TECHNOLOGY 125–139 (2016), at 133.
[382] GDPR, *supra* note 330, art. 35(1).
[383] Id. art. 35(2).
[384] Ibid.
[385] Id. art. 35(4) and 35(5).
[386] Id. art. 36(1).
[387] Id. art. 37(1)(a).
[388] Id. art. 37(1)(b).
[389] Id. art. 37(1)(c).

advise the controller or the processor regarding the compliance with the GDPR, to give advice related to the impact assessment, to cooperate with the supervisory authority and act as a point of contact on behalf of the supervisory authority[391].

4.3.14. Article 45 Transfers on the Basis of an Adequacy Decision

The GDPR provides grounds to an adequacy decision under the Article 45. On the other hand, DPD has similar provisions under the Article 25. According to the DPD, the Commission should take into account "all the circumstances surrounding" the transfer, the sectoral and general "rules of law", "the professional rules and security measures" and "the international commitments[392]".

The Article 45 of the GDPR, on the other hand, has more specific provisions[393]. In addition to the elements listed in the DPD, Commission should take into account:

i. The rule of law concerning "public security, defense, national security and criminal law and the access of public authorities to personal data and its implementation[394];"
ii. "Rules for the onward transfer[395];"
iii. "Case-law[396];"
iv. The existence of effective and enforceable data subject rights as well as effective administrative and judicial redress for data subjects[397];
v. "The existence and effective functioning of one or more independent supervisory authorities" with relevant enforcement and investigatory powers[398];

For the adequacy decisions that exist on the basis of DPD such as Privacy Shield adequacy decision, the GDPR has relevant provisions. They will be in

---

[390] Id. art. 37(3).
[391] Id. art. 39.
[392] DPD, *supra* note 1, art. 25.
[393] THE EUROPEAN DATA PROTECTION SUPERVISOR, OPINION 4/2016: OPINION ON THE EU-U.S. PRIVACY SHIELD DRAFT ADEQUACY DECISION, 6 (2016), [hereinafter EDPS].
[394] GDPR, *supra* note 330, art. 45(2)(a).
[395] Ibid.
[396] Ibid.
[397] Ibid.
[398] Id. art. 45(2)(b).

effect until the Commission finds that the third country in question provides, or no longer provides an adequate level, and decides to amend, replace or repeal those decisions[399].

4.3.15. Article 77 Right to Lodge a Complaint with a Supervisory Body

Article 77 dictates that every data subject should be able to to make a complaint before the supervisory authority, if they believe that their rights are infringed by means of processing their data[400]. The data subjects should be informed regarding the result of the complaint[401]. The same right is provided under the Article 28(4) of the DPD[402].

4.4. THE EVALUATION OF THE GDPR WITH REFERENCE TO THE DPD

The GDPR, compared to the DPD, is more demanding regarding the adequacy decisions[403], as the Article 45, from the third countries, demands:

i. one or more independent supervisory authorities[404],
ii. administrative and judicial redress for data subjects[405],
iii. effective safeguards for the access of public authorities to personal data for the necessities of public security, defense, national security and criminal law[406],
iv. Proper rules for the onward transfers[407].

The data protection authority of the US in relation to the rights and freedoms protected by the Safe Harbour was FTC[408]. This is also the case for the Privacy

---

399 Id. art. 45(5).
400 Id. art. 77(1).
401 Id. art. 77(2).
402 DPD, *supra* note 1, art. 28(4).
403 Bieker, *supra* note 381, at 136.
404 GDPR, *supra* note 330, art. 45(2)(b).
405 Id. art. 45(2)(a).
406 Ibid.
407 Ibid.
408 Safe Harbour, *supra* note 246, ANNEX III.
See, 15 U.S.C. §§41-58.

Shield[409]. As stated earlier, whether the FTC has adequate, investigatory, enforcement and monitoring powers is arguable, in particular because of the limitations to the jurisdiction of the FTC[410]. As the GDPR mandates a supervisory authority with specific powers for a country to provide an adequate level of protection, a further overview and analysis is necessary to be able to conclude whether the supervisory authorities in the US regarding data protection are adequate in relation to the Article 45(2)(b) of the GDPR[411].

According to the GDPR, to provide effective protection, a third country must provide administrative and judicial redress for the data subjects[412]. In that regard, the U.S. as a third country must provide those redress options. To be able to assert that the U.S. provides those options, an analysis of the U.S. Law is required.

According to the GDPR, the interference of the public authorities is another issue to consider in evaluation of level of adequacy of a third country[413]. Public security, defense, national security and criminal law are considered to be valid purposes for the public authorities to interfere the personal data[414]. In this connection, effective safeguards must be provided to prevent not necessary, or in proportionate interference[415]. The Commission is obliged to evaluate those safeguards in an adequacy decision[416]. Therefore, the pertinent safeguards in the U.S. Law will also be examined in this study.

Onward transfers are another issue to be considered related to an adequacy decision[417]. As there is a risk that the personal data can be transferred from a safe country[418] to non-safe countries[419], the rules for onward transfers in a country are

---

[409] Privacy Shield, *supra* note 42, ANNEX IV.
[410] See, Tourkochuriti, *supra* note 5, at 169.
[411] Article 45(2)(b) of the GDPR provides the elemensts of evaluation that the Commission should take into account in evaluation of the level of data protection of third countries for the adequacy decisions. See, GDPR, *supra* note 330, art. 45(2)(b).
[412] Id. art. 45(2)(a).
[413] Ibid.
[414] Ibid.
[415] Ibid.
[416] Ibid.
[417] Ibid.
[418] In this study, a safe country is a country, which is, by the virtue of a Commission Decision, considered to provide adequate level of data protection.
[419] In this study, a non-safe country is a country for which there is no Commission Decision showing that that country provides an adequate level of data protection.

other indicators of the data protection level. Therefore, the pertinent rules in the U.S. Law will also be examined in this study.

SECTION 5

THE EMERGENCE OF THE PRIVACY SHIELD

5.1. INTRODUCTION

Following the invalidity decision of the CJEU, a new political agreement has been reached to establish a new framework, the EU-U.S Privacy Shield[420]. To the Commission, the new framework guarantees an adequate level of protection for the EU individuals, protecting their fundamental rights[421]. In addition to that, the Commission stated that the new framework provided the legal stability for the European and American companies that work together[422]. The reason is that, the Privacy Shield was a sufficient reaction to the Commission's suggestions and the Schrem's Decision[423]. The Commission asserts that all of the neccessary elemensts for an adequacy decision was evaluated: the domestic law of the U.S. in practice; the international commitments of the certified U.S. companies; the interference of the U.S. public authorities to the transferred data[424].

The EU-U.S. Privacy Shield framework entered into the force by the Commission Implementing Decision on 12 July 2016[425]. As stated earlier, the authority of the Commission to find that a country out of the EU provides an adequate level of protection is based on the Article 25(6) of the DPD[426]. However, a Commission Adequacy Decision does not necessarily imply that a third country in question provides an adequate level of protection nor the privacy and data

[420] See, Privacy Shield, *supra* note 42.
[421] Id. art. 1(1).
[422] EUROPEAN COMMISSION, COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL TRANSATLANTIC DATA FLOWS: RESTORING TRUST THROUGH STRONG SAFEGUARDS, COM(2016) 117, 8 (Feb. 29, 2016).
[423] Id. at 8.
[424] Ibid.
[425] See, Privacy Shield, *supra* note 42.
[426] DPD, *supra* note 1, art. 25(6).

protection framework of the country in question is robust to the legal challenge as the Schrems case showed[427]. Thus, an analysis of the legal framework of a third country in question should not be limited to the Commission Adequacy Decision. However, the Commission Decision will provide a road map understanding the Privacy Shield.

As the CJEU formulated, the domestic law and international commitments of the country in question should be examined, then the level of protection of fundamental rights and freedoms within the scope of DPD and the Charter should be taken into account in such an evaluation[428]. In this connection, in this section, the Commission Adequacy Decision[429] will be examined to draw the road map for a further analysis of the Privacy Shield in the following sections.

5.2. THE ADEQUACY DECISION

The Privacy Shield is based on the Principles and Supplemental Principles[430] issued by the U.S. Department of Commerce[431] (hereafter the DoC). The Principles are designed to protect EU individuals whose personal data are transferred from the Union to U.S. organizations, which are self-certified to the Privacy Shield Framework[432]. The Principles issued by the DoC is in the Annex II of the Decision[433]. The following principles are of particular importance as they provide basis to Privacy Shield Decision. To evaluate the lawfulness of the Privacy Shield Decision, it is vital to understand the grounds of the Commission Decision. That's why this part of the study provides a mere summary of the Decision. The content of the Principles hereby provided reflects the point of view of the Commission. The Principles independent from the view of the Commission will be evaluated later on.

---

[427] Critics argue that the Commission Decision in Privacy Shield as well misleading. See, Vermeulen, *supra* note 40, at. 7.
See also, Bräutigam, *supra* note 38, at 164.
[428] Maximillian Schrems, *supra* note 102, art. 1.
[429] See, Ibid.
[430] Supplemental Principles replaced the Frequently Asked Questions of the Safe Harbor.
[431] Privacy Shield, *supra* note 42, ANNEX II.
[432] See, Surveillance by Intelligence Services, *supra* note 65, at 22.
[433] Privacy Shield, *supra* note 42, ANNEX II.

5.2.1. The Notice Principle as Stated by the Commission

The *Notice Principle* requires the organizations to inform the data subjects regarding the key elements of the processing, make privacy policies publicly available, provide links to the DoC's website that contains information related to the certification, Principles and the available recourse mechanisms, and a link to the website of an alternative dispute resolution provider[434].

5.2.2. The Choice Principle as Stated by the Commission

The *Choice Principle* provides to the data subject the right to object when the purpose is changed but still compatible with the original purpose[435]. The data subjects have the right to object anytime the use of personal data for direct marketing purposes; the data subject's affirmative express consent is needed[436].

5.2.3. The Rules for Onward Transfers as Stated by the Commission

There are special rules depending on the location of third party processor or controller regarding the *onward transfers*. The goal of these rules is to prevent the organizations from circumventing and undermining the Principles by transferring the personal data to third parties, which are not subject to the Principles[437]. The *Accountability for Onward Transfer Principle* restricts the onward transfers with (i) limited and specified purposes, (ii) the transfers should be on the basis of a contract, (iii) the contract should provide the same level of protection with the Principles[438]. Those accountability rules do not apply to the onward transfers in the presence of the national security, law enforcement and other public interest

[434] Id. recital 20.
See, Id. ANNEX II.II.1.
[435] Id. recital 22.
See, Id. ANNEX II.II.2.
[436] Id. recital 22.
See, Id. ANNEX II.II.2.
[437] Id. recital 27.
[438] Id. recital 28.

purposes[439]. The *Notice* and *Choice* Principles also do not apply in the presence of those purposes[440].

5.2.4. The Security Principle as Stated by the Commission

The *Security Principle* sets forth the requirements for the organizations to create, maintain, use or disseminate personal data under "reasonable and appropriate" security measures, evaluating all of the risks around the processing and the nature of the data[441]. If the sub-processor performs the processing, then the organization and the sub-processor should conclude a contract that ensures that the sub-processor also provides the level of the protection mandated by the Principles[442].

5.2.5. The Data Integrity and Purpose Limitation Principle as Stated by the Commission

The *Data Integrity and Purpose Limitation Principle* requires that the personal data should be limited to what is relevant for the purpose of processing, reliable for its intended use, accurate, complete and current[443]. This principle does not allow an organization to process personal data in a way that is incompatible with the purpose for which it was originally collected or subsequently authorized by the data subject[444]. Organizations are obliged to ensure that the personal data is reliable for its intended use, accurate, complete and current[445]. According to this Principle, the organization may process the personal information for longer periods of time if the processing is for archiving in the public interest, journalism, literature and art, scientific and historical research and statistical analysis.

---

[439] Ibid.
[440] Ibid.
See, Id. ANNEX II.II.3
[441] Id. recital 24.
[442] Ibid.
See, Id. ANNEX II.II.4.a.
[443] Id. recital 23.
[444] Ibid.
[445] Id. ANNEX II.II.5.b.

5.2.6. The Access Principle as Put by the Commission

The *Access Principle* enables the data subjects to demand confirmation whether the organization processes their data[446]. The organization is obliged to provide the information within a reasonable time, with a non-excessive fee, without obtaining the justification from the data subject[447]. The data subject has the right to contact the organization to correct, amend or delete personal information where it is inaccurate or has been processed in violation of the Principles[448]. In areas where it is commonly required automated processing, the Commission solely relies on the U.S. Law, which protects the data subjects against the adverse decisions[449]. The U.S. Law allows the data subjects to be informed by the reasons of the automated decisions, if the data subject believes that his data is inaccurate or incomplete, he can open a dispute to seek redress[450]. The lack of legislation regarding the automated decisions within the Privacy Shield requires additional monitoring; the Commission states that this issue will be elaborated in the first annual review[451].

5.2.7. The Recourse, Enforcement and Liability Principle as Stated by the Commission

The *Recourse, Enforcement and Liability Principle* sets forth the requirements for the companies to provide recourse mechanisms including effective remedies for the EU data subjects[452]. Effective and readily available independent recourse mechanisms that will deal with the complaints and disputes will be provided to the data subjects at no cost[453]. The organizations are free to choose any independent recourse mechanism; the location of the independent recourse body

---

[446] Id. recital 25.
See, Id. ANNEX II.II.6.a.
[447] Id. recital 25.
[448] Ibid.
[449] Ibid.
[450] Ibid.
[451] Ibid.
[452] Id. recital 26.
[453] Ibid.

can be either in the Union or in the United States[454]. The organizations can also cooperate with the European Union DPAs if they prefer[455]. Independent Alternative Dispute Resolution or private sector developed privacy programs are the other alternatives[456]. On the other hand, the individuals can lodge a complaint directly to the organization, to an independent dispute resolution body (hereafter IRM), which is chosen by the organization, to national DPAs or to the FTC[457]. If the individual is not satisfied by the resolution provided by one of those bodies, the individual has a right to demand from the Privacy Shield Panel to resolve the issue[458].

The Commission notes that, the Foreign Intelligence Surveillance Act provides recourse mechanisms for both the U.S. and the non-U.S. citizens[459]. If the individual believes that his personal data is subject to unlawful electronic surveillance, he has right to bring a civil cause of action, to sue U.S. government officials for the money damages[460]. Unlawful government access to, or use of personal data, including the national security purposes is also the causes of having recourse[461]

Even though certification is voluntary, once the company is certified, complying the principles is compulsory[462]. Moreover, the self-certification process should be repeated each year to continue to receive data from the EU within the Privacy Shield schema[463].

---

[454] Ibid.
[455] Ibid.
[456] Ibid.
[457] Ibid.
[458] Ibid.
See, Id. ANNEX II.II.7.
[459] Id. recital 112.
[460] Ibid.
[461] Ibid.
See, Id. ANNEX VI.V.
[462] Id. recital 26.
[463] See, Id. ANNEX II.I.6.

5.2.8. The Ombudsperson Mechanism as Evaluated by the Commission

By the letter signed by the Secretary of State and sent to the Commission, the U.S. government has undertaken the commitment to create a new mechanism called the Privacy Shield Ombudsperson[464]. Under-Secretary[465] functions as the Privacy Shield Ombudsperson, and this new oversight mechanism is independent from the Intelligence Community and is responsible from the oversight of the national security interference[466]. Regarding the interference with the law enforcement and other public interest purposes, the U.S. Department of Justice provided the related U.S legal framework to the Commission[467]. The Ombudsperson also ensures that individual complaints are addressed and the non-compliance is effectively remedied[468]. The Ombudsperson is able to accept complaints from the individuals, alternatively the individuals may prefer to lodge a complaint in the public authorities, the public authorities than channel the complaints to the Ombudsperson[469]. The individuals do not have to show evidence related to the unlawful processing of the data by the U.S. public authorities[470].

5.2.9. The Signal Intelligence Activities as Evaluated by the Commission

According to the Commission's evaluation, the president administers the foreign intelligence activities under the U.S. Constitution[471]. The Congress has the power to lay out the boundaries of those activities[472]. In the areas where there are no guidance by the Congress, those activities are administered by the Presidential

---

[464] Id. recital 65.
[465] Id. recital 116.
[466] Id. recital 65.
[467] Ibid.
See, Id. ANNEX VII.
[468] Id. recital 117.
[469] Ibid.
[470] Id. recital 119.
See, Id. ANNEX II.I.6
[471] Id. recital 68.
[472] Ibid.

Directives and and the Executive Orders[473]. The Legal Framework is mainly comprised of Executive Order 12333 and PPD-28[474].

The PPD-28 is evaluated to be legally binding on U.S. Intelligence Authorities[475]. The importance of the PPD-28 is in terms of its coverage. The non-US persons are also protected[476]. The important aspects of the PPD-28 is pointed out as following:

i. The collection of signal intelligence is dictated by the statute or the U.S. constitution[477].
ii. All persons irrespective of their nationalities deserve dignity and respect[478].
iii. Handling the data, all persons have legitimate privacy interests[479].
iv. The U.S. Signal Intelligence planning should be performed taking the privacy and civil liberties into account[480].
v. U.S. signal intelligence activities should provide appropriate safeguards to protect the data for all of the individuals[481].

According to the PPD-28, the signals intelligence can be performed merely for the foreign intelligence or counterintelligence purposes[482]. In this connection, the ODNI communicates that the Intelligence community agencies comply with the rule that "collection should be focused on specific foreign intelligence targets or topics through the use of discriminants (e.g. specific facilities, selection terms and identifiers)[483]."

The "National Intelligence Priorities Framework" (NIPF) ensures that high-level policy makers determine the selectors, and the selectors are regularly

[473] Ibid.
[474] Id. recital 68.
[475] Id. recital. 69.
[476] Id. recital 74.
[477] Id. recital 69(a).
[478] Id. recital 69(b).
[479] Id. recital 69(c).
[480] Id. recital 69(c).
[481] Id. recital 69(d).
[482] Id. recital 70.
[483] Ibid.

reviewed[484]. However, PPD-28 dictates that intelligence collection should always be done "as tailored as feasible[485]". The concerns of the Commission regarding that the feasibility criteria will result in mass and indiscriminate collection of data is eliminated by the ODNI[486]. The ODNI assures that the bulk collection will not be done "mass" or "indiscriminate[487]". However the PPD-28 dictates that in the absence of new and emerging threats, if the use of discriminants is not possible "due to technical and operational considerations" bulk collection might occur[488]. On the other hand, the ODNI ensured that even in that case the the collection will be narrowed down "as much as possible", filters and technical tools will be designed in a way to minimize the amount of "non-pertinent" information[489].

To limit the extent of the national security purposes, in the PPD-28 six national security purposes "espionage, terrorism, weapons of mass destruction, threats to cybersecurity, to the Armed Forces or military personnel, as well as transnational criminal threats related to the other five purposes" and only the signals that conform with these purposes will be collected[490]. And, the Community Elements "ensure that only those items believed to be of potential intelligence value are ever presented to analysts to examine[491]."

5.2.10. The Limitations and Safeguards for the Interference by the Public Authorities as Evaluated by the Commission

The Commission considers that since the targeted collection is prioritized, the bulk collection is limited with the technical and operational reason, and further use of the data is limited to specific national security purposes, the principles of necessity and proportionality are satisfied[492]. In that regard, the Commission states that the limitations on the interference by the U.S. public authorities is in parallel

[484] Ibid.
[485] Id. recital 71.
[486] Ibid.
[487] Ibid.
[488] Id. recital 72.
[489] Id. recital 73.
[490] Id. recital 74.
[491] Ibid.
[492] Id. recital 76.

with the standards set out by the CJEU in the Schrems judgment and the article 7 and 8 of the Charter[493].

Interference by the U.S. public authorities for law enforcement purposes are also in great interest of the Commission, and the Department of Justice ("DOJ") explained the applicable limitations and safeguards in its letter to the Commission[494] (Annex VII). According to the letter, the general principal for searches and seizures as dictated by the constitution is obtaining a court ordered warrant[495]. In some special cases however, the general principle does not apply. In any case, the *reasonableness* test is utilized and the need of legitimate governmental interests and individual's privacy interests are evaluated together[496].

For the law enforcement investigations in the State Level the same level or higher degrees of protections apply[497].

The protection provided by the constitution does not directly apply to the individuals other than the US residents by its nature, but indirectly protects the rights of those individuals, since there are additional requirements[498] for the law enforcement authorities to investigate the data held in the companies[499]. In case that individual believes the actions of the public authorities do not have legal basis in this context, there are judicial redress avenues in the U.S.[500].

5.2.11. The Commission's Overview of the Intelligence Community Elements

In the context of oversight of the policies and procedures of Intelligence Community Elements, the PPD-28 lays out the oversight mechanisms including civil liberties of privacy officers, Inspector Generals, the ODNI Civil Liberties and Privacy Office, the PCLOB, and the President's Intelligence Oversight

[493] Id. recital 90.
[494] Id. recital 65.
See, Id. ANNEX VII.
[495] Id. recital 126.
[496] Ibid.
[497] Id. recital 127.
[498] Judicial authorization or reasonabless test. See, Ibid.
[499] Ibid.
[500] Id. recital 130.

Board[501]. Civil liberties and privacy officers periodically report to Congress and the PCLOB regarding the complaints lodged to the agencies. They claim that they do not have the required level of independence[502].

Commission in the recital 97, communicates that each Intelligence Community has a special Inspector General, and the Inspector General within the ODNI has comprehensive jurisdiction over the entire Intelligence Community; the Inspector Generals are statutorily independent, and they act independently conducting audits and investigations, they have the authority to examine all records, reports, audits, reviews, documents, papers, recommendations or other relevant material and may take testimony. Furthermore, Commission considers that even though, the reports that the Inspector Generals issue are non-binding recommendations in nature, the reports and the follow-up actions are made public. Commission notes that The Privacy and Civil Liberties Oversight Board has access to all relevant agency records, reports, audits, reviews, documents, papers and recommendations, including classified information, conduct interviews and hear testimony.

The Board regularly issues reports to the Congressional Committees and the President, more importantly prepare a report assessing the implementation of the PPD-28[503]. The President appoints the Board Members, however the Board is independent. There is also the Intelligence Oversight Board, which is established under the President's Intelligence Advisory Board[504]. The Board evaluates the level of compliance of U.S. intelligence authorities to the Constitution and all applicable rules[505].

In addition to the oversight bodies, there are also mechanisms providing the compliance such as reporting requirements within the Intelligence Community Elements, oversight activities of the U.S. Congress directed by the National

[501] Id. recital 95.
[502] Id. recital 96.
[503] Id. recital 98.
[504] Id. recital 99.
[505] Ibid.

Security Act, the responsibility of the President to report any illegal intelligence activity directed by the National Security Act[506].

5.2.12. The Commission's Conclusion Regarding the Privacy Shield

Taking into account all those facts, the Commission in the scope of the Privacy Shield, finds that the data protection level of the U.S. is adequate and essentially equivalent to the protection ensured by the DPD and the Charter[507].

SECTION 6

EVALUATION OF THE COMMERCIAL ASPECTS OF THE PRIVACY SHIELD

6.1. INTRODUCTION

The Schrems Decision made it clear that the Safe Harbor had not been providing an adequate level of the protection in the context of Article 25 of the DPD[508]. This is the reason why the Privacy Shield is designed. As the Commission found that, in the scope of the Privacy Shield, the U.S. provides an adequate level of data protection, the Privacy Shield became a valid legal instrument providing supervision of data processing operations of the U.S. organizations[509].

However, the Commission's new decision finding that in the scope of the Privacy Shield, the data protection level in the U.S. is adequate will be scrutinized by the CJEU soon[510]. The previous decision of the CJEU regarding the Safe Harbour framework shows that Commission Decisions might conflict with the EU Law, and CJEU might rule that those decisions invalid[511]. Therefore, the

[506] Id. recital 102.
[507] Id. art. 1(1).
[508] See, See, Burri & Schär, *supra* note 250, at 487.
[509] See, Kuner, *supra* note 252, at 883.
[510] For the Cases Before the CJEU see, Digital Rights Ireland v. Commission, C. T-670/16, (2016, CJEU), and La Quadrature du Net and Others v. Commission, C. T-738/16, (2017, CJEU).
[511] See, Maximillian Schrems, *supra* note 102.

Commission Decision alone does not ensure that the Privacy Shield provides an adequate level of data protection in the context of the Article 25 of the DPD.

To identify the shortcomings of the Privacy Shield, comprehensively, if any, one needs to compare the provisions of the Privacy Shield with its previous version the Safe Harbour firstly. Secondly, since the adequacy decisions are based on the DPD and the CFEU, the relevant provisions of the DPD should also be considered in such an evaluation. Thirdly, the fact that the DPD will be obsolete soon, as the GDPR will take effect on 25 May 2018, a further evaluation taking into consideration the provisions of the GDPR could be useful[512]. Lastly, as a reference, the CJEU's findings in the Schrems Decision should also be included in that analysis.

To finalize the evaluation in this section, doctrinal legal analysis will be made. In that regard, relevant scholarly articles, books, documents and reports evaluating the Privacy Shield will be examined. In the conclusion part of this section, the results of the evaluation will be provided.

6.2.1. The Notice Principle

6.2.1.1. Improvements over the Safe Harbour Regarding the Notice Principle

Under *the Notice Principle*, there are a number of improvements. According to the updated Notice Principle, the organizations which are self-certified under the Privacy Shield should provide a link to, or the web address for the Privacy Shield List, information regarding the right to access to personal data, the name of the independent dispute resolution body, the name of the authorized statutory U.S. bodies that have investigatory and enforcement powers on the organization, the information regarding the right for binding arbitration, the requirements for disclosure of information to the public authorities on the basis of national security and law enforcement purposes, the liability of the organization pertaining to the onward transfers to the third parties[513].

[512] See, Jan P. Albrecht, *How the GDPR Will Change the World*, 2 EUR. DATA PROT. LAW REV. 287–289 (2016), at 287.
[513] Privacy Shield, *supra* note 42, ANNEX II.II.1.

6.2.1.2. Evaluation of the Notice Principle with Reference to the DPD and GDPR

Under the *Notice* principle: organization "should inform individuals about the purposes for which it collects and uses personal information about them[514]..." In that regard, the notification obligation of the organizations is limited with the cases where they collect and use personal data. The other forms of the processing are not covered which creates loopholes[515].

Article 2(b) of the DPD defines the processing as operation(s) performed on personal data such as "collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction[516]." The Notice Principle of the Privacy Shield does not cover recording, organization, storage, adaptation or alteration, retrieval, consultation, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction of the data[517].

The Article 4(2) of the GDPR provides a similar definition of the processing[518]. Therefore, the lacking elements in the definition of the processing of the Privacy Shield does not comply with the GDPR in a similar fashion.

In addition to that it is criticized that the Notice Principle does not cover the rights of the data subjects regarding the access, rectification or erasure of their data[519]. According to the WP29, Notice Principle should provide that the Privacy Shield organizations inform the data subjects regarding those rights[520].

Furthermore, it could be more reasonable if the notice was to be provided by the organizations the moment they receive the personal data, instead of the moment when the data is collected[521]. Because, the Privacy Shield organizations

---

514 Id. ANNEX II, II.1.a.iv
515 WP29 Opinion, *supra* note 327, at 13 n.10.
516 DPD, *supra* note 1, art. 2(b).
517 See, WP29 Opinion, *supra* note 327, at 13 n.10.
518 GDPR, supra note 42, art. 4(2).
519 WP29 Opinion, *supra* note 327, at 18-19.
520 Ibid.
521 Id. at 19.

in most of the cases do not directly collect the personal data, instead they receive the personal data from the EU organizations[522].

Another issue is the confusion regarding the autonomy of the processors. The notice, in the meaning of the Notice Principle, cannot be provided to the data subjects by the processors[523]. The reason is the Privacy Shield organizations, which act as processors do not determine the purposes of processing[524]. However, as DoC states, the Department does not differentiate the controllers and processors while registering the Privacy Shield certificates[525]. On this matter, as the WP29 puts, the U.S. authorities should issue additional guidelines to distinguish the obligations of the controllers and processors[526].

It is argued that under the Notice Principle, the fact that organizations should give notice to the data subjects regarding the listed overly detailed thirteen items will make it impossible for the organizations to comply with the obligation that the notice should be given in "clear and conspicuous language[527]." Simplifying the content of the Notice might eliminate that issue.

6.2.2. The Choice Principle

6.2.2.1. Improvements over the Safe Harbour Regarding the Notice Principle

There are no changes Under *the Choice Principle*[528].

6.2.2.2. Evaluation of the Choice Principle with Reference to the DPD and GDPR

The Choice Principle with regards to the sensitive data allows disclosure of the sensitive personal data to third parties, and use of the personal data for non-legitimate purposes[529], through the exercise of the opt-in choice[530].

See also, Schrems, *supra* note 41, at 148.
[522] Ibid.
[523] WP29, *supra* note 54, at 11.
[524] Id. at 11.
[525] Id. at 12.
[526] Ibid.
[527] Bräutigam, *supra* note 38, at 160.
[528] Privacy Shield, supra note 42, ANNEX II.II.2.

The Article 8(2) of the DPD provides that the special categories of data can only be processed under certain conditions[531]. Neither that article nor other articles of the DPD allows disclosure or use of personal data for non-legitimate purposes. The consent of the data subject (opt-in choice by the wording of the Privacy Shield) does not make non-legitimate purposes legitimate.

Under the Article 9(2) of the GDPR, there are similar provisions regarding the limitations on processing of the special categories of data[532]. In that regard, the GDPR also does not allow disclosure and use of the personal data for non-legitimate purposes even if the data subject has affirmative consent.

Furthermore, there is another issue under the Supplemental Principles, Sensitive Data. The conditions under which there is no need for an opt-in choice of the data subject to process the data for non-legitimate purposes[533]. That also conflicts with the EU Law, as it conflicts with the purpose limitation principle[534]. Bräutigam argues that the U.S. legal culture differs from that of the EU[535]. In the U.S., it is lawful to process personal data for materially different purposes without an affirmative consent[536]. Therefore, that issue regarding the Choice Principle is because of the influence of the U.S. legal culture. However, for the Privacy Shield to provide an adequate level of protection in the meaning of the Article 25 of the DPD, the provision allowing the processing for the non-legitimate purposes should be updated.

To overcome the issue resulting from the difference of legal cultures of two sides, additional guidance should be provided in the Choice Principle regarding the time and procedures of opt-out for materially different purposes[537].

---

[529] Legitimate purposes are the purposes which are compatible with the purposes for which the data was originally collected or subsequently authorized by the individual.
See, Weiss & Archick, *supra* note 311, at 5.
[530] Privacy Shield, *supra* note 42, ANNEX II.II.2.c.
See also, WP29 Opinion, *supra* note 327, at 24.
[531] DPD, *supra* note 1, art. 8(2).
[532] GDPR, *supra* note 42, art. 9(2).
[533] Privacy Shield, *supra* note 42, ANNEX III.I.a.
[534] WP29 Opinion, *supra* note 327, at 24.
[535] Bräutigam, *supra* note 38, at 159.
[536] Ibid.
See, Monteleone & Puccio, *supra* note 153, at 32.
[537] See, WP29 Opinion, *supra* note 327, at 8.

6.2.3. Accountability For Onward Transfer

6.2.3.1. Improvements over the Safe Harbour Regarding the Accountability For Onward Transfer

The name of the Principle of *the Onward Transfer* has been changed as *the Accountability For Onward Transfer* under the Privacy Shield[538]. With the Privacy shield, transfer of personal data to a third party acting as a controller, and to a third party acting as an agent are subject to different requirements[539]. To transfer personal data to a third party controller, the organization should conclude a contract with the third party controller subject to the Annex II.II.3 of the Privacy Shield[540].

It is argued that Accountability for Onward Transfers Principle is strongly improved over the Safe Harbor[541]. The reason is that, with the Privacy Shield, when the importer of the data and the third party receiver enter into a contract, they should include a clause, which provides the third party must notify the importer when the third party no longer meets the requirements of the Principles[542].

6.2.3.2. Evaluation of the Accountability For Onward Transfer with Reference to the DPD and GDPR

The Article 25 of the DPD dictates that the transfer to a third country can take place if "the third country in question ensures an adequate level of protection[543]." Furthermore, the Article 26 of the DPD provides derogations: if the country in question does not provide an adequate level of protection, the transfer can take place if the data subject gives consent to the transfer, for the interests of the data

---

[538] GDPR, *supra* note 42, ANNEX II.II.3.
[539] Ibid.
See, Bräutigam, *supra* note 38, at 160.
[540] Ibid.
See, Brennan et. al, *supra* note 161, at 23-24.
[541] Bräutigam, *supra* note 38, at 161.
[542] Ibid.
[543] DPD, *supra* note 1, art. 25(1).

subject, for the public interests, on the grounds of the authorization of a Member State which relies on the adequate safeguards affirmed by a controller[544].

As mentioned earlier, Privacy Shield, under *The Accountability for Onward Transfer* Principle, there are similar conditions for the transfer to take place to a third country: the organizations should enter into a contract which guarantees that the personal data will only be processed subject to the legitimate purposes and the recipient should provide the same level of protection with the Principles[545].

The application of the Principles however, is limited to national security, public interest and law enforcement requirements[546]. It might be inferred that the third country in question can provide the same level of protection with the Principles, even if it makes exceptions for the national security, public interest or law enforcement requirements.

Taking into account that Privacy Shield Principles do not provide any safeguards, or limitations for those exceptions[547] in the Annex II.I.5., the recipient country might also not provide any safeguards and limitations for those exceptions. Eventually, that may pose a risk for the personal data of the EU subjects.

As mentioned earlier, the Chapter V of the GDPR brings about more specific conditions for cross-border data transfers and adequacy decisions compared to the DPD[548]. For the Commission to find that a third country in question provides adequate level of data protection, the Article 45 of the GDPR provides a guideline[549]. However, there is no such guideline provided by the Privacy Shield. It is not clear how the evaluation will be made on the data protection level of a third country and how to find that a third country provides an adequate level of data protection. Moreover, there is lack of clearance in that area in the evaluation part of the Commission Decision[550].

---

[544] Id. art. 26.
[545] Privacy Shield, *supra* note 42, ANNEX III.I.a.
[546] Id. ANNEX II,I.5.
[547] EDPS, *supra* note 319, at 7-8.
[548] GDPR, *supra* note 330, §V.
[549] Id. art. 45.
[550] See, Privacy Shield, *supra* note 42.

Other than the evaluation of data protection level, the procedures of inspection for the contracts made according to the Principle of *Accountability for Onward Transfer* is not clear and not documented[551]. Those procedures should be documented to eliminate misconducts regarding the transfers made under that principle[552].

6.2.4. Security Principle

6.2.4.1. Improvements over the Safe Harbour Regarding the Security Principle

Under *the Security Principle*, there are no changes to the Safe Harbour[553].

It is argued that the Security Principle is inadequately worded[554]. As he puts, "reasonable and appropriate measures" are not specific enough[555]. He also mentions that the data loss is a very common issue and the cause is insufficient security measures most of the time[556].

6.2.4.2. Evaluation of the Security Principle with Reference to the DPD and GDPR

According to the Security Principle of the Privacy Shield: "Organizations creating, maintaining, using or disseminating personal information should take reasonable and appropriate measures to protect it from loss, misuse and unauthorized access, disclosure, alteration and destruction[557]..." The principle does not cover the other forms of processing which are listed under the definition

[551] WP29, *supra* note 54, at 10-11.
[552] See, Ibid.
[553] See, Privacy Shield, *supra* note 42, ANNEX II.II.4. and Safe Harbour, *supra* note 246, ANNEX I, Security.
See also, Brennan et. al, *supra* note 161, at 24.
[554] Bräutigam, *supra* note 38, at 161.
[555] Ibid.
[556] Ibid.
[557] Privacy Shield, *supra* note 42, ANNEX II.II.4.a.

of processing [558] collection, recording, organization, structuring, storage, adaptation, alteration, retrieval, consultation, alignment or combination, restriction, erasure or destruction[559]. In that connection, it can be argued that, an organization which does not take any measures in destruction of the personal data, will not be responsible for the damages resulted from the unauthorized access to data[560].

Besides, the Security Principle of the Privacy Shield does not have provisions related to the methods that the organizations should utilize such as pseudonymization, encryption, regular assessment of the data systems[561]. It can be argued that the the Security Principle under the Privacy Shield does not provide the same level of protection with that of provided by the Article 25 and 31 of the GDPR[562].

6.2.5. Data Integrity and Purpose Limitation Principle

6.2.5.1. Improvements over the Safe Harbour Regarding the Data Integrity and Purpose Limitation Principle

The name of *the Data Integrity Principle* has been changed under the Privacy Shield as *Data Integrity and Purpose Limitation Principle*[563]. The amendment to the principle provides that the information that is capable of identifying the individual can only be retained by the organization if the legitimate purposes of the processing require that[564]. However, for the purposes of archiving in the public interest, journalism, literature and art, scientific or historical research, and

---

[558] Article 2(b) of DPD and Article 4(2) of the GDPR gives the definition of processing as "any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction."

[559] See, WP29 Opinion, *supra* note 327, at 13 n.13.

[560] Unathorized access to personal data was one one of the reasons of the invalidation of the Safe Harbour. See, Haufbaer & Jung, *supra* note 152, at 1-2.

[561] See, Gerrit Hornung, *Regulating privacy enhancing technologies: seizing the opportunity of the future European Data Protection Framework*, 26 EUR. J. SOC. SCI. RES. 1351–16101 (2017), at 186-187.

[562] See, GDPR, *supra* note 330, art. 25 and 31.

[563] See Privacy Shield, *supra* note 42, ANNEX II.II.5 and Safe Harbour, *supra* note 246, ANNEX I, Data Integrity Principle.

[564] See Privacy Shield, *supra* note 42, ANNEX II.II.5.

statistical analysis, the organizations can retain the data for longer periods of time[565].

6.2.5.2. Evaluation of the Data Integrity and Purpose Limitation Principle with Reference to the DPD and GDPR

Article 6(c) of the DPD dictates that personal data should be "not excessive in relation to the purposes for which they are collected and/or further processed[566]..." Thereby, Article 6(c) of the DPD frames the proportionality principle[567]. The Privacy Shield, on the other hand, under the *Data Integrity and Purpose Limitation* principle, provides that personal information should be limited to the information that is relevant for the purposes of processing[568]." Clearly, the data relevant for the processing might be excess in relation to the purposes[569]. As a result, the essence of the proportionality principle does not exist in the Privacy Shield[570].

Article 5(c) of the GDPR sets forth a similar provision with the Article 6(c) of the DPD[571]. Therefore, the same arguments hold in the context of the GDPR.

Article 6(e) of the DPD dictates that personal data should be "kept in a form which permits identification of data subjects for no longer than is necessary" for the purposes for which the data were collected or for which they are further processed[572]." The article is of great importance in that the retention of the data is limited with the legitimate purposes, and when the purpose is already realized the data should be deleted. The case law of the CJEU also provides that retention must be limited to what is strictly necessary[573]. However, the Privacy Shield does not provide a similar safeguard for data retention[574]. The *Data Integrity and*

---

[565] Ibid.
[566] DPD, *supra* note 1, art. 6(c).
[567] See, Tourkochuriti, *supra* note 5, at 166.
[568] See, Privacy Shield, *supra* note 42, ANNEX II.II.5.a.
[569] WP29 Opinion, *supra* note 327, at 23.
[570] See, Ibid.
[571] GDPR, *supra* note 330, art. 5(c).
[572] DPD, *supra* note 1, art. 6(e).
[573] See, Digital Rights Ireland and Seitlinger and Others, Joined Cases C-293/12 and C-594/12 (CJEU, Apr. 8, 2014).
[574] WP29 Opinion, *supra* note 327, at 17.

Purpose Limitation Principle provides that the personal data may be retained as long as the data is "relevant for the purposes of processing[575]." In the footnote 1, the examples of compatible processing purposes are given as: "customer relations, compliance and legal considerations, auditing, security and fraud prevention, preserving or defending the organization's legal rights[576]." It can be argued that for an organization to ensure that it can defend its legal rights, it can retain the data as long as it wishes[577]. This, clearly do not comply with the provisions of the Article 6(e) of the DPD[578].

Article 5(e) of the GDPR sets forth a similar provision with the Article 6(e) of the DPD. Therefore, the same arguments hold in the context of the GDPR[579].

6.2.5.3. Further Analysis of the Data Integrity and Purpose Limitation Principle

It is argued that even though the data integrity and purpose limitation principles are written in parallel with the DPD, the footnote to those principles leave a room for the exploitation[580]. In some cases, IT companies need to process as much data as possible, and the Privacy Shield does not provide the sufficient limitations for those cases[581]. According to the footnote, compatible processing purposes are determined by expectations of a reasonable person[582].

As mentioned earlier, EU data protection law is based on an "opt-in" system. This is the case as well, in the context of purpose limitation[583]. However the U.S.

See, Bräutigam, *supra* note 38, at 65.
[575] WP29 Opinion, *supra* note 327, at 3.
See, Privacy Shield, *supra* note 42, ANNEX II.II.5.
[576] Privacy Shield, *supra* note 42. ANNEX II.II.5 n.1.
[577] WP29 Opinion, *supra* note 327, at 17.
[578] See, DPD, *supra* note 1, art. 6(e).
[579] GDPR, *supra* note 330, art. 5(e).
[580] Bräutigam, *supra* note 38, at 159.
[581] Ibid.
[582] Privacy Shield, *supra* note 42. ANNEX II.II.5 n.1.
[583] Francois Mestre, THE UGLY TRUTH BEHIND THE PRIVACY SHIELD, https://ciolawsdotcom.wordpress.com/2016/08/21/the-ugly-truth-behind-the-privacy-shield/ (last visited Dec 14, 2017).

has a different approach, which might be called as an "opt-out" system[584]. As a result of that EU companies seek affirmative consent of the data subjects for the processing operations regarding the marketing purposes, however it is the data subject's duty to state his will to "opt-out" in the U.S. system.[585]

6.2.6. Access Principle

6.2.6.1. Improvements over the Safe Harbour Regarding the Access Principle

Under *the Access Principle*, there are no changes.[586]

6.2.6.2. Evaluation of the Access Principle with Reference to the DPD and GDPR

Under the DPD, every data subject has right to access[587]. More specifically, the Article 12 of the DPD provides that every data subject has the right to be informed by the controller "whether or not data relating to him are being processed and information at least as to the purposes of the processing, the categories of data concerned, and the recipients or categories of recipients to whom the data are disclosed[588]..." Article 8(2) of the CFEU has a similar provision[589].

The Privacy Shield has a provision, which seems similar to that of the DPD[590]. The Access Principle provides that, "individuals should have access to personal information about them[591]..." However, a clear approach to right to access, as provided by the Directive does not exist[592]. Thus, one cannot infer under the Privacy Shield whether the individuals have the right to get informed on purposes

---

584 Ibid.
585 Ibid.
586 See Privacy Shield, *supra* note 42, ANNEX II.II.6 and Safe Harbour, *supra* note 246, ANNEX I, Access Principle.
See also, Brennan et al., *supra* note 161, at 24.
587 DPD, supra note 1, art. 12.
588 Ibid.
589 See, CFEU, *supra* note 6, art. 8(2).
590 Privacy Shield, *supra* note 42, ANNEX II, II.6.
591 Privacy Shield, *supra* note 42, ANNEX II, II.6.a and ANNEX II, III.8.a.i.
592 Monteleone & Puccio, *supra* note 153, at 11.

under which their data can be processed, to whom the data is disclosed or the categories of the data processed.

Furthermore, the right to access is limited by the exceptions set forth in the Supplemental Principles. These exceptions are:

i. "interference with the execution or enforcement of the law or with private causes of action, including the prevention, investigation or detection of offenses or the right to a fair trial;
ii. disclosure where the legitimate rights or important interests of others would be violated;
iii. breaching a legal or other professional privilege or obligation;
iv. prejudicing employee security investigations or grievance proceedings or in connection with employee succession planning and corporate re-organizations; or
v. prejudicing the confidentiality necessary in monitoring, inspection or regulatory functions connected with sound management, or in future or ongoing negotiations involving the organization[593]."

As the WP29 puts forward, the exceptions enumerated here are not balanced with the right to access[594]. The right to access is a fundamental part of the right of protection of data, and a prerequisite for the right of correction and erasure of the data[595]. It is noteworthy to mention that the exceptions set forth here to the right to access exceed the exemptions under the Article 13 of the DPD[596]. Therefore it can be concluded that the right to access is much narrower, and in connection with that, the right to have the data amended and erased is also narrower under the Privacy Shield and should be improved[597].

[593] Privacy Shield, *supra* note 42, ANNEX II, III.8.e.
[594] WP29 Opinion, *supra* note 327, at 26.
[595] Ibid.
See also, CFEU, *supra* note 6, art. 8(2).
[596] DPD, *supra* note 1, art. 13.
[597] EDPS, *supra* note 319, at 7.

6.2.6.3. Evaluation of the Automated Decisions in Relation with the Access Principle

In Schrems Decision, CJEU found that, the Safe Harbour does not provide safeguards providing sufficient guarantees against abuse in the context of automatic processing[598]. The processing by automated means however requires effective safeguards, as the risk of unlawful access to data is greater[599].

As underlined by the assessment of the Article 29 Working Party (WP29) earlier, automated decisions might have significant effects on the individuals[600]. To assess an individual in certain areas such as performance at work, creditworthiness, reliability and conduct, organizations use automated decision making methods[601]. According to the WP29, the Privacy Shield does not provide any legal guarantees in this area[602].

The Annual Joint Review of the Privacy Shield showed that none of the companies were using the automated decision methods[603]. However, WP29 notes that this might not reflect the reality[604]. And, there must be additional rules and limitaitons in that area[605].

The fact that automated decision-making methods are utilized by the companies in a growing fashion makes the matter critical[606]. The data subjects do not have any recourse, even though the automated decisions have the potential to negatively affect the individuals for instance depriving individuals from certain rights by blacklisting practices[607]. The WP29 asserts that individuals should have the right to know the logic behind the processing or request reconsideration. Even

---

598 Maximillian Schrems, *supra* note 102, at art. 1.
599 See, Digital Rights Ireland, *supra* note 573, para. 54-55.
600 WP29 Opinion, *supra* note 327, at 17-18.
601 For the automated decision methods used in the U.S. see, Monteleone & Puccio, *supra* note 153, at 24.
602 WP 29 Opinion, *supra* note 327, at 17-18.
603 WP29, *supra* note 54, at 12.
604 Ibid.
605 Ibid.
606 WP 29 Opinion, *supra* note 327. at 18.
607 Ibid.

though, the assessment of the WP29 was published before the final draft of the Privacy Shield, the necessary improvements are not made to the framework[608].

Regarding the automated processing of data, an update to the Privacy Shield should be made to provide that there are effective measures to prevent abuse of the personal data[609].

6.2.7. Recourse, Enforcement and Liability Principle

6.2.7.1. Improvements over the Safe Harbour Regarding the Recourse, Enforcement and Liability Principle

The name of *the Enforcement Principle* has been changed as *Recourse, enforcement and liability*[610]. With the Privacy Shield, new requirements are provided for the independent recourse mechanisms, which should resolve the issues expeditiously at no cost to the individual[611]. Unlike in the Safe Harbor, in the context of investigation and resolution of complaints, the Privacy Shield dictates that the organizations and independent recourse mechanisms should promptly respond to the Department, the EU members through the Department, if an organization have chosen to interact with DPAs, and then it should promptly respond to the DPAs[612]. If an individual invokes binding arbitration, the organization should arbitrate the claims[613].

There is also a new provision related to the onward transfers[614]. An organization is responsible, if its agent processes the personal data in a way inconsistent with the Principles, however the organization may avoid that

---

[608] Ibid.
[609] EDPS, *supra* note 319, at 9.
[610] See Privacy Shield, *supra* note 42, ANNEX II.II.7 and Safe Harbour, *supra* note 246, ANNEX I, Enforcement Principle.
[611] Privacy Shield, *supra* note 42, ANNEX II.II.7.
See, Brennan et. al, *supra* note 161, at 61.
[612] Privacy Shield, *supra* note 42, ANNEX II.II.7.
See, Brennan et. al, *supra* note 161, at 61.
[613] Privacy Shield, *supra* note 42, ANNEX II.II.7.
See, Brennan et. al, *supra* note 161, at 61.
[614] WP29 Opinion, supra note 327, at 15.

responsibility proving that it is not responsible from the event, giving rise to the damage[615].

Organizations are obliged to submit any compliance or assessment reports in the presence of a court order, or an inquiry by the FTC[616]. The FTC undertakes the task of prioritizing the referrals of non-compliance from the Department, and EU data protection authorities[617].

It is argued that Privacy Shield provides a greater number of obligations for the controllers compared to the Safe Harbour[618]. The rules for the contracts controllers enter into are more detailed and more specific than the Article 17 of the DPD provides[619]. Under the Privacy Shield, controllers must provide a copy of the contract that they enter into with their agents[620]. Controllers will be liable in case that the rights of the data subjects are violated[621]. They cannot shift the burden of proof in a simple way, since they have to prove that they are not responsible for the event that gives rise to the damage[622].

For those reasons, it can be argued that the Recourse, Enforcement and Liability Principle provides notable improvements. However, the recourse and enforcement provided by the Privacy Shield will be elaborated in a more detailed way in the Section 8 of this study.

6.2.7.2. The Comparison of the Approaches to the Enforcement under the Privacy Shield and the Safe Harbor frameworks

6.2.7.2.1. The Privacy Enforcement provided by the FTC

The enforcement power of the United States Federal Trade Commission (FTC) is communicated under the ANNEX IV of the Commission Adequacy Decision of

615 Privacy Shield, *supra* note 42, ANNEX II.II.7.
616 Ibid.
617 Ibid.
618 Bräutigam, *supra* note 38, at 158.
619 Ibid.
620 Ibid.
621 Ibid.
622 Ibid.

the Privacy Shield[623]. Whereas the enforcement power of the FTC is gave an overview of under the ANNEX III of the Commission Adequacy Decision of the Safe Harbour[624]. The FTC is established as a civil enforcement authority, which is responsible for consumer protection and promotion of the commercial competition[625]. The primary source of the law for the FTC is the FTC Act, and the main function of the act is to prohibit the *unfair* and *deceptive* acts[626]. The FTC is authorized to protect information in the health, credit and other financial matters as well as children's online information[627]. However, commercial activities of the banks, airlines, the business of insurance and the common activities of telecommunication service providers and most of the non-profit organizations are out of the FTC's jurisdiction[628].

With the Privacy Shield Framework, the FTC committed to work in four areas to enforce the framework. These are enumerated as

i. "referral prioritization and investigations;
ii. addressing false or deceptive Privacy Shield membership claims;
iii. continued order monitoring; and
iv. enhanced engagement and enforcement cooperation with EU DPAs[629]."

The only difference here between the Safe Harbour and the Privacy Shield is that with the new framework, FTC commits to cooperate with the EU DPAs[630]. EU members were able to send referrals to the FTC within the Safe Harbour, however there were no provisions that enabled cooperation between EU DPAs and the FTC[631].

The Privacy Shield sets forth a number of ways that enables the cooperation between the EU DPAs and the FTC. The first is the annual review of the

---

[623] Privacy Shield, supra note 42, ANNEX IV.
[624] Id. ANNEX III.
[625] See, Brennan et. al, *supra* note 161, at 7.
See also, Weiss & Archick, *supra* note 311, at 6.
[626] See, 15 U.S.C. §§41-58.
[627] Ibid.
[628] The areas in which FTC does not have jurisdiction are provided by the FTC act, See, 15 U.S.C. § 57a(f)(3), 15 U.S.C. § 57a(f)(4), 15 U.S.C. § 45(a)(2).
[629] Privacy Shield, supra note 42, ANNEX III.
[630] WP29 Opinion, *supra* note 327, at 27.
[631] See, Bräutigam, *supra* note 38, at 161.
See also, Brennan et al., *supra* note 161, at 48.

Framework that requires the contribution of the U.S. Department of Commerce, the European Commission, the FTC, and article 29 Working Party Representatives[632].

According to the Privacy Shield, the DoC is committed to counduct ex officio compliance reviews. However, the annual review does not include any information regarding those reviews[633].

Nevertheless, there is no information regarding the procedures for monitoring of the activities of the Privacy Shield organizations by the FTC[634]. According to the WP29, FTC, DoC or DoT should utilize site visits, web searches as well as surveys to verify that the participating organizations comply with the Principles[635].

6.2.7.2.2. The Privacy Enforcement provided by the U.S. Department of Transportation

The Department of Transportation (the DOT) is authorized to protect the privacy of consumer information that is given to airlines and ticket agents[636]. The methods of enforcement and approaches to the enforcement by the DOT do not differ under the Safe Harbour and Privacy Shield Frameworks[637]. When a carrier or seller of air transportation company participates to the framework, the DOT can monitor the operations of that company and enforce adherence to the Principles[638]. If the company is not self-certified under the Privacy Shield, the DOT can take action, if the company engages in *unfair or deceptive practice or an unfair method of competition*[639].

On the other hand, the annual joint review of the Privacy Shield shows that DOT does not conduct any ex officio investigations on, check the

[632] Privacy Shield, supra note 42, ANNEX I.
[633] WP29, *supra* note 54, at 10.
[634] WP29, *supra* note 54, at 11.
[635] Ibid.
See, EDPS, *supra* note 319, at 10.
[636] 49 U.S.C. § 41712.
[637] See, Brennan et al., *supra* note 161, at 25.
[638] Privacy Shield, *supra* note 42, ANNEX V.
[639] Ibid.

self-certification statements or the privacy policies of the organizations, which are subject to the enforcement of the DOT[640]. According to the WP29, DOT, by ex-officio investigations, should verify that those organizations comply with the Privacy Shield Principles[641].

6.2.7.3. Identification of the Enhancements Provided by the EU-U.S. Privacy Shield In Relation to the Redress Mechanisms

6.2.7.3.1. Resolution within the Organization

Under the Supplemental Principle Dispute Resolution and Enforcement, the Privacy Shield dictates that before proceeding to the independent recourse mechanism, the data subjects should be encouraged lodge a complaint within the organization[642]. When the data subject lodges a complaint in an organization, the organization should respond in 45 days[643]. Even though, there the same dispute resolution mechanism existed under the Safe Harbor, the Privacy Shield added a limited time frame for the organizations to respond to the complaints[644].

6.2.7.3.2. Independent Recourse Mechanisms

The Recourse, Enforcement and Liability Principle Under the Privacy Shield Framework dictates that the participating organizations should provide an Independent Recourse Mechanism to promptly resolve the complaints of the individuals, and rectify damages[645]. The option to proceed to an Independent Recourse Mechanism should be provided to the data subjects free of charge[646]. It

---

[640] WP29, *supra* note 54, at 11.
[641] Ibid.
[642] Privacy Shield, supra note 42, ANNEX II.III.11.d.i.
See, Bräutigam, *supra* note 38, at 163.
[643] Privacy Shield, supra note 42, ANNEX II.III.11.d.i.
[644] Ibid.
See, Monteleone & Puccio, *supra* note 153, at 25.
[645] Privacy Shield, supra note 42, ANNEX II.III.11.d.
See, Monteleone & Puccio, *supra* note 153, at 25.
See also, Brennan et. al, *supra* note 161, at 25.
[646] Privacy Shield, supra note 42, ANNEX II.III.11.d.
See, Monteleone & Puccio, *supra* note 153, at 25.

is the responsibility of the recourse mechanisms to provide information to the individuals about how the dispute resolution mechanism works[647]. Concerning the independent recourse mechanisms the only significant improvement is that access to the independent recourse mechanisms is now free of charge[648].

6.2.7.3.3. Lodging a Complaint Through Data Protection Authority

Under the Privacy Shield, the self-certified organizations which process Human Recources Data, or which commit to cooperate with the EU DPAs receive complaints directly from the EU DPAs[649].

The Recourse, Enforcement and Liability Principle Under the Privacy Shield Framework dictates that the participating organizations should promptly respond to the complaints which are referred by the EU Member State Authorities[650]. In that connnection, whether the self-certified organization commits to cooperate with the EU DPAs or not, a European data subject can lodge a complaint in the EU DPAs[651]. Then, the DoC and FTC will be investigating to resolve the referral[652].

The Privacy Shield in this regard does not bring significant improvements, since under the Safe Harbour, the authorities in the EU members were able to send referrals of non-compliance to the FTC and the Department of Transportation[653].

---

[647] Privacy Shield, supra note 42, ANNEX II.III.11.d.
See, Monteleone & Puccio, *supra* note 153, at 25.
See also, Brennan et. al, *supra* note 161, at 25.
[648] Under the Safe Harbour Framework, access to the indepndent recourse mechanism was "affordable". See, Safe Harbour, supra note 246, ANNEX I, Enforcement.
[649] Privacy Shield, *supra* note 42, recitals 47-51.
See, Bräutigam, *supra* note 38, at 163.
See also, Monteleone & Puccio, *supra* note 153, at 11.
[650] Privacy Shield, *supra* note 42, ANNEX V.II.A.
[651] See, Brennan et al., *supra* note 161, at 25.
[652] Ibid.
[653] See, Safe Harbour, *supra* note 246, ANNEX I, Faq No 11.

6.2.7.3.4. Arbitration

The Arbitration Mechanism is set forth in the Annex I of the Privacy Shield Decision[654]. In case that the other redress options do not remedy the violations completely or partially, under this option the Privacy Shield Panel works as the arbitrator and provides individual-specific, non-monetary equitable relief to the individuals, for instance access, correction, deletion, or return of the data[655]. Under the Safe Harbour a similar binding arbitration mechanism did not exist[656].

6.2.7.3.5. Remedies Available Under the State Law

Without prejudice to the other remedies, a data subject can always seek legal redress in the U.S. courts[657].

6.2.7.3.6. Evaluation of the Legal Redress Options under the Privacy Shield

It is argued that the multilevel redress system provided by the Privacy Shield is too complex similar to the rest of the framework[658]. The structure of the Principles is in a form where there is "rule, exception to that rule and exception to the exception[659]." It is argued that it is overly difficult for the data subjects to figure out which of the recourse mechanisms are before the Privacy Shield Arbitration Panel[660].

The argument regarding the complexity of the legal redress system provided by the Privacy Shield coincides with the reality[661]. Because, there is neither a

---

[654] Privacy Shield, *supra* note 42, ANNEX I.
[655] Id. ANNEX I.
See, Bräutigam, *supra* note 38, at 164.
See also, Monteleone & Puccio, *supra* note 153, at 26.
[656] Hufbauer & Jung, *supra* note 152, at 2.
[657] Privacy Shield, *supra* note 42, recital 59.
[658] Bräutigam, *supra* note 38, at 158.
[659] Ibid.
[660] Ibid.
See, Monteleone & Puccio, *supra* note 153, at 18.
[661] See, WP29, *supra* note 54, at 8.

principle nor an official letter under the Privacy Shield, that explains the redress options in a comprehensive and simple way[662]. The reader has to assemble the information provided in the recitals, Annex II under the title "Available Remedies" along with the Principles[663] and Annex I[664] to have a complete picture of the redress mechanisms. Therefore, both the information provided by the Privacy Shield and the redress mechanisms by their characteristics are overly complex which results in ineffectiveness of the redress mechanisms[665].

It is also argued that, the new redress mechanisms and the already provided mechanisms under the Safe Harbour are not accessible and affordable[666]. The reason is that if the data subject believes that his right to data protection is violated, he has to lodge a complaint in the U.S. and in English[667].

Under the Privacy Shield, the EU subjects have the option to lodge a complaint in the EU DPAs in their home countries[668]. The EU DPAs then refer the complaints to the FTC or DoT[669]. However, if the data subjects need to seek legal redress in the U.S. courts, the complicated legal system of the U.S. along with the obligation to use English will create a significant burden[670].

6.2.7.4. Evaluation of the Supervisory Bodies in the U.S. with Reference to the Schrems Decision

In Schrems Decision, CJEU states that National supervisory authorities should have the power to examine any claim related to the unlawful processing of the data[671], and in parallel with the Article 25(6) of the DPD, there must be detection and supervision mechanisms to protect the fundamental rights of the

---

See also, Weiss & Archick, *supra* note 311, at 11.
See also, EDPS, *supra* note 319, at 11.
662 Id. at 9.
663 Recourse, Enforcement and Liability Principles.
664 Under the ANNEX I, there is information regarding the binding arbitration mechanism.
665 WP29 Opinion, *supra* note 327, at 3.
666 Mestre, supra note 583.
667 Ibid.
668 Privacy Shield, *supra* note 42, recital 52.
669 Ibid.
670 The U.S. legal system is evaluated to be too complex. See, WP29, *supra* note 54, at 3.
See also, WP29 Opinion, *supra* note 327, at 48.
671 Maximillian Schrems, *supra* note 102, para. 99.

data subjects[672]. As mentioned in this section, the relevant supervisory bodies in the U.S. are FTC and the DOT[673]. Since the findings of the CJEU regarding the detection and supervision mechanisms are relevant for the FTC and DOT. However, their investigatory and jurisdictory powers are limited to certain sectors[674]. The fact that jurisdiction of those authorities are limited causes confusion in identification of the supervision and detection mechanisms[675].

6.3. Evaluation of the Supplemental Principles Related to the Commercial Aspects of the Privacy Shield

In addition to the Principles, Supplemental Principles (SP) are also introduced by the Privacy Shield[676]. There were no supplemental principles in the Safe Harbour, instead there was an additional section called Frequently Asked Questions (FAQ)[677]. The provisions laid down by the FAQ and SP are similar, even though the way the provisions are organized differ to some extent[678].

6.3.1. Sensitive Data

6.3.1.1. Improvements over the Safe Harbour Regarding the Supplemental Principle "Sensitive Data"

The first principle under the Supplemental Principles is *Sensitive Data*; under the *Sensitive Data* there are no improvements[679].

---

[672] Id. para. 81.
[673] Privacy Shield, *supra* note 42, ANNEX II.I.4.
[674] The areas in which FTC does not have jurisdiction are provided by the FTC act, See, 15 U.S.C. § 57a(f)(3), 15 U.S.C. § 57a(f)(4), 15 U.S.C. § 45(a)(2).
The DOT has jurisdiction is limited to Airlines and Ticket Agents. See, 49 U.S.C. § 41712.
[675] See, WP29, *supra* note 54, at 26.
See also, WP29 Opinion, *supra* note 327, at 12.
[676] See, Privacy Shield, *supra* note 42, ANNEX II,III.
[677] See, Safe Harbour, *supra* note 246, ANNEX II.
[678] See, Bräutigam, *supra* note 38, at 146.
See also, Id. at 160.
[679] The content of the *Sensitive Data* is identical. See, Privacy Shield, *supra* note 42, ANNEX II.III.1.

6.3.2. Journalistic Exceptions

6.3.2.1. Improvements over the Safe Harbour Regarding the Supplemental Principle "Journalistic Exceptions"

The second principle under the Supplemental Principles is *Journalistic Exceptions*; under the *Journalistic Exceptions* there are no improvements[680].

6.3.3. Secondary Liability

6.3.3.1. Improvements over the Safe Harbour Regarding the Supplemental Principle "Secondary Liability"

The third principle under the Supplemental Principles is *Secondary Liability*; under the *Secondary Liability* there are no improvements[681].

6.3.4. Performing Due Diligence and Conducting Audits

6.3.4.1. Improvements over the Safe Harbour Regarding the Supplemental Principle "Performing Due Diligence and Conducting Audits"

The fourth principle under the Supplemental Principles is *Performing Due Diligence and Conducting Audits*; under *the Performing Due Diligence and Conducting Audits* there are no improvements[682].

6.3.5. The Role of the Data Protection Authorities

6.3.5.1. Improvements over the Safe Harbour Regarding the Supplemental Principle "The Role of the Data Protection Authorities"

The fifth principle under the Supplemental Principles is *the Role of the Data Protection Authorities*. Under this principle, a new provision is added related to

---

[680] The content of the *Journalistic Exceptions* is identical. See, Privacy Shield, supra note 42, ANNEX II.III.2.

[681] The content of the *Secondary Liability* is identical. See, Privacy Shield, supra note 42, ANNEX II.III.3.

[682] The content of the *Performing Due Diligence and Conducting Audits* is identical. See, Privacy Shield, supra note 42, ANNEX II.III.4.

the human resources data. If the Privacy Shield covers the human resources data transferred from the EU pertaining to the employment relationship, then the organization should cooperate with the DPAs. The same provision was laid down in the FAQ 9 under the Safe Harbour[683].

6.3.6. Self-Certification

6.3.6.1. Improvements over the Safe Harbour Regarding the Supplemental Principle "Self-Certification"

The sixth principle under the Supplemental Principles is Self-Certification; the first improvement is related to the control mechanism performed by the DoC. To benefit from the certification, the Department has to determine that the submission is complete and place the organization to the Privacy Shield List[684]. Under the FAQ 6 of the Safe Harbor schema however, the submission of the required documents to the Department was enough to benefit from the certification[685].

The second improvement is that, if the privacy policy of the organization is publicly available, the organization is obliged to provide a hyperlink to the Department's Privacy Shield website, along with the hyperlink of the website or complaint submission form of the independent recourse mechanism[686].

The third improvement is that, in a specified interim period, the organizations which transfer data to a third party are obliged to, according to *the Accountability for Onward Transfer Principle*, should apply the Notice and Choice Principle, and ensure that the third party agent provides the same level of protection as is required by the Principles[687].

---

[683] See, Safe Harbour, *supra* note 246, ANNEX II, FAQ 9 and Privacy Shield, *supra* note 42, ANNEX II.III.5.
[684] See, Bräutigam, *supra* note 38, at 162.
See also, WP29, *supra* note 54, at 12.
[685] See, Safe Harbour, *supra* note 246, ANNEX II, FAQ 6 and Privacy Shield, *supra* note 42, ANNEX II.III.6.
[686] Privacy Shield, *supra* note 42, ANNEX II.III.6.
See also, WP29, *supra* note 54, at 12.
[687] Privacy Shield, *supra* note 42, ANNEX II.III.6.

The fourth improvement is that if a self-certified organization withdraws from the Privacy Shield, the organization should return or delete all the data, which was formerly transferred within the Privacy Shield, or utilize other authorized tools to retain the data[688].

6.3.6.1. Evaluation of the Improvements Regarding the Supplemental Principle "Self-Certification" with reference to the Schrems Decision

In Schrems Decision, the CJEU found that establishment of effective detection and supervision mechanisms under self-certification system is necessary[689]. The Self-Certification principle provides improvements on this issue. Under the Safe Harbour, it was possible to self-certify without the confirmation of the DoC[690]. However, the new framework dictates that DoC should determine that the submission is complete, only then should place the organization on the Privacy Shield List[691]. The requirements for the submission include mentioning the specific statutory body which has the authority to hear any privacy related claims, that is FTC as declared in the annexes, providing an independent recourse mechanism and a privacy policy[692].

The participating organizations may also voluntarily choose to cooperate with the EU DPAs[693]. However, if the organization receives human resources information, it is an obligation for the company to cooperate with the DPAs[694]. If the company wishes to cooperate with the DPAs, that information should be added to the submission form, and will be subject to the evaluation of the Department of Commerce[695].

---

[688] Ibid.
See also, WP29 Opinion, *supra* note 327, at 29.
[689] Maximillian Schrems, *supra* note 102, para. 99.
[690] Safe Harbour, *supra* note 246, ANNEX II, FAQ 6.
[691] Privacy Shield, *supra* note 42, ANNEX II.III.6.
See also, WP29, *supra* note 54, at 12.
[692] Privacy Shield, *supra* note 42, ANNEX II.III.6.
[693] Ibid.
[694] Ibid.
[695] Ibid.

The Department of Commerce, in addition to the verification of the information submitted by the organizations, has the authority to remove an organization from the Privacy Shield List, if the Department finds that an organization is subject to the persistence failure to comply[696]. Besides that, the Department commits to administer follow up procedures when an organization is removed from the Privacy Shield List, or the organization chooses to withdraw from the framework[697]. In this case, the Department commits to send questionnaires to those organizations to clarify whether the organization will return, delete, or continue to apply the Principles to the retained personal data[698].

Additionally, the Department requests a contact point within the organization to continue to communicate with the organization[699]. Also, the Department, on an ongoing basis monitors certified along with the previously certified organizations to search for any false claims of participation[700]. If the Department finds that the organization has a false claim of participation, it can warn the organization, refer to the matter to the FTC, or Department of Commerce and pursue any kind of legal recourse[701].

To increase the effectiveness of the monitoring, the Department commits to establish a contact point for the cooperation with the EU DPAs[702]. DPAs are able to send referrals related to the false claims of participation through this contact point. The Department processes the complaint within 90 days[703]. At the end of each year the Department publishes a report analyzing those complaints[704].

In connection with the Schrems Case, the main issue regarding the certification mechanisms is that upon the certification effective mechanisms of enforcement should be exercised to ensure that the self-certified organizations in

[696] Ibid.
[697] Ibid.
[698] Ibid.
[699] Ibid.
[700] Ibid.
[701] Ibid.
[702] Ibid.
[703] Ibid.
[704] Ibid.

fact conduct the processing operations complying with the Principles[705]. That issue was not merely a result of the self-certification mechanism[706].

Another issue with the self-certification mechanism is that the organizations, before submitting the required information to the DoC, place information to their websites indicating that they are in the Privacy Shield List[707]. DoC may find that such an organization actually is not eligible for the Privacy Shield[708]. However, in that evaluation period, which might be as long as 45 days, data subjects are misinformed, and they might believe that such an organization is already certified[709]. To overcome that issue, the organizations should, in their websites, provide the information regarding the status of the certification[710]. If they are not yet found eligibile to be placed into the Privacy Shield List, they may indicate their status as passive[711].

6.3.7. Verification

6.3.7.1. Improvements over the Safe Harbour Regarding the Supplemental Principle "Verification"

The seventh principle under the Supplemental Principles is *Verification*, under this principle there are no improvements[712].

---

[705] Bräutigam, *supra* note 38, at 154.
Under the Safe Harbour, there were issues regarding the compliance with the Principles. Maximillian Schrems, *supra* note 102, para. 99.
[706] Monteleone & Puccio, *supra* note 153, at 9.
See also, Brennan et. al, *supra* note 161, at 20.
[707] WP29, *supra* note 54, at 12.
[708] To be eligible for the Privacy Shield certificate, the organizations should meet certain conditions. See, Privacy Shield, *supra* note 42, ANNEX II.III.6.
[709] Ibid.
[710] Ibid.
[711] Ibid.
[712] Id. ANNEX II.III.7.

6.3.8. Access

6.3.8.1. Improvements over the Safe Harbour Regarding the Supplemental Principle "Access"

The eighth principle under the Supplemental Principles is *Access*, under this principle the coverage of the principle is explained by the Privacy Shield in a more elaborate way. According to the Access Principle, the individuals have right to:

i. "obtain confirmation from the organization whether the organization is processing his or her personal data;

ii. to obtain the content of that data to verify its accuracy and lawfulness of the processing.

iii. have the data corrected amended, or deleted if the processing of the data violates the principles or the data is inaccurate[713]."

As the right to access to data along with the right to correct, ammend and delete the data is essential elements of the right to data protection[714], improvements in this area contribute to a higher level of data protection.

6.3.9. Human Resources Data

6.3.9.1. Improvements over the Safe Harbour Regarding the Supplemental Principle "Human Resources Data"

The ninth principle under the Supplemental Principles is *Human Resources Data*[715]. Under this principle, there are some improvements. Firstly, if an organization wishes to use personal data collected through the employment relationship, for the purposes that are not related to the employment, that usage should not be incompatible with the purposes for which the personal information

[713] Id. ANNEX II.III.8.
[714] See, CFEU, supra note 6, at art. 8.
See also, Guide the EU-U.S. Privacy Shield, at 11.
[715] Privacy Shield, *supra* note 42, ANNEX II.III.9.

has been collected or subsequently authorized by the individual[716]. Therefore, the Privacy Shield emphasizes the obligation to comply with *the Notice and Choice Principle* in the context of Human Resources Data[717]. However, the Notice and Choice Principle provides an exemption that allows diverging from the Principles, employment decisions are not covered[718]. That exemption is criticized by the WP29 as the exemption is too broad[719].

The second change is related to the occasional employment related operational needs, such as the booking of a flight, hotel room, or insurance coverage[720]. The Privacy Shield allows the organizations not to apply the Access Principle, or enter into a contract with the third party controller in such cases[721]. However, the existence of those exceptions is not understandable, and undermines the protection provided by the principle[722].

6.3.10. Obligatory Contracts for Onward Transfers

6.3.10.1. Improvements over the Safe Harbour Regarding the Supplemental Principle "Obligatory Contracts for Onward Transfers"

The tenth principle under the Supplemental Principles is *Obligatory Contracts for Onward Transfers*, under this principle there are some improvements[723]. Data Processors in the EU are always obliged to enter into a contract regardless of the location of the processor, and the participation of the processor to the Privacy Shield[724]. The Privacy Shield clarifies the purpose of the contract, by the contract the processor:

i) "acts only on instructions from the controller;

---

716 Ibid.
717 Ibid.
718 Id. ANNEX II.III.9.iv.
719 WP29 Opinion, *supra* note 327, at 31.
720 Ibid.
721 Ibid.
722 See, WP29 Opinion, *supra* note 327, at 31.
723 Privacy Shield, *supra* note 42, ANNEX II.III.10.
724 Ibid.

ii) provides appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alternation, unauthorized disclosure or access, and understands whether onward transfer is allowed; and

iii) taking into account the nature of the processing, assists the controller in responding to individuals exercising their rights under the Principles[725]."

The second improvement is related to the transfers between two controllers within a controlled group of corporations or entities[726]. According to the Privacy Shield, a contract is not needed in such transfers, however the self-certified organization remains responsible[727].

The third improvement is related to the transfers between the controllers in general[728]. According to the Privacy Shield, the third-party controller does not have to be in the Privacy Shield list nor provide an independent recourse mechanism to receive personal data from the Privacy Shield Organization[729]. However, it should provide the same level of protection as is available under the Privacy Shield, and provide an equivalent mechanism to an independent recourse mechanism[730].

6.3.11. Dispute Resolution and Enforcement

6.3.11.1. Improvements over the Safe Harbour Regarding the Supplemental Principle "Dispute Resolution and Enforcement"

The eleventh principle under the Supplemental Principles is Dispute Resolution and Enforcement, under this principle there are some improvements. The Privacy Shield dictates that the participating organizations and their independent recourse mechanisms should provide information whenever

[725] Ibid.
[726] Ibid.
[727] Ibid.
[728] Id. ANNEX II.III.10.b.
[729] Ibid.
[730] Ibid.

requested by the department[731]. The information should consist the grounds of the compliant as well as how the organization will rectify the problem[732].

Under the Recourse Mechanism section, the Privacy Shield dictates that organizations should respond to the data subject within the 45 days of the complaint[733]. The Privacy Shield also brings a number of obligations for the independent recourse mechanisms. The first obligation is providing the following information on their websites:

i. "information on or a link to the Privacy Shield Principles' requirements for independent recourse mechanisms;

ii. a link to the Department's Privacy Shield website;

iii. an explanation that their dispute resolution services under the Privacy Shield are free of charge to individuals;

iv. a description of how a Privacy Shield-related complaint can be filed;

v. the timeframe in which Privacy Shield-related complaints are processed; and

vi. a description of the range of potential remedies[734]."

The second obligation is related to the annual report[735]. In the annual reports published by the independent recourse mechanisms, this information should take place:

i. "the total number of Privacy Shield-related complaints received during the reporting year;

ii. the types of complaints received;

iii. dispute resolution quality measures, such as the length of time taken to process complaints; and

iv. the outcomes of the complaints received, notably the number and types of remedies or sanctions imposed[736]."

[731] Id. ANNEX II.III.11.
[732] Ibid.
[733] Ibid.
[734] Ibid.
[735] Ibid.
[736] Ibid.

The principle also sets forth the provisions related to the arbitration option. The arbitration option can only be utilized when a participating organization infringes its obligations within the framework, and the violation is fully or partially not remedied by the organization[737]. The arbitration mechanism is not an option to evaluate the adequacy of the Privacy Shield, and only for the individual specific non-monetary reliefs such as access, correction, deletion, or return of the data[738]. The arbitral decisions are enforced within the U.S. Law[739]. In addition to that, there is the judicial review option for the individuals[740].

Under the FTC Action section of the principle, the Privacy Shield sets forth the provisions regulating the commitments of the FTC[741]. The FTC has committed to review the referrals on non-compliance from the

i. "privacy self-regulatory organizations and other independent dispute resolution bodies;

ii. EU Member States; and

iii. the Department[742]."

As a side note, the Safe Harbor did not include the referrals from the independent dispute resolution bodies[743].

6.3.12. Choice - Timing of Opt Out

6.3.12.1. Improvements over the Safe Harbour Regarding the Supplemental Principle "Choice - Timing of Opt Out"

The twelfth principle under the Supplemental Principles is *Choice - Timing of Opt Out*, under this principle there are no improvements[744] (Annex II.III.12).

[737] Ibid.
[738] Ibid.
[739] Ibid.
[740] Ibid.
[741] Id. ANNEX II.III.11.f.
[742] Ibid.
[743] Safe Harbour, *supra* note 246, ANNEX II, FAQ No 11.
[744] Privacy Shield, *supra* note 42, ANNEX II.III.12.

6.3.13. Travel Information

6.3.13.1. Improvements over the Safe Harbour Regarding the Supplemental Principle "Travel Information"

The thirteenth principle under the Supplemental Principles is *Travel Information*, under this principle there are no improvements[745].

6.3.14. Pharmaceutical and Medical Products

6.3.14.1. Improvements over the Safe Harbour Regarding the Supplemental Principle "Pharmaceutical and Medical Products"

The fourteenth principle under the Supplemental Principles is *Pharmaceutical and Medical Products*, under this principle there are no improvements[746].

6.3.15. Public Record and Publicly Available Information

6.3.15.1. Improvements over the Safe Harbour Regarding the Supplemental Principle "Public Record and Publicly Available Information"

The fifteenth principle under the Supplemental Principles is *Public Record and Publicly Available Information*, under this principle there are improvements. The Privacy Shield clarifies that the obtaining personal data from the publicly available sources requires application of the Security, Data Integrity and Purpose Limitation, and Recourse, Enforcement and Liability principles[747]. If the information that is obtained from the publicly available sources does not contain other types of personal information, the Access Principle is not applied unless relevant jurisdiction does not require[748]. If the organization is in the business of

[745] Id. ANNEX II.III.13.
[746] Id. ANNEX II.III.14.
[747] Id. ANNEX II.III.15.
[748] Ibid.

selling publicly available information, the individuals should be able to access the data due to a customary fee determined by the company[749].

The Principle is criticized due to the fact that it provides exemptions for the Principles Notice, Choice, Access, and Accountability for Onward Transfers[750]. WP29 states that, whether the information is publicly available or not, the data belongs to the data subject, and such an exemption will cause a loss of control over the data for the data subjects[751]. Such an exception does not exist under the DPD[752].

6.4. CONCLUSION

To identify the shortcomings of the commercial aspects of the Privacy Shield, in this section, firstly, the provisions of the Privacy Shield was compared with its previous version the Safe Harbour. Secondly, the relevant provisions of the DPD and GDPR were taken into the consideration. Thirdly, as a reference, the CJEU's findings in the Schrems Decision were included in that analysis. The views of the scholars were examined to provide guidance to the analysis.

According to the analysis made in this section, in order to bring the data protection level provided by the Privacy Shield closer to that of EU, the U.S. authorities might consider the options below:

Under the *Notice* principle, the notification obligation of the organizations is limited with the cases where they collect and use personal data; the other forms[753] of processing can be added to cover all forms of processing in order to prevent confusion and misinterpretation. The content of the notice can be simplified in order to ensure that the language of the notice is genuinely clear and conspicuous. An update can be made providing guidelines that will distinguish the obligations of the controllers and processors.

---

[749] Ibid.
[750] Id. ANNEX II.III.15.b.
[751] WP29 Opinion, *supra* note 327, at 33.
[752] Weiss & Archick, *supra* note 311, at 2.
[753] Recording, organization, storage, adaptation or alteration, retrieval, consultation, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction of the data.

The *Choice Principle* can be updated to ensure that personal data are not processed for non-legitimate purposes. The provision that allows processing for non-legitimate purposes can be removed. An update to the Principle can provide the time and procedures of opt-out for materially different purposes.

Under *The Accountability for Onward Transfer* Principle, the cross-border data transfers from the U.S. constitute risks, since a third country does not have to provide safeguards or limitations against the interference for national security, public interest and law enforcement requirements. In addition to that, there are no guidelines for evaluation of third countries in terms of level of data protection. With an amendment to the Principle, a guideline for that evaluation can be provided and an obligation for third countries can be added to ensure that they provide aforementioned safeguards or limitations. The procedures of inspection of the contracts made under this principle should be well documented to avoid confusion.

Under the Security Principle, there are missing forms of processing. Moreover, there are no specific measures required. With an amendment to the Principle other forms[754] of processing can be added, and specific measures such as pseudonymization, encryption, regular assessment of the data systems can be integrated to the principle.

Under the *Data Integrity and Purpose Limitation* principle the notion "data relevant for the processing" does not limit the data the way the Article 6(c) of the DPD and the Article 5(c) of the GDPR does. Therefore, with an amendment to the Principle the notion "not excessive in relation to the purposes" can be used.

Moreover, the *Data Integrity and Purpose Limitation* principle allows data to be retained as long as the data is "relevant for the purposes of processing." Since, this notion does not limit the period as effective as the Article 6(e) of the DPD and Article 5(e) of the GDPR, the notion "for no longer than is necessary for the purposes…" can be used. The footnote limiting the time period of retention of data with the "expectations of a reasonable person" can be removed.

---

[754] Collection, recording, organization, structuring, storage, adaptation, alteration, retrieval, consultation, alignment or combination, restriction, erasure or destruction

Under the Access Principle, the right to access can be defined in a more clear way so that the data subjects will not be hesitant to requesting information on purposes under which their data can be processed, to whom the data is disclosed or the categories of the data processed. Exceptions to the Access Principle can be reduced or removed to broaden the right to access.

A paragraph can be added to the Access Principle regarding the Automated Decisions so that individuals will have the right to know the logic behind the processing or request reconsideration.

Since it is not clear how the FTC and DoT will conduct evaluations regarding the compliance of the self-certified organizations, additional information can be provided to ensure that compliance is periodically monitored.

Under the Supplemental Principles is *Public Record and Publicly Available Information,* the exemptions that cause the loss of control over data can be removed.

SECTION 7

EVALUATION OF THE ACCESS BY PUBLIC AUTHORITIES TO DATA TRANSFERRED UNDER THE PRIVACY SHIELD

7.1. INTRODUCTION

Under the Safe Harbor Decision, the legal framework of the U.S. regarding the interference by the public authorities was not evaluated[755]. As mentioned earlier, this is one of the reasons why CJEU declared Safe Harbour invalid[756]. Under the Privacy Shield however, the General Counsel from the Office of the Director of National Intelligence (hereafter ODNI) gave an overview of the legal framework regarding that issue, regarding the national security exception of the

[755] Maximillian Schrems, *supra* note 102, para. 93.
For other cases of CJEU related to the unlawful access to the data by the public authorities see, Digital Rights Ireland, *supra* note 573, para. 57-61.
[756] See Ibid.

Privacy Shield in his letter[757]. The information provided by the General Counsel is concentrated on the U.S. Constitution, PPD-28, the Foreign Intelligence Surveillance Act (50 U.S.C. § 1801 et seq.), the Privacy and Civil Liberties Oversight Board (PCLOB) and Inspectors General[758].

In the Privacy Shield Decision, the Commission evaluated the legal framework of the U.S. regarding the interference by the public authorities according to the provided documents by the U.S. side[759]. The evaluation in this section will have a broader scope, and will include related legal framework not limited with the provided documents by the U.S. side in the Privacy Shield memorandum.

However, as mentioned earlier, the data protection in the U.S. is governed by diverse, sector-specific and multilevel legislations, which sometimes conflict with each other[760]. A comprehensive review of the U.S. data protection legal framework will be well beyond the scope of this study.

7.2. EVALUATION OF THE PRINCIPLES RELATED TO THE ACCESS BY THE U.S. PUBLIC AUTHORITIES TO DATA TRANSFERRED UNDER THE PRIVACY SHIELD

As mentioned earlier, the limitations and safeguards in the U.S. regarding the interference by public authorities are provided in the Privacy Shield memorandum[761]. However, there is one principle related to this section of the study under the Supplemental Principles of the Privacy Shield. That principle is Access Requests by the U.S. Public Authorities.

---

[757] The letter is in the ANNEX VI of the Privacy Shield Commission Adequacy Decision. See, Privacy Shield, *supra* note 42, ANNEX VI.
[758] See Ibid.
[759] See, Privacy Shield, *supra* note 42.
[760] See, Frasher, *supra* note 141, at 791.
See also, WP 29 Opinion, *supra* note 327, at 12.
[761] See annexes, Privacy Shield, *supra* note 42.

7.2.1. Improvements over the Safe Harbour Regarding the Supplemental Principle "Public Record and Publicly Available Information"

The sixteenth principle under the Supplemental Principles is *Access Requests by Public Authorities*. The Privacy Shield Framework introduces this principle for the first time. According to the principle, the participating organizations may publish periodic transparency reports to reveal the number of requests by public authorities, if the U.S. Law permits the disclosure. The Principle also dictates that if an organization does not comply with the Notice Principle, it is still obliged to respond to the requests of the public authorities[762].

7.3. REVIEW OF THE DATA PROTECTION LEGISLATION OF THE U.S. REGARDING THE SURVEILLANCE

7.3.1. PPD 28

In the overview, it is stated that PPD-28 provides that, the signals intelligence can only be performed provided in the presence of an authorization by the statute, or Presidential authorization with the purposes of foreign intelligence or counterintelligence[763]. The PPD-28 also mandates that the signals intelligence should be performed in a feasible way, therefore bulk collection can only take place when it is not practicable to collect the data in a targeted[764] manner[765]. In addition to that, the signals collection mechanisms should be reasonably designed to minimize the dissemination and retention of the personal information[766].

Bulk collection and use of personal data by PPD-28 is allowed under certain conditions. These are:

i. "detecting and countering certain activities of foreign powers; counterterrorism;

---

[762] Id. ANNEX II.III.16.

[763] Id. ANNEX VI.
See, Presidential Policy Directive, supra note 158.

[764] Targeting stands for utilizing specific facilities, selection terms and identifiers according to the PPD 28.

[765] Ibid.

[766] Ibid.

ii. counter-proliferation; cybersecurity; detecting and countering threats to U.S. or allied armed forces; and

iii. combating transnational criminal threats, including sanctions evasion[767]."

The limits to protect the privacy and civil liberties are not only intended for U.S. citizens but also for all the persons independent from the nationalities of the data subjects[768]. Moreover, the requirements set by the PPD-28 are applicable to all of the intelligence methods and operations performed by the United States, independent of the source or type of the data[769].

The retention of the data is subject to certain limitations under the PPD-28. If the collected data is reasonably believed to be evidence of a crime, or meets the standards set forth by the Executive Order 12333[770], section 2.3. the data may be retained. Otherwise, the data may not be retained longer than five years[771]. The conditions that allow the retention of such data is numerous under the Executive Order 12333, section 2.3.[772] For instance, collection, retention and dissemination of the data is considered to be lawful, if the information is obtained in the course of a lawful foreign intelligence, counterintelligence international drug, or international terrorism investigation, or the information is simply necessary for administrative purposes[773].

The Compliance and the Oversight of the Signals Intelligence Activities are, according to the PPD-28, performed by the oversight personnel of the Intelligence Community, for instance NSA, the Department of Justice, the Department of Defense, and by the Office of the Inspector General which exists in each element of the Intelligence Community, ODNI's Civil Liberties and Privacy Office, the

---

[767] Ibid.
See, Presidential Policy Directive, supra note 158, §2.
[768] Ibid.
[769] Ibid.
[770] See, Center Intelligence Agency Intelligence Activities: Procedures Approved by the Attorney General Pursuant to Executive Order 12333,
https://www.cia.gov/about-cia/privacy-and-civil-liberties/CIA-AG-Guidelines-Signed.pdf.
[771] Privacy Shield, *supra* note 42, ANNEX VI.
[772] Ibid.
[773] See Section 2.3, Executive Order 12333 United States Intelligence Activities.

Privacy and Civil Liberties Oversight Board, the Foreign Intelligence Surveillance Court and the U.S. Congress[774].

7.3.2. Foreign Intelligence Surveillance Act - Section 702

The General Counsel Rober Litt in the Privacy Shield memorandum provides a review of the Section 702[775]. The interference by the public authorities, under Section 702 is performed in a focused way with a specific target[776]. The requirements set forth in the PPD-28 are also valid for the Section 702 and the collection is subject to the both independent judicial supervision and substantial review and oversight within the Executive Branch and Congress[777]. The Section 702 allows the U.S. authorities collect personal data of the non-U.S. persons located outside of the United States[778]. The collection may also be performed with the helps of U.S. electronic communications service providers[779].

To collect signals intelligence under Section 702, the FISA Court should approve certifications issued by the Attorney General and DNI, and the certifications should include "targeting" and "minimization" procedures[780]. The FISA Court, evaluating the certifications, rules that that those "targeting" and "minimization" procedures do not permit bulk or indiscriminate collection of data. The targeting requires that the collection should be performed by using selectors such as email addresses or telephone numbers[781].

7.3.3. USA FREEDOM Act

The General Counsel Rober Litt in the Privacy Shield memorandum provides a review of the USA Freedom Act[782]. The Act entered into the force in June 2015,

---

[774] See, Presidential Policy Directive, supra note 158, §4(a).
[775] Privacy Shield, *supra* note 42, ANNEX VI.
[776] Id. ANNEX VI.II.
[777] Ibid.
[778] Ibid.
[779] Ibid.
[780] Ibid.
[781] See, PPD-28, §4(a).
[781] See, Section 702 of the FISA Amendments Act of 2008
[782] Privacy Shield, *supra* note 42, ANNEX VI.

and prohibits the bulk collection of any records regardless of the location or nationality of the data subjects. According to the Act, the public authorities should use "specific selection terms" identifying a person, account, address or personal device[783]. The public authorities should select those terms in a way that terms should precisely identify a specific target and focus on that target whenever reasonably practicable[784]. The Act also mandates a standing panel of lawyers who are experts in privacy and civil liberties, intelligence collection, communications technology and similar areas[785]. The panel functions before the court as amicus curiae[786].

The General Counsel emphasizes that the Act mandates that the public reports should be published indicating the number of the National Security Letter Requests about both U.S. and non-US persons[787].

7.3.4. Redress Mechanisms in the Context of Interference by the Public Authorities

The Commission evaluates that under FISA data subjects can sue the U.S. government or U.S. government officials in case that they are subject of unlawful electronic surveillance[788]. In the memorandum General Counsel communicates that the data subjects can sue for money damages including the punitive damages and attorney's fees[789]. Also, the unlawful use or disclose of the information can be suppressed and criminal penalties can be provided under FISA[790].

Furthermore, The Computer Fraud and Abuse Act[791] provides redress in case of intentional unauthorized access or exceeding authorized access to the data[792].

---

[783] See, USA FREEDOM Act of 2015, Pub. L. No 114-23, § 401, 129 Stat. 268.
[784] Ibid.
[785] Ibid.
[786] See, USA FREEDOM Act of 2015, Pub. L. No 114-23, § 401.
[787] Privacy Shield, *supra* note 42, ANNEX VI.II.
See, USA FREEDOM Act of 2015, Pub. L. No 114-23, § 601.
[788] Privacy Shield, *supra* note 42, recital 111.
[789] Id. ANNEX VI.V.
[790] Ibid.
[791] See, 18 U.S.C. § 1030.
[792] Privacy Shield, *supra* note 42, ANNEX VI.V.

The Electronic Communications Privacy Act[793] provides redress in case that government officials unlawfully access the personal data[794]. The Right to Financial Privacy Act[795] provides redress in case that government unlawfully accesses the bank customer's records[796]. The Freedom of Information Act[797] provides redress in case that a federal agency keeps records not complying with the 5 U.S.C[798].

Taking into account that the U.S. does not provide effective access to civil disputes, and there are unreasonable delays in the civil justice, the mere existence of the right to redress does not mean that the U.S. Law provides effective redress mechanisms[799]. That point will be evaluated in this section.

7.3.5. Judicial Redress Act

Judicial Redress Act (JRA) is a federal law enacted by the Congress in 2016. The aim of the JRA is to provide the right to redress for a number of U.S. allies including the EU members. The redress act under the JRA enables the EU subjects seek redress in the U.S. courts when they believe their personal data is unlawfully disclosed to the U.S. public authorities for the purpose of law enforcement[800].

It is argued that the Judicial Redress Act only allows EU subjects to seek redress in the U.S. Courts within the scope of the Privacy Act of 1974[801]. The Privacy Act of 1974, however merely provides principles related to the access to

---

[793] See, 18 U.S.C. §§ 2701-2712.
[794] Privacy Shield, *supra* note 42, ANNEX VI.V.
[795] See, 12 U.S.C. §§ 3401-3422.
[796] Privacy Shield, *supra* note 42, ANNEX VI.V.
[797] See, 5 U.S.C. § 552(b).
[798] Privacy Shield, *supra* note 42, ANNEX VI.V.
[799] Roderick B. Mathews & Juan Carlos Botero, *Access to Justice in the United States*, 59 VIRGINIA LAWYER 24–25 (2010), at 25.
[800] Martin A. Weiss & Kristin Archick, U.S.-EU Data Privacy: From Safe Harbor to Privacy Shield (2016), p.13-14.
[801] Danny O'brien & Rainey Reitman, THE PRIVACY SHIELD IS RIDDLED WITH SURVEILLANCE HOLES | ELECTRONIC FRONTIER FOUNDATION (2016), https://www.eff.org/deeplinks/2016/03/privacy-shield-riddled-surveillance-holes (last visited Dec 24, 2017).

the records maintained by the government[802]. Moreover, the right to seek redress provided by the Privacy Act of 1974 is excessively complex to use even for the U.S. citizens, as there is a good number of exceptions in the context of national security[803]. Therefore, O'Brien and Reitman consider the Judicial Redress Act as "worthless" in the context of Privacy Shield[804].

7.4. FINDINGS OF THE CJEU IN THE SCHREMS DECISION REGARDING THE ACCESS BY THE U.S. PUBLIC AUTHORITIES

As discussed earlier, in its invalidity decision, CJEU investigated the Safe Harbour Decision, and identified the points that infringe the EU Law[805]. The findings regarding the access by the U.S. public authorities can be evaluated under these topics:

i. The Safe Harbour enables interference without any limitations. Sensitive information, or adverse consequences of the interference are not of importance;

ii. There is no effective legal protection against the interference of the public authorities;

iii. The Safe Harbour permits bulk collection of data on a generalized basis[806];

To be able to claim that the Privacy Shield provides an adequate level of data protection, it must be showed that the Privacy Shield provides improvements in accordance with the criterion set forth in the Schrems Decision[807]. Therefore, the points mentioned above will be evaluated in this section.

---

802 Ibid.
803 Ibid.
804 Ibid.
805 See, Maximillian Schrems, *supra* note 102.
806 Ibid.
807 See, Bräutigam, *supra* note 38, at 166.
See also, Monteleone & Puccio, *supra* note 153, at 16.

7.4.1. Limitations to the Interference, Sensitive Information, and Adverse Consequences of the Interference

In the Privacy Shield memorandum, the U.S. Secretary of State John Kerry in his letter to the Commissioner Jourova, states the commitment of the U.S. side related to the Ombudsperson mechanism[808]. The Ombudsperson mechanism, as was discussed earlier, provides a contact point for the requests and complaints related to the interference of the public authorities to ensure that the Intelligence Community performs within the limitations provided by the U.S. Law and Privacy Shield[809]. However, as stated earlier, there is a discussion regarding the sufficiency of powers of the Ombudsperson[810].

In the Annex V and Annex VI, General Counsel Robert Litt from the Office of the Director of National Intelligence provides an overview of the legal context around the signals intelligence collection activities, since the Privacy Shield Principles do not provide those limitations[811]. The U.S. law as reviewed in memorandums is in help for the Commission to analyze[812]. However, there is little information in the annexes related to the secret status of the Foreign Intelligence Surveillance Act (FISA) Court. Moreover, there is lack of judicial oversight in conducting targeting surveilance[813].

Besides, application for surveillance warrants and FISA hearings are highly classified, and the information related to the applications and court hearings are not available to the EU officials[814]. The only possible way of communication is case-by-case consultation. Additionally, they state that the limitations to the signals collection activities are insufficient in the Privacy Shield[815].

---

[808] Privacy Shield, *supra* note 42, ANNEX III.
[809] Id. ANNEX III. Annex A.
[810] See, Bräutigam, *supra* note 38, at 166.
See also, Monteleone & Puccio, *supra* note 153, at 32.
See also, Brennan et. al, *supra* note 161, at 48-49.
See also, WP29, *supra* note 54, at 19.
[811] Privacy Shield, *supra* note 42, ANNEX V and VI.
[812] Id. recitals 125-135.
[813] WP29 Opinion, *supra* note 327, at 43.
[814] GARY CLYDE HUFBAUER & EUIJIN JUNG, PB 16-12 THE US-EU PRIVACY SHIELD PACT: A WORK IN PROGRESS (2016), at 5.
[815] Ibid.

To exhibit how the FISA court functions in the context of surveillance, 2007-2008 Yahoo case[816] is of importance. The FISA court, under the Section 702 of the FISA Amendments Act, requested user information from Yahoo for the purpose of national security. The Court's order and the hearings were classified and close to the public. Yahoo General Counsel Ron Bell comments that the decisions that publicize records of the FISA courts are highly rare. Yahoo challenged the court order on the grounds that the order did not comply with the constitution, in result the U.S. government forced Yahoo to pay $250,000 in fines per day if Yahoo refused to comply. The decision of the FISA court was opened to the public only after Yahoo appealed[817].

Even though, the approach of Yahoo to surveillance activities might be an indication of the respect to the right to privacy by the U.S. organizations, in 2013, Yahoo CEO Marissa Mayer stated that the non-compliance to the classified FISA court orders result in fines for the companies and charges of treason for the employees, it is not sensible to resist those orders[818]. Therefore, it can be argued that the companies are relucatant to object to the classified FISA court orders for the purposes of protecting the fundamental rights of their consumers.

As mentioned in the supplemental principle *Access Requests by Public Authorities*, participating organizations may voluntarily publish transparency reports to reveal the number of the requests from the public authorities[819]. However, the U.S. companies wishing to publish transparency reports face a number of difficulties. According to the FISA, the number of National Security Letters can only be indicated as between 0 to 999, 1000 to 1999 and so on. On November 2015, Commissioner Jourova stated that the number of public requests is not of importance in evaluation of the necessity and proportionality of the access requests. She added that the transparency reports should be structured in a

[816] Yahoo v. United States, No.08-01. (May 29, 2008, FISC).
[817] See, Shedding Light on the Foreign Intelligence Surveillance Court (FISC): Court Findings from Our 2007-2008 Case, https://yahoopolicy.tumblr.com/post/97238899258/shedding-light-on-the-foreign-intelligence (last visited Dec 24, 2017).
[818] Hare, *supra* note 251, at 5.
[819] Privacy Shield, *supra* note 42, ANNEX II.III.16.

way that the necessity and proportionality of the access requests can be evaluated[820]. In addition to this the New America Foundation, in its report showed that none of the world's top companies were able to inform their users on basic disclosures about privacy and censorship[821]. However, neither Privacy Shield nor the updated U.S. legislation brings improvements regarding the transparency reports, and WP29 ciriticizes the lack of information in transparency reports[822].

In the Data Retention Judgment, the CJEU ruled that both the collection of and the access to the data should be subject to the limitations[823]. The Court also finds the Data Retention Directive (hereafter DRD) does not comply with the Article 7 and Article 8 of the Charter due to the fact that Article 4 of the DRD does not limit the access and use of the personal data by the public authorities[824]. The Court rules that the directive should ensure that the competent national authorities have access to the data and can use them only for the purposes of prevention, detection or criminal prosecutions concerning offenses taking into account the principle of proportionality, ensuring that the interference is limited to what is strictly necessary[825]. In that way, the Court sets forth the principles for the limitations to the interference of the public authorities.

According to the DPD, both access to and collection of the personal data are accepted as forms of processing[826]. In this connection, it is argued that Commission Decision is misleading in its analysis, categorizing the collection of the personal data and access to the personal data differently[827]. In addition to that under the Privacy Shield, public authorities are able to collect, access to, and use the personal data not only in the context of criminal offenses but also under the national security, public interest and law enforcement purposes which does not

---

[820] See, http://www.pcworld.com/article/3004836/eu-wants-us-companies-to-report-intelligence-agency-data-access-requests.html

[821] Hare, *supra* note 251.

[822] WP29, *supra* note 54, at 33.

[823] Digital Rights Ireland, *supra* note 573.

[824] Id. para. 34-35.

[825] Id. para. 61.

[826] See, DPD, *supra* note 1, art. 2(b).

[827] Gert Vermeulen, *The paper shield: on the degree of protection of the EU-US privacy shield against unnecessary or disproportionate data collection by the US intelligence and law enforcement services* (2016). at 7.

comply with the DPD[828]. In this connection, limitations provided by the Privacy Shield to the interference are insufficient[829].

Under the Privacy Shield framework, in parallel with the Schrems Decision, there are some improvements in the context of collection of sensitive information by the public authorities. Firstly, under PPD-28, if the target or means of the collection is sensitive, then senior policymakers should review the collection activity[830]. Secondly, the Intelligence Community developed a new mechanism for the enhanced monitoring of the sensitive data[831]. Thirdly, the Intelligence Community provides further transparency for the sensitive information wherever feasible[832].

However all of the additional safeguards provided rely on PPD-28, which is a mere guidance and not enforceable by the law[833]. Furthermore, as the CJEU puts in the data retention case, the proportionality is a key issue regarding the interference[834]. However, Privacy Shield limits the lawfulness of the interference with the feasibility[835]. Consequently, wherever not feasible, the collection will be massive and unlawful[836].

7.4.2. Effective legal protection and safeguards against interference of public authorities

As discussed earlier, under annex VI of the Privacy Shield, a number of redress mechanisms provided by the U.S. law are explained[837]. FISA, the Computer Fraud and Abuse Act, the Electronic Communications Privacy Act, the Right to Financial Privacy Act and the Freedom of Information Act provide avenues of redress[838].

---

828 Id. at 6.
829 Ibid.
830 Privacy Shield, *supra* note 42, ANNEX VI.I.
831 Id. para. 83.
832 Id. ANNEX VI.IV.
833 PPD-28, §6(d) and PPD-28, §6(b).
834 Digital Rights Ireland, *supra* note 573.
835 Privacy Shield, *supra* note 42, recital 71.
836 See, Monteleone & Puccio, *supra* note 153, at 18.
837 Privacy Shield, *supra* note 42, ANNEX VI.IV.
838 Ibid.

Regarding the intelligence cases, the individuals have right to redress under the acts, which are enumerated here[839]. For EU citizens to employ their rights against abuse of or unlawful access to their data, first of all, they should learn about the violation. It is argued that there are two conditions for that: first, the organization which holds the data of the data subject should be aware of it; second, the organization should notify the DPA about it[840]. And, even if these conditions were satisfied, it would be difficult for a EU citizen to prove the non-compliance[841]. What is worse, if the organization does not report it to the data subject or the DPA, it is almost impossible for the data subject to learn about the violation[842]. To add to that, it is extremely difficult to bring surveillance related cases before the ordinary courts in the U.S.; the Supreme Court denies to stand in the intelligence cases, unless the individual shows "concrete, particularized, and actual or imminent injury[843]."

7.4.2.1. The Ombudsperson Mechanism

In the Zakharov Case, the ECHR stated that there are several stages to the surveillance, such as ordering the surveillance, carrying out, and terminating the surveillance[844]. The independent oversight is needed at those stages[845]. Since the risks of abuse in surveillance activities are not only related to the individual, but also to the democratic society, the Court finds that a judge should perform the supervision[846]. The Court adds that other bodies might also be responsible, however, they should be "sufficiently independent from the executive[847]" and the

[839] See, Brennan et. al, *supra* note 161, at 34-35.
[840] Hare, *supra* note 251, at 555.
[841] Ibid.
[842] Ibid.
[843] James R. Clapper, Jr., Director of National Intelligence, et al., Petitioners v. Amnesty International USA, et al. 568 U.S. 398 (February 26, 2013), I.
[844] Roman Zakharov, *supra* note 66, para. 233.
See, Shimovolos, *supra* note 67, Malone, *supra* note 67, Leander, *supra* note 67, Huvig, *supra* note 67, Kennedy, *supra* note 69, Huvig, *supra* note 67, at para. 34, Amann, *supra note 20*, Valenzuela, *supra note 20*, Prado, *supra note 20*, Klass and Others, *supra* note 71, Weber and Saravia, *supra* note 71, Kvasnica, *supra* note 71.
[845] Ibid.
[846] Id. para. 2.
[847] Id. para. 258.

authorities performing surveillance activities, the authority of that independent body should allow an effective and continuous control[848].

In addition to that, the Court states that the procedures of nomination and dismissal of the members of the body as well as the legal status of the members of the body are of particular importance[849]. In this connection, the legal status, the nomination and dismissal, level of independence from both the IC and the executive of the Ombudsperson should be taken into account to be able to make a conclusion on the adequacy of the Ombudsperson mechanism in the context of EU law.

Under the Annex III of the Privacy Shield, the authorities and responsibilities of the Ombudsperson mechanism is introduced[850]. According of the Annex III, the Ombudsperson's authority is not only related to the data transfers from the EU to U.S. under the Privacy Shield, but also under the standard contractual clauses and binding corporate rules[851]. Whenever a complaint is referred to the mechanism alleging a violation of law or other misconduct, Inspectors General and Privacy and Civil Liberties offices have the full authority to investigate the claims[852]. It can be stated that the Ombudsperson's authority is limited to referring the complaints to the relevant office[853].

As can be concluded from the methods of evaluation of the Commission in its Privacy Shield adequacy decision, the evaluations rely on the annexes provided by the U.S. side. It is argued that the Commission did not analyze the relevant U.S. law other than the annexes provided by the U.S[854]. Moreover, there are no changes to the U.S law after the Schrem's judgement. In this connection, the

---

[848] Klass and Others, *supra* note 71, at para. 56.
[849] Roman Zakharov, *supra* note 66, para. 278.
See, Shimovolos, *supra* note 67, Malone, *supra* note 67, Leander, *supra* note 67, Huvig, *supra* note 67, Kennedy, *supra* note 69, Huvig, *supra* note 67, at para. 34, Amann, *supra note 20*, Valenzuela, *supra note 20*, Prado, *supra note 20*, Klass and Others, *supra* note 71, Weber and Saravia, *supra* note 71, Kvasnica, *supra* note 71.
[850] Privacy Shield, *supra* note 42, ANNEX III, Annex A.
[851] Ibid.
[852] Ibid.
[853] See, WP29, *supra* note 54, at 37.
[854] Xavier Tracol, *EU–U.S. Privacy Shield: The saga continues*, 32 COMPUT. LAW SECUR. REV. 775–777 (2016), at 776.

Commission adequacy decision does not comply with the substantive criterion set forth in the Schrems Case[855].

The Commission in the adequacy decision emphasizes the independence of the Ombudsperson mechanism[856]. However, as the mechanism is formed under secretary of State, many commentators argue that the mechanism is actually not independent[857]. As WP29 states, Under Secretary in the Department of State is nominated by the President as well as it can be dismissed by the president[858]. The Privacy Shield does not provide any criteria for the dismissal of the Ombudsperson, which means the president, might dismiss the Ombudsperson whenever he wishes[859]. Which means, the independence of a court and the independence of the Ombudsperson cannot be compared in the meaning of Article 47 of the Charter[860]. To add that, the physical office of the Ombudsperson is in the US Department of State, the individual Catherine A. Novelli[861] appointed to act as Ombudsperson is Under Secretary of State, and has certain responsibilities as a member of the intelligence community[862]. Therefore, the mechanism cannot be regarded as an independent oversight body[863].

It is also statesd that the Ombudsperson mechanism is actually not a safeguard[864]. There is no EU-involvement in the mechanism: the only function of the Ombudsperson is to receive complaints from the EU side and refer them to the related authority[865]. To add to that the Privacy Shield is insufficient in designating

---

855 Id. at 776-777.
856 Privacy Shield, *supra* note 42, recital 117.
857 See, Monteleone & Puccio, *supra* note 153, at 32.
See also, Schrems, *supra* note 41, at 149.
See also, Peter Margulies, *Global Cybersecurity, Surveillance, and Privacy: The Obama Administration's Conflicted Legacy* (2017). at 22.
858 WP29 Opinion, *supra* note 327, at 49.
859 Ibid.
860 Id. at 51.
861 See, Weiss & Archick, *supra* note 311, at 10.
862 Estelle Masse & Amie Stepanovich, THREE FACTS ABOUT US SURVEILLANCE THE EUROPEAN COMMISSION GETS WRONG IN PRIVACY SHIELD - ACCESS NOW, https://www.accessnow.org/three-facts-us-surveillance-european-commission-gets-wrong-privacy-shield/ (last visited Dec 24, 2017).
863 Opinion 01/2016 on the EU – U.S. Privacy Shield draft adequacy decision, (2016), p.49.
864 Vermeulen, *supra* note 40, at. 11.
865 Ibid.

the powers and responsibilities of the Ombudsperson mechanism[866]. The existing rules are not specific[867]. The lack of the binding rules and the characteristic features of the soft law will result in a mechanism, which will not be effective in monitoring the U.S. intelligence community[868]. It is argued that, a strong track record of recourse provided by the Ombudsperson mechanism is the only way that can persuade the CJEU on its effectiveness[869].

In the Kadi II case, the CJEU set forth the substantive criteria regarding the way supervisory authorities make decisions: the person concerned should be able to learn the reasons of the decision for the person to defend his rights fully[870]. However, according to the Annex III, the Ombudsperson does not have the authority to access to the data of the concerned individual to carry out the investigation[871]. In addition to this, the Ombudsperson cannot disclose any information related to the compliance or the non-compliance nor the reasons behind them[872]. The mechanism can only communicate the result which is the issue is remedied[873]. Besides, the person concerned cannot appeal against or demand review of the decision[874].

Another issue with the Ombudsperson mechanism is that the authority of the mechanism is limited with the signal intelligence as set forth in the Annex III of the Privacy Shield[875]. WP29 puts that there is an uncertainty regarding the access by law enforcement agencies such as CIA[876]. Even though, the concerns pertaining to that uncertainty is expressed before the final draft, the final draft of the Privacy Shield does not include any clarifications or improvements on this

[866] Peter Margulies, *supra* note 857, at 5.
[867] Ibid.
[868] Ibid.
[869] Id. at 24-25.
[870] Yassin Abdullah Kadi and Al Barakaat International Foundation v. Council of the European Union and Commission of the European Communities, C-402/05 P, (Sep. 3, 2008, CJEU) para. 100.
[871] Privacy Shield, *supra* note 42, ANNEX III.
[872] WP29 Opinion, *supra* note 327, at 50-51.
[873] Ibid.
[874] Ibid.
[875] Privacy Shield, *supra* note 42, ANNEX III, Annex A.
[876] WP29 Opinion, *supra* note 327, at 48.

matter. This can be interpreted as the Ombudsperson mechanism does not have any authority regarding to the access by law enforcement agencies[877].

7.4.2.2. Administrative Subpoenas

The Commission analyzes data collection by the public authorities for the purposes of law enforcement and public interest. The Commission finds that, since the 4th amendment to the U.S. constitution requires that the interference to the electronic communications to be subject to a court order or under certain circumstances subject to a reasonability test, the US data protection level is adequate[878]. On the other hand, it must be noted that fourth amendment is not applicable to non-US citizens out of the US territory; therefore the public authorities can access the personal data of the EU individuals performing only the reasonability test[879].

Furthermore, it is criticized that the Commission did not sufficiently evaluate the administrative subpoenas[880]. Unde the U.S. law allows certain public authorities might utilize this option to access the data[881]. The Commission communicates that administrative subpoenas are subject to the judicial review[882]. However, the administrative subpoenas are subject to judicial review only provided that the organization refuses to submit data under the subpoena[883].

7.4.3. Bulk Collection of Data on a Generalized Basis

Bulk collection is defined by the PPD-28 as "acquisition of a relatively large volume of signals intelligence information or data under circumstances where the Intelligence Community cannot use an identifier associated with a specific target (such as the target's email address or phone number) to focus the collection." General Counsel Robert Litt admits that there are instances where the Intelligence

[877] See, Margulies, *supra* note 857, at 24.
[878] Privacy Shield, *supra* note 42, para. 126.
[879] Vermeulen, *supra* note 40, at 11.
[880] Id. at 12.
[881] Id. at 12.
[882] Privacy Shield, *supra* note 42, at para. 128.
[883] Vermeulen, *supra* note 40, at 12.

Community cannot use identifiers. However, the way the data is collected is in parallel with the PPD-28, which requires that the signal intelligence activities should be as tailored as feasible. Therefore, he explains that those activities can only be performed minimizing the non-pertinent data, eliminating it completely is not possible. He argues that, if the IC narrows down the collection using discriminants, the collection will not be mass or indiscriminate collection, even though it will be considered as bulk collection. As the nature of the bulk collection appears to be more risky due to the collection of non-pertinent data, PPD-28 provides six purposes only under which the bulk collection may be performed.

As the specific administrative purposes are not specified, it can be argued that the Executive Order 12333, and PPD-28 do not effectively limit retention of data[884]. Retention of data however is an important concept in EU data protection law[885].

It is argued that the adoption of the amendment to the Section 2.3 of the Executive Order 12333 on 3 January 2017 by the U.S. Attorney General jeopardized the sustainability of the Privacy Shield[886]. The amended Section 2.3, enables NSA access to, and process all of the data of the EU citizens "without any clear or effective supervision, judicial guarantees and effective remedies[887]."

Commission evaluates that signal intelligence activities are conducted according to the limitations of PPD-28 therefore; bulk collection of data is limited to the instances mentioned above[888]. However, Commission does not admit that targeted collection of data is only performed after acquisition of bulk data[889].

---

[884] Monteleone & Puccio, *supra* note 153, at 29 n.114.
See, Bräutigam, *supra* note 38, at 165.
[885] See, Digital Rights Ireland, *supra* note 573.
See also, CFEU, *supra* note 6, art. 7, 8 and 11.
[886] Elspeth Guild, Didier Bigo & Sergio Carrera, *Harvesting personal data and requiem for the EU-US Privacy Shield* (2017), at 6.
[887] Ibid.
[888] Privacy Shield, supra note 42, recital 61.
[889] Brennan et. al, *supra* note 161, at 38.

In addition to that PPD-28 does not create any rights, and it is not an enforcable legal document[890].

As can be inferred from the annexes and the evaluations of the Commission decision, the Privacy Shield framework does not outlaw the bulk collection of data[891]. Furthermore, the bulk collection of the data is not limited by the Principles by any means[892]. The only limitation to the bulk collection is provided by the U.S law[893].

Critics are concerned that the US Intelligence Community has excess power on the U.S. organizations from the various sectors such as financial, telecommunications, and internet companies[894]. Nevertheless, major technology companies in the U.S. resist bulk collection of data[895]. Also, new technologies provide encryption mechanisms that the IC does not have the sufficient means to decrypt[896].

The excess power of the U.S. authorities as was discussed earlier results in an increase of the obedience of the organizations to the unlawful public requests[897]. As stated earlier objecting the requests is not always possible[898]. However, the encryption methods and how the organizations utilize them are of particular importance, because they are capable of limiting the interference[899].

It is argued that bulk collection is still possible under the Privacy Shield, and only this fact is enough to state that the Privacy Shield does not comply with the DPD and CFEU. Furthermore, the six circumstances under which the bulk collection can be performed are not specific[900]. The Commission in its analysis does not mention those six circumstances, instead only exemplifies the situations

---

[890] PPD-28, §6(d) and PPD-28, §6(b).
See, WP29, *supra* note 54, at 19.
[891] See, Bräutigam, *supra* note 38, at 165.
See also, Monteleone & Puccio, *supra* note 153, at 18.
[892] Ibid.
[893] See, Brennan et. al, *supra* note 161, at 30.
[894] Haufbaer & Jung, *supra* note 814, at 2.
[895] Ibid.
[896] Ibid.
[897] See, Yahoo, *supra* note 816.
[898] Ibid.
[899] See, Haufbaer & Jung, *supra* note 152, at 6.
[900] WP29 Opinion, *supra* note 327, at 39.

where bulk collection may occur[901]. It can be argued that the Commission in the Privacy Shield Decision makes an effort to persuade the reader, rather than providing a genuine evaluation[902].

As mentioned earlier, the Commission in the Privacy Shield Decision did not provide an overall assessment of the US Legislation, instead relied on letters, which explain the relevant U.S. legislation sent from the U.S. side to the Commission[903]. However, that violates the Article 25(2) of the Directive and the findings of the CJEU in the Schrem's Decision[904]. What's more, after the Schrem's Decision there is no change in the legal system of the U.S.[905]

According to the Article 2 of the Data Protection Directive, collection, recording, and storage of the personal data are regarded as processing[906]. In this connection, collection of the personal data, whether bulk or not, constitutes processing of the data. In Malone case, ECHR finds that, the processing should be based on a precise, clear and accessible legal basis, and the interference should be foreseeable[907]. In the Zakharov case, ECHR finds that, in the context of secret measures of surveillance, the risk of arbitrariness is higher, therefore the rules of interference should be sufficiently clear and detailed for the individuals to foresee under which circumstances the public authorities are empowered to interfere[908].

Since the nature of the bulk collection results in processing of the personal data in an arbitrary way, the existence of the bulk collection as a method constitutes non-compliance with the EU law[909]. Even though, in the memorandum, the U.S. Side states that the methods of collection of the data is designed "as

---

[901] Vermeulen, *supra* note 40, at 9.
[902] See, Id. at 7.
[903] Tracol, *supra* note 854, at 776.
[904] Ibid.
[905] Id. at 777.
[906] See, DPD, *supra* note 1, art. 2.
[907] See, Malone v. the United Kingdom, supra note 67, para. 65, 66, 70.
[908] Roman Zakharov v. Russia, supra note 66, at 229.
See, Shimovolos, *supra* note 67, Malone, *supra* note 67, Leander, *supra* note 67, Huvig, *supra* note 67, Kennedy, *supra* note 69, Huvig, *supra* note 67, at para. 34, Amann, *supra note 20*, Valenzuela, *supra note 20*, Prado, *supra note 20*, Klass and Others, *supra* note 71, Weber and Saravia, *supra* note 71, Kvasnica, *supra* note 71.
[909] See, Vermeulen, *supra* note 40, at. 9.

tailored as feasible[910]" to minimize the collection of the data by elimination of the collection of the irrelevant data, the limits of feasibility cannot be inferred from the memorandum[911]. In addition to this, minimizing the irrelevant data by targeting, using relevant discriminants does not eliminate the risks of processing of the irrelevant individuals' data. This clearly contradicts the findings of the ECHR in the Zakharov case, since according to the Court, there should be reasonable suspicion against the person concerned and that person should be identified by name, address, telephone number or by some other similar discriminant. Thus, only the targeted information should be collected[912].

Nevertheless, the six circumstances of bulk collection should be analyzed to evaluate whether they are sufficiently clear. The section where PPD-28 enumerates those six circumstances begins with: "in particular, when the United States collects non-publicly available signals intelligence in bulk, it should use that data only for the purposes ...[913]" It is clear that those six purposes are not related to the collection of the data, but the use of it[914]. Considering that the collection is also a form of processing, the PPD-28 enables bulk collection of the data, in other words, bulk processing of the data without any limitations.

Those six purposes are:

i. "Espionage and other threats and activities directed by foreign powers or their intelligence services against the United States and its interests;
ii. Threats to the United States and its interests from terrorism;
iii. Threats to the United States and its interests from the development, possession, proliferation, or use of weapons of mass destruction;
iv. Cybersecurity threats;

---

[910] See, Privacy Shield, *supra* note 42, ANNEX VI.
[911] See, WP29 Opinion, *supra* note 327, at 38.
[912] Roman Zakharov v. Russia, supra note 66, at 264.
See, Shimovolos, *supra* note 67, Malone, *supra* note 67, Leander, *supra* note 67, Huvig, *supra* note 67, Kennedy, *supra* note 69, Huvig, *supra* note 67, at para. 34, Amann, *supra note 20*, Valenzuela, *supra note 20*, Prado, *supra note 20*, Klass and Others, *supra* note 71, Weber and Saravia, *supra* note 71, Kvasnica, *supra* note 71.
[913] See PPD-28, supra note 158.
[914] See, Vermeulen, *supra* note 40, at. 7.

v. Threats to U.S. or allied Armed Forces or other U.S or allied personnel; and

vi. Transnational criminal threats, including illicit finance and sanctions evasion related to the other purposes named in this section[915]"

The first purpose enables the U.S. Public authorities to collect bulk data regarding "any activity against the interests of the United States". It can be stated that, the first purpose is wide enough to cover the rest of the purposes. As minimum, the PPD-28 under the first purpose should have limited the type of activities and specified the regarding U.S. interests. Looking back to the Zakharov case[916], there is no way an individual can foresee under which circumstances the public authorities are empowered to interfere. For the mentioned reasons, Privacy Shield does enable the bulk collection of the data on a generalized basis and do not comply with the EU law.

7.5. CONCLUSION

The analysis in this section shows that the Privacy Shield does not meet the substantive criterion of the Schrems Judgement. Particularly, the following findings of the CJEU are still valid for the Privacy Shield.

i. There is no effective legal protection against the interference of the public authorities;

ii. The data protection legal framework (Safe Harbour) permits bulk collection of data on a generalized basis;

There is no effective legal protection against the interference of the public authorities, because,

i. administrative subpoenas are not subject to the judicial review by default,

ii. Under very limited conditions, are there options for EU citizens to seek redress in the U.S. courts,

---

[915] See, Presidential Policy Directive 28 (PPD-28) Signals Intelligence Activities, p.4.

[916] See, Roman Zakharov, *supra* note 66.
See also, Shimovolos, *supra* note 67, Malone, *supra* note 67, Leander, *supra* note 67, Huvig, *supra* note 67, Kennedy, *supra* note 69, Huvig, *supra* note 67, at para. 34, Amann, *supra note 20*, Valenzuela, *supra note 20*, Prado, *supra note 20*, Klass and Others, *supra* note 71, Weber and Saravia, *supra* note 71, Kvasnica, *supra* note 71.

iii. Ombudsperson cannot be considered as a mechanism of legal protection, because it is not independent and lacks the investigatory powers.

The bulk collection is still possible under the Privacy Shield because the U.S. legislation allows bulk collection of personal data and mass surveillance.

Since the findings in the Schrems Decision are valid for the Privacy Shield as well, highly likely, the CJEU will invalidate the Privacy Shield Decision.

SECTION 8

THE WAYS IN, WHICH THE PRIVACY SHIELD CAN BE IMPROVED

8.1. INTRODUCTION

In this section, additional options other than the options which are provided in the previous sections will be examined. These alternatives will be:

i. data localization,
ii. ceasing the privacy shield and relying on other methods of cross-border data transfers under the DPD and GDPR,
iii. leaving the surveillance practices out of the scope of the adequacy decisions,
iv. relying on the encryption methods,
v. establishing an Independent Data Authority in the U.S.,
vi. Simplifying and improving the redress options.

8.2. EVALUATION OF THE POSSIBLE OPTIONS

8.2.1. Data Localization

It is argued that data localization restrains the reach of the national intelligence agencies[917]. On the other hand, it is also stated that data localization is not an option, because the EU subjects are in communication with the U.S. subjects, as well as subjects of other countries[918]. Therefore, the data localization

[917] Haufbaer & Jung, *supra* note 152, at 2.
[918] See, e.g., Kuner, supra note 252, at 914.

cannot be a large scale solution, even all of the companies which process data, install data servers within the borders of the EU[919].

However, installing data servers within the borders of the EU in an attempt to circumvent the interference of the U.S. authorities is not a viable option[920]. The reason is that the excessive cost and time needed for such an investment[921].

It can be argued that centralizing data will make the data more vulnerable to interventions[922]. On the other hand, not centralizing it makes it more difficult for third parties to intervene, and draw meaningful conclusions out of the decentralized data[923]. Therefore, seperation of data will yield better privacy protection[924].

In the context of data localization, the new legislation, which is to be enforced by Russia in 2018, is worth consideration. The new legislation, Act 242, requires all of the personal data to be kept within the borders of Russia[925]. The technology company Twitter declared, that they will comply with that legislation[926]. However, the famous technology company Facebook does not have such plans. Russian Federal Service for Supervision of Communications, Information Technology and Mass Media (hereafter Roskomnadzor) declares that they will block the access to Facebook, in case of non-compliance, by the time the the legislation enters into force[927]. On the other hand, another technology company, Linkedin declared that they will cease the operations in Russia[928].

As can be seen in the Russia case, data localization undermines even the operations of giant technology companies, let alone the small and medium scale businesses. Setting aside the economical impacts, data localization practice in the

---

919 Ibid.
920 Deckelboim, *supra* note 57, at 295.
921 Ibid.
922 Colesky & Ghanavati, supra note 340, at 274.
923 Ibid.
924 Ibid.
925 Anastasia Agamalova & Ksenia Boletskaya, Roskomnadzor prigrozil Facebook blokirovkoi Vedomosti (2017), http://rodina.news/roskomnadzor-prigrozil-facebook-blokirovkoi-2018-godu-17092614153034.htm (last visited Dec 14, 2017).
926 Ibid.
927 Ibid.
928 Ibid.

EU could jeopardize the rights protected under the Charter, such as freedom of thought, conscience and religion (Article 10), freedom of expression and information (Article 11), and freedom of assembly and of association[929] (Article 12).

8.2.2. Ceasing the Privacy Shield and Relying on Other Methods of Cross-Border Data Transfers under the DPD and GDPR

As mentioned earlier, according the DPD, there are a number of options that can be utilized to transfer data out of the EU when there is no adequacy decision indicating that the target country provides an adequate level of data protection. Those options are provided under the Article 26 and categorized under "adequate safeguards" and "derogations[930]." The adequate safeguards are contractual clauses and binding corporate rules[931]. Contractual clauses are basically contracts between the sending and receiving parties[932]. Binding corporate rules are rules of a company or a group of companies regarding the transfer of data, which are approved by the DPAs[933].

As can be observed, the adequacy decisions are not the only instruments to provide data transfers between EU and third countries. In that connection, it is argued that there are Standard Contractual Clauses and Binding Corporate Rules, so the future of the transatlantic data transfers neither depends on the Privacy Shield nor the forthcoming adequacy decisions completely[934].

To evaluate the possibility of relying on standard contractual clauses and binding corporate rules instead of adequacy decisions, an overview of the practical implications of those approaches should be reviewed.

---

[929] Nicola Lucchi, *Access to network services and protection of constitutional rights: Recognising the essential role of internet access for the freedom of expression*, 19 CARDOZO J. INT. COMP. LAW 645–678 (2011), at 648.
[930] DPD, *supra* note 1, art. 26.
[931] Ibid.
[932] Ibid.
[933] Ibid.
[934] W. Gregory Voss, *The Future of Transatlantic Data Flows: Privacy Shield or Bust?*, 19 J. INTERNET LAW 1 (2016), at 16.

Model Contract Clauses require the importer and the receiver of personal data to enter into a contract of which there are standard clauses issued by the Commission[935]. This method is more suitable for large companies, and large U.S. companies[936] already use this method for data transfers. On the other hand, it would be not practical for the small and medium scale companies, since implementation of this method is costly and cumbersome[937].

Binding Corporate Rules (BCRs) are standards, which are determined with a EU DPA, and the transfers under the BCRs can only be performed within the company. Moreover, the implementation of this method is also time-consuming; it can take up to two years[938].

It is however, argued that the binding corporate rules and contractual clauses do not provide protection against the surveillance activities, since they are mere contracts between private parties[939]. The interference of the public authorities can no way be restricted or limited by the virtue of those legal instruments[940]. For comparison, the Privacy Shield at least comprises a set of commitments of the U.S. side. The Article 26 of the DPD provides derogations under which the personal data can be transferred[941]. The derogations can be utilized when there is no Commission adequacy decision for a third country[942]. The GDPR lays out similar provisions under the Article 49[943]. The Article 26 of the DPD provides that, such a transfer can be performed if:

i. "the data subject has given his consent unambiguously to the proposed transfer; or

---

[935] Lingjie Kong, *Data Protection and Transborder Data Flow in the European and Global Context*, 21 EUR. J. INT. LAW EJIL 441–456 (2010), at 450
[936] e.g. Microsoft, Google.
[937] Weiss & Archick, *supra* note 311, at 14.
See also, Lingjie Kong, *supra* note 935, at 455.
[938] Weiss & Archick, *supra* note 311, at 14.
[939] Kuner, supra note 252, at 907.
[940] Ibid.
[941] DPD, supra note 1, art. 26.
[942] Ibid.
[943] GDPR, *supra* note 330, art. 49.

ii. 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
iii. 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
iv. the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defence of legal claims; or
v. the transfer is necessary in order to protect the vital interests of the data subject; or
vi. 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."

Kuner asserts that the transfers under derogations are performed without any kind of protection[944]. In addition to that, the derogations cannot be used for long term, nor can they be used for "repeated or structural data transfers[945]."

As can be observed, the conditions for the derogations are softer than those of the adequate safeguards. For that reason, and taking into account that there is no DPA involvement in the evaluation of the conditions for them, and the fact they cannot be used in a long term fashion, it can be claimed that, neither can the derogations replace the Privacy Shield.

The standard contractual clauses and derogations could replace the Privacy Shield, if those were cost and time efficient. However, it is not the case. Moreover, under the DPD and the GDPR, there are no alternative methods other than adequacy decisions, standard contractual clauses and derogations.

---

[944] Kuner, *supra* note 252, at 909.
[945] Ibid.
See also, WORKING PARTY ON THE PROTECTION OF INDIVIDUALS & WITH REGARD TO THE PROCESSING OF PERSONAL DATA, TRANSFERS OF PERSONAL DATA TO THIRD COUNTRIES: APPLYING ARTICLES 25 AND 26 OF THE EU DATA PROTECTION DIRECTIVE, 22 (1998).

Therefore, the only option left out is the effective application of the adequacy decisions. In the case of the U.S., it is updating the Privacy Shield in a way that, it essentially provides an adequate level of data protection.

8.2.3. Leaving the Surveillance Practices Out of the Scope of the Adequacy Decisions

Some of the authors argue that the EU members also conduct surveillance activities similar to that of the U.S. that is why it is not legally correct to evaluate the data protection level in the U.S. limiting the scope of the evaluation with the written law. Brautigam states that the German Secret Service (the BND) conducts surveillance activities on EU partners and NATO[946]. UK, France and the Netherlands also conduct mass surveillance practices[947].

EU-U.S. NGO Letter on Safe Harbor After Schrems also include and argument that EU members conduct surveillance activities, which are in the form of mass surveillance[948].

In addition to that, some of the authors argue that legal texts are not capable of changing the surveillance practices. Kuner argues that the both the Commission's evaluation of the Privacy Shield in the Privacy Shield Decision and the CJEU's Schrems's Decision rely on legal texts[949]. CJEU can only find the contradictions in the text and make conclusions out of those contradictions[950]. Therefore, a through evaluation of the intelligence surveillance practices can be conducted neither by the Commission nor by the CJEU[951].

Lam argues that CJEU evaluation by the CJEU on the data protection level of the U.S. is contrary to the international customs[952]. Moreover, the fact that many

---

[946] Bräutigam, *supra* note 38, at 168.
[947] Jens Henrik Jeppesen, CJEU GENERAL ADVOCATE OPINION IN SCHREMS CASE A WAKE-UP CALL | CENTER FOR DEMOCRACY & TECHNOLOGY, https://cdt.org/blog/cjeu-general-advocate-opinion-in-schrems-case-a-wake-up-call/ (last visited Dec 24, 2017).
[948] EU-US NGO Letter, *supra* note 46, at 8.
[949] Kuner, supra note 252, at 910.
[950] Ibid.
[951] Ibid.
[952] Lam,

countries, including the EU members, engage in surveillance practices undermines the legal grounds of the Schrem's Decision[953].

Haufbaer and Jung argue that since the practices of the U.S. intelligence community is highly classified, the best way that U.S. side can comfort the EU side regarding the lawfulness of the surveillance practices is through the letters such as those provided under the Privacy Shield[954].

Therefore, it can be argued that it is neither practical nor lawful to evaluate U.S. written law relevant to the surveillance practices, as the written law does not reflect the real world practices. However, leaving the intelligence surveillance practices of the U.S out of the evaluation is also not a desired approach, since it would be against the provisions in the article 7 and 8 of the of the Charter regarding the right to data protection, necessity and proportionality requirements regarding the interference by the public authorities, and decisions of the ECtHR[955].

8.2.4. Relying on the Encryption Methods

EU-U.S. NGO Letter on Safe Harbor After Schrems recommends The U.S. law and policies should provide an increase in the level of encryption to provide a stronger level of data encryption[956].

Haufbaer and Jung argue that the state-of-the-art encryption techniques limit the reach of the NSA, since NSA has limited decoding capabilities[957]. To add that, major U.S. technology companies are against the mass surveillance of the NSA[958]. For instance, Facebook utilizes such encryption methods, and even Facebook

---

[953] Paul de Hert & Vagelis Papakonstantinou, *The new General Data Protection Regulation: Still a sound system for the protection of individuals?*, 32 COMPUT. LAW SECUR. REV. 179–194 (2016), at 11.
[954] Haufbaer & Jung, *supra* note 152, at 5.
[955] See, Roman Zakharov, *supra* note 66.
See also, See also, Shimovolos, *supra* note 67, Malone, *supra* note 67, Leander, *supra* note 67, Huvig, *supra* note 67, Kennedy, *supra* note 69, Huvig, *supra* note 67, at para. 34, Amann, *supra note 20*, Valenzuela, *supra note 20*, Prado, *supra note 20*, Klass and Others, *supra* note 71, Weber and Saravia, *supra* note 71, Kvasnica, *supra* note 71.
[956] EU-US NGO Letter, supra note 46.
[957] Haufbaer & Jung, *supra* note 152, at 2.
[958] Ibid.

cannot read the contents of the data packets, let alone the NSA and Federal Bureau of Investigation (hereafter the FBI)[959].

According to Hare, law enforcement and intelligence agencies demand legislation that will increase their reach to data[960]. However, the application of the proper encryption techniques might leave those agencies ineffective in bringing terrorists and criminals to justice[961]. On the other hand, increasing the level of encryption will not only provide more room for privacy, but also increase the overall security of the data systems[962].

Deckelboim argues that encryption techniques can make the surveillance tools[963] of the NSA useless[964]. He also asserts that, in the absence of an adequacy decision, U.S. companies might rely on encryption, and that way the required adequacy standards can be reached[965]. In that case, the U.S. public authorities could access the data only on a targeted basis, and that would not undermine the right to privacy and right to data protection in a way mass surveillance does[966].

Gross argues that encryption techniques such as "end-to-end encryption with no middle man" would make interference quite difficult[967]. Moreover, court-authorized interference[968] as well would be non-executable, since it would be technologically not possible, the companies, which keep the data, would not have access to data too[969].

The main issue with the forcing the organizations to apply specific encryption techniques is that, there is no reference to it in the Privacy Shield. The only related article is the Security Principle. However, the Principle merely states that "reasonable and appropriate measures" must be taken by the organizations.

---

[959] Id. at 6.
[960] Hare, *supra* note 251, at 551-552.
[961] Ibid.
[962] Id., p.557.
[963] Such as PRISM. The PRISM program collects user data from companies such as Google, Apple and Facebook based on certain keywords. See, See, Tourkochoriti, *supra* note 329, at 462.
[964] Deckelboim, *supra* note 57, at 291.
[965] Ibid.
[966] Id. at 292.
[967] Shannon Gross, *A Mystery Wrapped in an Encryption : Surveillance and Privacy in the Encrypted Era in the Encrypted Era*, 15 NW. J. TECH. INTELL. PROP. 73 (2017) at 885.
[968] Search warrant or wiretap.
[969] Ibid.

According to Kuner, EU DPAs play a significant role in data protection, however they have limited ability when it comes to dealing with the cross-border issues, and enforcing the EU Law in the global scale[970]. Kuner asserts that the Schrems Decision is an evidence of that the EU DPAs were not able to enforce the EU Law in the context of the Safe Harbour[971].

However, the informal panel of DPAs has the authority to annul the certificate of a Privacy Shield Organization, if the organization commits to comply with the advice of the DPAs[972]. In that regard, if the Privacy Shield were updated in a way that the compliance with the advice of the DPAs were mandatory for all kinds of certified organizations, it would be possible for the informal panel of DPAs to develop its own law. In that way, the informal panel of DPAs would be able to issue its own guideline[973] extending the Principles, which could bring the data protection level provided by the Principles closer to that of the EU law. That would also make it possible for the informal panel of DPAs to require the implementation of specific encryption techniques from the Privacy Shield organizations, for a complete adherence to the Security Principle. By this way, the risk of unlawful interference of the U.S. public authorities could be lessened.

8.2.5. Establishing an Independent Data Authority in the U.S.

As mentioned earlier, the FTC and DoT provide the enforcement of the Privacy Shield[974]. However, it was found that neither the FTC nor the DoT has the sufficient enforcement powers to be able to enforce the Privacy Shield, and monitor other commitments the U.S. side made under the Privacy Shield in every sector. Besides, neither FTC nor DoT is independent. In addition to that, the absence of a comprehensive data protection legal framework jeopardizes the

[970] Kuner, supra note 252, at 885.
[971] Ibid.
[972] Privacy Shield, supra note 42, ANNEX II, III.5.c.2.
[973] Similar to the Frequently Asked Questions of the Safe Harbour.
[974] Privacy Shield, *supra* note 42, ANNEX VII.

enforcement of an adequate level of data protection in accordance with the EU standards.

In that regard, EU-U.S. NGO Letter on Safe Harbor After Schrems recommends that an independent data authority in the U.S. should be established[975]. In addition to that a comprehensive data protection legal framework should be enacted[976].

The report of the European Data Protection Supervisor (hereafter the EDPS), issued well before the Privacy Shield Decision, points out the Article 45 of the GDPR, and states that as the date of the enforcement of the GDPR, the U.S. will be obliged to establish an independent supervisory authority to be able to sustain the Privacy Shield[977].

As discussed in this study, the main issue with the enforcement of the Privacy Shield and other relevant data protection legislation in the U.S. is the lack of authority of the FTC in the context of commercial activities of the banks, airlines, the business of insurance and the common activities of telecommunication service providers and most of the non-profit organizations[978]. The privacy enforcement in the context of commercial activities of airlines is provided by the Department of Transportation[979]. However, in the memorandum of the Privacy Shield, there is no answer to the question regarding the instution that provides enforcement in the context of commercial activities of the banks, the business of insurance and the common activities of telecommunication service providers and most of the non-profit organizations. More interestingly, there is no detail regarding the exceptions to the FTC enforcement in the aforementioned areas.

In that regard, the options below should be considered by the U.S. side:

i. The exceptions to the enforcement of the FTC should be documented in great detail also, the law enforcement agencies which fill the gaps of the FTC should be provided in that document or,

---

975 EU-US NGO Letter, *supra note 46*, at 9.
976 Ibid.
977 EDPS, *supra* note 319, at 12.
978 Privacy Shield, *supra* note 42, ANNEX IV.I.A.
979 Id. ANNEX V.I.A.

ii. The FTC should be endowed with full privacy enforcement powers without exceptions or,

iii. A brand new independent data protection authority in the U.S. should be established as suggested by other authors.

8.2.6. Simplifying and Improving the Redress Options

8.2.6.1. Simplifying and Improving the Redress Options in the Context of Commercial Aspects of the Privacy Shield

Throughout this study, it is many times mentioned that, the Redress Mechanisms under the Privacy Shield are overly complex. Including the lodging a complaint in the Ombudsperson and seeking redress according to the Privacy Act of 1974, there are nine options to consider. Adding to that a convoluted document of Privacy Shield with a good number of annexes might be responsible from the low number of complaints.

By the time the Annual Review of the Privacy Shield was issued, in the context of the compliance to the Privacy Shield,

i. only seven certified companies received direct complaints from the complainants[980],

ii. only four complaints were received by the independent recourse mechanisms[981],

iii. no complaints were received by the DoC or FTC via the EU DPAs[982],

iv. only three complaints were received by the FTC directly from the complainants[983],

v. the binding arbitration mechanism were not yet operational[984].

---

[980] EUROPEAN COMMISSION, COM(2017) 611 FINAL, COMMISSION STAFF WORKING DOCUMENT ACCOMPANYING THE DOCUMENT REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL ON THE FIRST ANNUAL REVIEW OF THE FUNCTIONING OF THE EU–U.S. PRIVACY SHIELD, 13 (2017).

[981] Id. at 15.

[982] Ibid.

[983] Id. at 16.

[984] Ibid.

The table below is a simplified representation of the Privacy Shield redress avenues, excluding the redress options in the context of interference by the public authorities. In addition to the complexity, the general problem with the redress options is lack of the monetary relieves[985]. If a Privacy Shield Organization recognizes the oversight of the EU DPAs, then obtaining monetary relief is relatively simpler[986]. The individual might directly lodge a complaint in the national DPA[987]. The DPA can provide monetary relief in that case[988]. Another option would be to seek redress in the U.S. courts according to the general provisions, however, as discussed earlier, that would be cumbersome for the individual taking into account the complexities of the legal system of the U.S[989].

[985] See, Guide the EU-U.S. Privacy Shield, supra note 26, at 18 and 21.
[986] See, Ibid.
[987] Privacy Shield, *supra* note 42, ANNEX II.II.5.b.
[988] Ibid.
[989] See, Weiss & Archick, *supra* note 311, at 14.
See also, Lingjie Kong, *supra* note 935, at 455.

Table 8.1: The Privacy Shield Redress Options

Redress Option	**Monetary Relief**	**Cost**	**The Authority to Enforce the Decision**	**Prior Redress options to be exhausted**	**Notes**
Complaint handling by organizations (Recital 43-44)	None	None	None	None	
Complaint handling by IRMs (recital 45)	Possible	None	The DoC and the FTC (upon filing a complaint)	None	
Lodging a complaint in the National DPA (recital 48)	Possible	None	informal panel of DPAs	None	The organization must recognize the oversight of the DPAs
Lodging a complaint in the National DPA (recital 51)	None	None	The DoC and the FTC (upon complaint referral)	None	If the organization does not recognize the oversight of the DPAs
Challenging the DPA's decision in the national courts (recital 50)	Depends on the jurisdiction	Depends on the jurisdiction	Depends on the jurisdiction	None	
The Binding Arbitration Mechanism (recital 42)	None	None (Only attorney fees)	The Decision of the BAM has the same effect with the court decisions	All of the options above must be exhausted	Not operational yet
Filing a case in The U.S. courts (recital 59)	Possible	High Costs	Execution of the Decisions of rhe Court According to the U.S. Law	None	

As can be seen in the table, there is a vast number of redress avenues which add to the complexity. Another problem is the lack of monetary reliefs in redress

options. To overcome those problems, this option should be considered by the U.S. side: All of the Privacy Shield organizations might recognize the oversight of the EU DPAs and, a three level redress mechanism might be adopted, where the first level has two options such as resolution within the organization or through the IRM, the second level is through the DPAs where it is possible to obtain monetary relief, and the third level is lodging a complaint in the binding arbitration mechanism which also might provide monetary relief. The table 2 shows the suggested option.

Table 8.2: The Suggested Simplified and Improved Redress Options

Redress Option	**Monetary Relief**	**Cost**	**The Authority to Enforce the Decision**	**Prior Redress options to be exhausted**	**Notes**
Complaint handling by organizations	None	None	None	None	
Complaint handling by IRMs	Possible	None	The DoC and the FTC (upon filing a complaint)	None	
Lodging a complaint in the National DPA (recital 48)	Possible	None	informal panel of DPAs	None	The organization must recognize the oversight of the DPAs
The Binding Arbitration Mechanism (recital 42)	Possible	None (Only attorney's fees)	The Decision of the BAM has the same effect with the court decisions	All of the options above must be exhausted	Not operational yet

8.2.6.2. Simplifying and Improving the Redress Options in the Context of Access by the U.S. Public Authorities

Setting aside the redress options in the context of the commercial aspects of the Privacy Shield, in the context of the access by the U.S. public authorities, there are two additional redress options, such as seeking redress in the Ombudsperson Mechanism and U.S. courts.

Beginning with the Ombudsperson Mechanism, Privacy Shield Decision gives importance to the Ombudsperson mechanis[990]. However, it is found that the Ombudsperson does not have investigatory powers and independence from the executive. The report of the European Data Protection Supervisor, issued well before the Privacy Shield Decision, has a number of recommendations worthwhile to consider. According to that, the U.S. side should ensure that:

i. the Ombudsperson should report to the Congress,

ii. the decisions and recommendations of the Ombudsperson are implemented,

iii. there is effective coordination between the Ombudsperson and the Inspector General[991].

In addition to that, by the time the Annual Review of the Privacy Shield was issued, a permanent Under-Secretary[992] in the State Department was not yet appointed by President Trump[993]. Therefore, the Ombudsperson Mechanism was not operational[994]. It is still the case[995].

Since the Ombudsperson mechanism is presented as an independent mechanism, the conditions to an independent authority, according to the EU law, as set forth by the Zakharov Case of the ECtHR[996], should be satisfied. The options below should be considered by the U.S. side:

i. A permanent Ombudsperson should be appointed;

ii. The office of the Ombudsperson should be moved to another place to lessen the influence of the executive and the intelligence community;

---

[990] In the recitals from 116 to 124 Commission evaluates the Ombudsperson mechanism and finds that it is a legitimate legal remedy against interference by the public authorities. See, Privacy Shield, *supra* note 42, recitals 116-124.

[991] EDPS, *supra* note 319, at 8.

[992] The same person with the Ombudsperson.

[993] Annual review, supra note 980, at 34.

[994] Ibid.

[995] By Nov. 27, 2017.

[996] See, Roman Zakharov, *supra* note 66.
See also, Shimovolos, *supra* note 67, Malone, *supra* note 67, Leander, *supra* note 67, Huvig, *supra* note 67, Kennedy, *supra* note 69, Huvig, *supra* note 67, at para. 34, Amann, *supra note 20*, Valenzuela, *supra note 20*, Prado, *supra note 20*, Klass and Others, *supra* note 71, Weber and Saravia, *supra* note 71, Kvasnica, *supra* note 71.

iii. The functional dependence of the Ombudsperson to the executive and intelligence community should be eliminated;

iv. A tenure should be provided to the Ombudsperson analogous to the tenure of judges;

v. Bare minimum investigatory powers should be provided to the Ombudsperson to ensure that the Ombudsperson can operate independently.

Secondly, as mentioned earlier, the JRA and Privacy Act of 1974 provide EU subjects right to seek redress in the U.S. courts[997]. However, that Privacy Act of 1974 does not allow EU subjects to seek redress as effective as the U.S. residents[998]. In that regard, an amendment is recomended to the Privacy Act of 1974 to enable EU data subjects to seek redress in the U.S. courts as effective as the U.S. subjects[999].

In that connection, a reform should take place amending the Privacy Act of 1974, to ensure that EU subjects can seek redress in the U.S. courts, regarding the violations to the right to privacy and right to data protection, caused by the misconducts of the U.S. authorities, not only in relation to the law enforcement purposes, but also the public interest and national security purposes.

CONCLUSION

As stated in the Section 1, the main objectives of this thesis are to investigate the reasons for the transition from the Safe Harbour to the Privacy Shield, identify the shortcomings of the Privacy Shield that might undermine the level of adequacy of the arrangement with reference to the EU law, subsequently suggest amendments that can eliminate those shortcomings. In that regard, the thesis aimed to review the U.S. and EU data protection legal frameworks along with the Privacy Shield. In the following sections, a good number of shortcomings of the Privacy Shield were identified, and a number of improvements to those

[997] See, Haufbaer & Jung, *supra* note 152, at 3.
[998] See, O'brien & Reitman, *supra* note 801.
[999] EU-US NGO Letter, supra note 46.

shortcomings were suggested. This section presents all of the suggested improvements.

THE COMPARISON OF THE APPROACHES OF THE U.S. AND EU TO THE RIGHT TO DATA PROTECTION

The comparison of the Approaches of the U.S. and EU is critical to the overall evaluation of the thesis. After all, the emergence of the Privacy Shield as a legal instrument, which aims to bring the data protection frameworks closer, is a consequence of different legal approaches of those two sides.

The analysis in the Section 2 showed that the EU considers the right to data protection as a fundamental right that is close to negotitaions, whereas the U.S. law treats that right as if it is a consumer right. That's why the U.S. intelligence agencies operate according to different principles when it comes to surveillance of foreign elements. They are capable of abusing personal data of the individuals in foreign countries, and U.S. legal system provides limited data protection and safeguards for those individuals.

Compared to that of the EU, the U.S. has a very complex legal system where the federal laws and state laws sometimes conflict, and there is no comprehensive data protection law. Considering all these, the agreements between the U.S. and the other governments on data protection should provide easily reachable redress avenues for the subjects of the contracting country.

THE DATA PROTECTION LEVEL PROVIDED BY THE EU

After providing a comparison of two legal approaches to the right to data protection, in order to provide a ground for comparison, an overview of the data protection law of the EU is given in the Section 3. In that regard the DPD played a significant role in identification of the data protection level of the EU. The Article 25 of the DPD is found to be significant as it provides the legal grounds of evaluation of third countries to which personal data are transferred. Consequently,

the Article 25 showed that "all the circumstances surrounding" the transfer has to be taken into account to make such an evaluation.

For similar reasons, the Section 5 provided an overview of the GDPR, as it will take effect soon, on 25 May 2018. That examination showed that the GDPR is more demanding on third countries to which the data transfers are performed from the EU. Particularly, the Article 45 of the GDPR demands that the third country in question must have one or more independent supervisory authorities, administrative and judicial redress for data subjects, effective safeguards for the access of public authorities to personal data for the necessities of public security, defense, national security and criminal law, and proper rules for the onward transfers.

THE INVALIDATION OF THE SAFE HARBOUR AND EMERGENCE OF THE PRIVACY SHIELD

As the Safe Harbour was invalidated by the CJEU because it does not provide an adequate level of data protection, clearly the new framework replacing the Safe Harbor should eliminate the shortcomings of the Safe Harbour to be able to survive when it will be challenged before the CJEU. This is the reason why the Safe Harbour is reviewed in the Section 4 of this study.

According to the evaluations in the Section 4, it is concluded that the new framework should provide safeguards against the interference by the public authorities under the "national security, public interest, or law enforcement" purposes. The new framework should also provide effective recourse mechanisms for the data subjects to have legal dress in case that their rights are violated by the U.S. organizations. The Commission on the other hand, to eliminate the legal uncertainty in the future, should examine the applicable rules of the domestic law and international commitments of the U.S.

In the Section Section 6 of the thesis, an overview of the Privacy Shield framework and the Commission Decision that made it a valid framework, the Privacy Shield Decision. The Commission Adequacy Decision was critical to the

evaluation in the following sections, because the CJEU not only evaluated the Safe Harbor, but also the evaluations in the Commission Decision that validated it.

IDENTIFICATION OF THE SHORTCOMINGS OF THE PRIVACY SHIELD

To provide a comprehensive analysis, both the commercial aspects and the aspects regarding the access by the U.S. public authorities were evaluated in this thesis. In the Section 7 the focus was put on the commercial aspects and in the Section 8 on the aspects regarding the access by the U.S. public authorities respectively. In these sections doctrinal legal analysis was made and the provisions of the Privacy Shield was compared with that of the Safe Harbour, its previous version. To complement that comparison, the provisions of the Privacy Shield are also compared with the relevant provisions of the DPD, and GDPR.

In the Section 7 and Section 8, it was found that , highly likely, the CJEU will invalidate the Privacy Shield Decision as the framework does not provide an adequate level of data protection. After the identification of the shortcomings the following suggestions were made:

The Choice Principle can be updated to ensure that personal data are not processed for non-legitimate purposes. An update to the Principle can provide the time and procedures of opt-out for materially different purposes.

Under The Accountability for Onward Transfer Principle, an amendment can be made. A guideline for evaluation of level of data protection of third countries can be added to ensure that they provide aforementioned safeguards or limitations. The procedures of inspection of the contracts made under this principle should be well documented to avoid confusion.

Under the Security Principle, an amendment can be made. The forms of processing that does not exist can be added, and specific measures such as pseudonymization, encryption, regular assessment of the data systems can be integrated to the principle.

Under the Data Integrity and Purpose Limitation principle, with an amendment to the Principle the notion "not excessive in relation to the purposes" can be added removing the notion "data relevant for the processing."

Moreover, the notion "for no longer than is necessary for the purposes…" can be added removing the notion "relevant for the purposes of processing." The footnote limiting the time period of retention of data with the "expectations of a reasonable person" can be removed.

Under the Access Principle, an amendment can be made to ensure that data subjects obtain information on purposes under which their data can be processed, to whom the data is disclosed or the categories of the data processed. Exceptions to the Access Principle can be reduced or removed to broaden the right to access.
A paragraph can be added to the Access Principle regarding the Automated Decisions so that individuals will have the right to know the logic behind the processing or request reconsideration.

Since it is not clear how the FTC and DoT will conduct evaluations regarding the compliance of the self-certified organizations, additional information can be provided to ensure that compliance is periodically monitored.

Under the Supplemental Principles is *Public Record and Publicly Available Information,* the exemptions that cause the loss of control over data can be removed.

Administrative subpoenas should be subject to the judicial review by default.
In the context of access to public authorities, EU subjects should be able to seek redress in the same way the U.S. subjects do.

The improvements on the Ombudsperson mechanism should be made to ensure that the Ombudsperson would be independent and have the investigatory powers.

THE EVALUATION OF THE OTHER POSSIBLE OPTIONS

Evaluating the other possible options in the Section 9, it has been found that:

i. An extensive data localization is not a viable option because of the excessive costs that come with it;

ii. Ceasing the Privacy Shield and relying on Standard Contractual Clauses or Derogations is not a viable option since that option is not time and cost effective;
iii. Leaving the Surveillance Practices out of the scope of the Adequacy Decisions is not an option, since it would be against the respect to fundamental rights;
iv. Relying on encryption methods might be an option, however it should be accompanied with effective enforcement;
v. Establishing an independent data authority in the U.S. should be considered by the U.S. side to comply with the upcoming GDPR;
vi. The U.S. authorities should consider simplifiying and improving the Redress Options, a possible solution is given in the Table 2 in the Section 9.

THE WAY FORWARD

The most challenging part of this thesis was the low number of academic sources, since the Privacy Shield is a relatively new, one year old framework. Moreover, the literature analyzing the Safe Harbour framework is already obsolete, since the Privacy Shield brings a good number of changes via principles and letters from the U.S. side. Also, the data protection legislation in the U.S. was subject to changes. In spite of all this, this thesis provided certain suggestions of improvements that can be useful in a future update to the Privacy Shield.

There is, however still room for improvement of the analysis and subsequent suggestions of this thesis. Particularly, a comprehensive analysis of the U.S. data protection legal framework could allow identifying the conflicting laws, as some authors argue that they exist. Furthermore, such an analysis could point out a better number of improvements to the U.S. data protection legal framework.

Apart from that, an empirical analysis could be conducted to be able to provide how the EU Law is practiced in each member state. That could allow to identify the data protection level of the EU in a much better way than the legal texts do. In that way, the answer to the question, whether the data protection level of the U.S.

is essentially equivalent to the data protection provided by the EU, could be answered in a more precise way.

BIBLIOGRAPHY

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 O.J. (L 281) 31–32.

Ionna Tourkochuriti, *The Snowden Revelations, the Transatlantic Trade and Investment Partnership and the Divide between U.S.-EU in Data Privacy Protection*, 36 UALR L. REV. 161 (2014),

Joel R. Reidenberg, *Resolving Conflicting International Data Privacy Rules in Cyberspace Resolving Conflicting International Data Privacy Rules in Cyberspace*, 1315 STAN. L. REV (1999),

Paul M. Schwartz, *The EU-U.S. Privacy Collision: A Turn to Institutions and Procedures*, 126 HARV. LAW REV. 1966 (2013),

Charter of Fundamental Rights of the European Union, Dec. 7, 2000, O.J. (C 364) 1.

Consolidated version of the Treaty on the Functioning of the European Union art. 63 OJ c 326/71, art. 107 OJ c 326/91, art. 108 OJ c 326/92, Dec. 13, 2007, O.J. (C 71)

U.S. CONST. amend. IV.

Ryan Strasser, FOURTH AMENDMENT: AN OVERVIEW, https://www.law.cornell.edu/wex/fourth_amendment (last visited Dec 14, 2017).

Francesca Bignami, THE US LEGAL SYSTEM ON DATA PROTECTION IN THE FIELD OF LAW ENFORCEMENT. SAFEGUARDS, RIGHTS AND REMEDIES FOR EU CITIZENS EUROPEAN PARLIAMENT 2015–54 (2015).

Paul M. Schwartz, Daniel J. Solove, *Defining "Personal Data" in the European Union and United States*, 13 PVLR 1581 (Sept. 15 2014), reprinted at 14 World Data Protection Report 4 (Sept. 2014).

OVERVIEW OF THE PRIVACY ACT OF 1974, http://www.justice.gov/opcl/privacyactoverview2012/1974compmatch.htm (last visited Dec 14, 2017).

Franziska Boehm, *A Comparison between US and EU Data Protection Legislation for Law Enforcement*, 81 STUDY LIBE COMM. (2015)

PRIVACY SHIELD PROGRAM OVERVIEW (2017), https://www.privacyshield.gov/Program-Overview (last visited Dec 14, 2017).

EUROPEAN COMMISSION, GUIDE TO EU-U.S. PRIVACY SHIELD (2016), http://ec.europa.eu/justice/data-protection/files/eu-us_privacy_shield_guide_en.pdf (last visited Dec 14, 2017).

Digital Globalization : The New Era Of Global Flows, (2016), https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/digital-globalization-the-new-era-of-global-flows (last visited Dec 14, 2017).

RACHEL F FEFER, SHAYERAH I AKHTAR & WAYNE M MORRISON, DIGITAL TRADE AND U.S. TRADE POLICY (2017).

United States Of America, 106 (2000), https://ec.europa.eu/energy/en/topics/international-cooperation/united-states-america (last visited Dec 14, 2017).

Nora Di Loidean, *The end of Safe Harbor: implications for EU digital privacy and data protection law*, 19 J. INTERNET LAW 7–14 (2016).

Christopher Kuner, *The European Union and the Search for an International Data Protection Framework*, 2 COPYR. GRONINGEN J. INT. LAW 222–228 (2014).

Tobias Bräutigam, *The Land of Confusion: International Data Transfers between Schrems and the GDPR*, (2016).

Francois Mestre, THE UGLY TRUTH BEHIND THE PRIVACY SHIELD, https://ciolawsdotcom.wordpress.com/2016/08/21/the-ugly-truth-behind-the-privacy-shield/ (last visited Dec 14, 2017).

Gert Vermeulen, *The paper shield: on the degree of protection of the EU-US privacy shield against unnecessary or disproportionate data collection by the US intelligence and law enforcement services, Svantesson*, 4 TRANSATLANTIC DATA PRIVACY RELATIONSHIPS AS A CHALLENGE FOR DEMOCRACY 1–16.

Max Schrems, *The Privacy Shield is a Soft Update of the Safe Harbor*, 2 EUROPEAN DATA PROTECTION LAW REVIEW 148–150 (2016).

Commission Implementing Decision of 12.7.2016 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, 2016 O.J. (C 4176) 4.

EU Organizations, and US Organizations. "EU-US NGO Letter Safe Harbor." Received by Secretary Pritzker and Commissioner Jourová, *The Public Voice*, 13 Nov. 2015, thepublicvoice.org/EU-US-NGO-letter-Safe-Harbor-11-15.pdf.

Estelle Masse & Amie Stepanovich, THREE FACTS ABOUT US SURVEILLANCE THE EUROPEAN COMMISSION GETS WRONG IN PRIVACY SHIELD (2016), https://www.accessnow.org/three-facts-us-surveillance-european-commission-gets-wrong-privacy-shield/ (last visited Oct 27, 2017).

ARTICLE 29 DATA PROTECTION WORKING PARTY, EU – U.S. PRIVACY SHIELD – FIRST ANNUAL JOINT REVIEW, WP 255, 9-10 (2017).

Graham Greenleaf, *2014-2017 Update to Graham Greenleaf's Asian Data Privacy Laws - Trade and Human Rights Perspectives*, UNSW LAW RESEARCH SERIES (2017).

Gehrd Steinke, *Data privacy approaches from US and EU perspectives*, 19 TELEMAT. INFORMATICS 193 (2002).

Sherri J. Deckelboim, *Consumer Privacy on an International Scale: Conflicting Viewpoints Underlying the EU-U.S. Privacy Shield Framework and How the Framework Will Impact Privacy Advocates, National Security, and Businesses*, 48 GEO. J. INT'L L. 263 (2016).

Council of Europe, European Convention on Human Rights, 4 Nov. 1950, (as amended).

Dainel Solove, *Understanding Privacy*, 13 HARVARD UNIV. PRESS 515–530 (2008).

Nora Ni Loideain, *EU Law and Mass Internet Metadata Surveillance in the Post-Snowden Era*, 3 MEDIA COMMUN. 53 (2015).

THE COURT IN BRIEF, http://www.echr.coe.int/Documents/Court_in_brief_ENG.pdf (last visited Dec 15, 2017).

PRESS RESOURCES - FACTSHEETS, COUNTRY PROFILES, http://www.echr.coe.int/Pages/home.aspx?p=press%2Ffactsheets&c=#n1347951547702_pointer (last visited Dec 15, 2017).

EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS, SURVEILLANCE BY INTELLIGENCE SERVICES: FUNDAMENTAL RIGHTS SAFEGUARDS AND REMEDIES IN THE EU VOLUME I: MEMBER STATES' LEGAL FRAMEWORKS, (2015).

SURVEILLANCE BY INTELLIGENCE SERVICES: FUNDAMENTAL RIGHTS SAFEGUARDS AND REMEDIES IN THE EU VOLUME II: MEMBER STATES' LEGAL FRAMEWORKS, (2015).

CETS 108: Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Jan. 1, 1981.

WJ MAXWELL, CAHIER DE PROSPECTIVE THE FUTURES OF PRIVACY FOUNDATION TELECOM, INSTITUT MINES-TELECOM (2014), https://www.fondation-mines-telecom.org/wp-content/uploads/2016/01/2014-The-Futures-of-Privacy-.pdf#page=56 (last visited Dec 10, 2017).

FULL LIST, https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures?p_auth=wKGN72rz (last visited Nov 7, 2017).

The Venice Commission of the Council of Europe, VENICE COMMISSION, http://www.venice.coe.int/WebForms/pages/?p=01_Presentation&lang=EN (last visited Nov 7, 2017).

EUROPEAN COMMISSION FOR DEMOCRACY THROUGH LAW (VENICE COMMISSION), REPORT ON THE DEMOCRATIC OVERSIGHT OF THE SECURITY SERVICES ADOPTED, para. 252 (2007).

EUROPEAN COMMISSION FOR DEMOCRACY THROUGH LAW (VENICE COMMISSION), UPDATE OF THE 2007 REPORT ON THE DEMOCRATIC OVERSIGHT OF THE SECURITY SERVICES AND REPORT ON THE DEMOCRATIC OVERSIGHT OF SIGNALS INTELLIGENCE AGENCIES, (2015).

European Union, THE HISTORY OF THE EUROPEAN UNION (2017), https://europa.eu/european-union/about-eu/history_en (last visited Nov 6, 2017).

See, European Parliament, FACT SHEETS ON THE EUROPEAN UNION, SOURCES AND SCOPE OF EUROPEAN http://www.europarl.europa.eu/atyourservice/en/displayFtu.html?ftuId=FTU_1.2.1.html (last visited Nov 10, 2017).

Richard J Peltz-Steele, *The pond betwixt: Differences in the US-EU data protection/safe harbor negotiation*, 19 J. INTERNET LAW 1–30 (2015),

Patrick G. Crago, *Fundamental Rights on the Infobahn : Regulating the Delivery of Internet Related Services Within the European*, 20 HAST. INT'L COMP. L. REV. 467 (1997).

SOURCES AND SCOPE OF EUROPEAN UNION LAW, http://www.europarl.europa.eu/atyourservice/en/displayFtu.html?ftuId=FTU_1.2.1.html (last visited Nov 10, 2017).

HOME PAGE OF EU GDPR, http://www.eugdpr.org/ (last visited Nov 11, 2017).

EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS AND THE COUNCIL OF EUROPE, HANDBOOK ON EUROPEAN DATA PROTECTION LAW (2014).

İKBAL GÜR, KIŞISEL VERILERIN KORUNMASI HUSUSUNDA AB ILE ABD ARASINDA ÇIKAN UYUŞMAZLIKLAR VE ÇÖZÜM YOLLARI, 138 (2010).

Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. LAW REV. 193–220 (1890).

Daniel J. Solove, *Understanding Privacy*, 13 HARVARD UNIV. PRESS 515–530 (2008).

Ieuan Jolly, DATA PROTECTION IN THE UNITED STATES: OVERVIEW, https://uk.practicallaw.thomsonreuters.com/6-502-0467?transitionType=Default&contextData=(sc.Default)&firstPage=true&bhcp=1, (last visited Nov 11, 2017).

Sherri J. Deckelbolm, *Consumer Privacy on an International Scale: Conflicting Viewpoints Underlying the EU-U.S. Privacy Shield Framework and How the Framework Will Impact Privacy Advocates, National Security, and Businesses*, 48 GEO. J. INT'L L. 263 (2016).

CAMERON F. KERRY ET AL., ESSENTIALLY EQUIVALENT: A COMPARISON OF THE LEGAL ORDERS FOR PRIVACY AND DATA PROTECTION IN THE EUROPEAN UNION AND UNITED STATES (2016).

Michelle Frasher, *Adequacy versus equivalency: Financial data protection and the U.S.-EU divide*, 56 BUS. HORIZ. 787–795 (2013).

Stephen Hinde, *Privacy legislation: A comparison of the US and European approaches*, 22 COMPUT. SECUR. 378–387 (2003).

GARY CLYDE HUFBAUER & EUIJIN JUNG, PB 16-12 THE US-EU PRIVACY SHIELD PACT : A WORK IN PROGRESS (2016).

SHARA MONTELEONE & LAURA PUCCIO, FROM SAFE HARBOUR TO PRIVACY SHIELD, (2017).

PRESIDENTIAL POLICY DIRECTIVE - SIGNALS INTELLIGENCE ACTIVITIES (2014), https://obamawhitehouse.archives.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities (last visited Dec 17, 2017).

EXECUTIVE ORDERS, https://www.archives.gov/federal-register/codification/executive-order/12333.html (last visited Dec 17, 2017).

MARK BRENNAN, BRET COHEN & VICTORIA HORDERN, LEGAL ANALYSIS OF THE EU-U.S. PRIVACY SHIELD, (2016).

Paul M. Schwartz & Danie J. Solove, *Reconciling Personal Information in the United States and European Union*, 102 SSRN ELECTRON. J. 877–916 (2013).

ARTICLE 29 DATA PROTECTION WORKING PARTY, EU – U.S. PRIVACY SHIELD – FIRST ANNUAL JOINT REVIEW, (2017).

RACHEL F FEFER, SHAYERAH I AKHTAR & WAYNE M MORRISON, DIGITAL TRADE AND U.S. TRADE POLICY, (2017).

Gerhard Steinke, *Data privacy approaches from US and EU perspectives*, 19 TELEMAT. INFORMATICS 193 (2002).

2000/520/EC: Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council 2441) on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions, O.J. (L 215) (2000).

EUROPEAN COMMISSION, COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL ON THE FUNCTIONING OF THE SAFE HARBOUR FROM THE PERSPECTIVE OF EU CITIZENS AND COMPANIES ESTABLISHED IN THE EU (2013).

FORTUNE 500 TECHNOLOGY COMPANIES | FORTUNE, http://fortune.com/2016/06/07/fortune-500-technology-companies/ (last visited Dec 18, 2017).

Mira Burri & Rahel Schär, *The Reform of the EU Data Protection Framework: Outlining Key Changes and Assessing Their Fitness for a Data-Driven Economy*, 6 J. INF. POLICY 479 (2016).

Stephanie Hare, *For your eyes only: U.S. technology companies, sovereign states, and the battle over data protection*, 59 BUS. HORIZ. 549–561 (2016).

Christopher Kuner, *Reality and Illusion in EU Data Transfer Regulation Post Schrems*, 18 GER. L.J. 881 (2017).

EUROPA - COURT OF JUSTICE OF THE EUROPEAN UNION (2014), Https://Europa.Eu/European-Union/About-Eu/Institutions-Bodies/Court-Justice_En (Last Visited Dec 18, 2017).

SHARA MONTELEONE & LAURA PUCCIO, FROM SAFE HARBOUR TO PRIVACY SHIELD, 6 (2017).

EUROPEAN COMMISSION, COM(2013) 846: COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL ON THE FUNCTIONING OF THE SAFE HARBOUR FROM THE PERSPECTIVE OF EU CITIZENS AND COMPANIES ESTABLISHED IN THE EU (Nov. 27, 2013)

SAFE HARBOR DATA PRIVACY BRIEFING: YOUR QUESTIONS ANSWERED BY GIOVANNI BUTTARELLI | INSIGHTS | SIDLEY AUSTIN LLP, https://www.sidley.com/en/insights/events/2015/10/safe-harbor-briefing-your-questions-answered-10-20 (last visited Dec 19, 2017).

MARTIN A WEISS & KRISTIN ARCHICK, U .S.-EU DATA PRIVACY : FROM SAFE HARBOR TO PRIVACY SHIELD (2016).

Press Release Issued by the Article 29 Data Protection Working Party, (Oct. 6, 2015), http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2015/20151006_wp29_press_release_on_safe_harbor.pdf (last visited Dec 19, 2017).

MODEL CONTRACTS FOR THE TRANSFER OF PERSONAL DATA TO THIRD COUNTRIES - EUROPEAN COMMISSION, http://ec.europa.eu/justice/data-protection/international-transfers/transfer/index_en.htm (last visited Dec 19, 2017).

ARTICLE 29 WORKING PARTY, WORKING DOCUMENT ON A COMMON INTERPRETATION OF ARTICLE 26(1) OF DIRECTIVE 95/46/EC OF 24 OCTOBER 1995 (2005).

THE EUROPEAN DATA PROTECTION SUPERVISOR, OPINION 4/2016: OPINION ON THE EU-U.S. PRIVACY SHIELD DRAFT ADEQUACY DECISION, (2016).

Jan P. Albrecht, *How the GDPR Will Change the World*, 2 EUR. DATA PROT. LAW REV. 287–289 (2016), at 287.

Bert-Jaap Koops & Ronald Leenes, *International Review of Law, Computers & Technology Privacy regulation cannot be hardcoded. A critical comment on the "privacy by design" provision in data-protection law Privacy regulation cannot be hardcoded. A critical comment on the 'privacy by de*, 28 INT. REV. LAW, COMPUT. TECHNOL. 159 (2017).

PROTECTION OF PERSONAL DATA, http://ec.europa.eu/justice/data-protection/ (last visited Dec 19, 2017).

KEY CHANGES WITH THE GENERAL DATA PROTECTION REGULATION, http://www.eugdpr.org/key-changes.html (last visited Nov 18, 2017).

ARTICLE 29 DATA PROTECTION WORKING PARTY, OPINION 01/2016 ON THE EU–U.S. PRIVACY SHIELD DRAFT ADEQUACY DECISION WORKING PARTY OPINIONS (2016).

Ioanna Tourkochoriti, *The Transatlantic Flow Of Data And The National Security Exception In The European Data Privacy Regulation : In Search For Legal Protection Against Surveillance Europe Regulates Data Privacy Against Violations Coming From The Private Sector More Strictly,* U. Pa. J. Int'l L. 459 (2015),

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, O.J. (L 119/1) (2016).

Melissa Ryan, *Navigating Privacy In A Sea Of Change*, INTERN. AUDIT. 68–69 (2017).

See, ELENI KOSTA, NADEZHDA PURTOVA & COLETTE CUJIPERS, DATA PROTECTION REFORM AND THE INTERNET : THE DRAFT DATA PROTECTION REGULATION TILBURG LAW SCHOOL LEGAL STUDIES RESEARCH PAPER SERIES, No:03/2014.

Leena Salolatva, *Privacy Shield Redress Mechanisms Assessment in the Light of the Schrems Case*, 2017.
WHO DOES THE EU GDPR APPLY TO?, https://www.varonis.com/learn/who-does-gdpr-apply-to/ (last visited Nov 18, 2017).

Michael Colesky, Sepideh Ghanavati Digital, *Privacy shielding by design - A strategies case for near-compliance*, *in* PROCEEDINGS - 2016 IEEE 24TH INTERNATIONAL REQUIREMENTS ENGINEERING CONFERENCE WORKSHOPS, REW 2016 271–275 (2017).

Directive 2000/31/EC of The European Parliament and of the Council of 8 June 2000 on Certain Legal Aspects of Information Society Services, in Particular Electronic Commerce, in The Internal Market (Directive on electronic commerce), O.J. (L 178/1) (2000).

COUNCIL OF EUROPE, COMMITTEE OF MINISTERS, RECOMMENDATION REC(97)5 TO MEMBER STATES ON THE PROTECTION OF MEDICAL DATA (13 February 1997).

Felix Bieker, *Enforcing data protection law - The role of the supervisory authorities in theory and practice*, 498 *in* IFIP ADVANCES IN INFORMATION AND COMMUNICATION TECHNOLOGY 125–139 (2016).

THE EUROPEAN DATA PROTECTION SUPERVISOR, OPINION 4/2016: OPINION ON THE EU-U.S. PRIVACY SHIELD DRAFT ADEQUACY DECISION (2016).

EUROPEAN COMMISSION, COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL TRANSATLANTIC DATA FLOWS: RESTORING TRUST THROUGH STRONG SAFEGUARDS, COM(2016) 117, 8 (Feb. 29, 2016).

Jan P. Albrecht, *How the GDPR Will Change the World*, 2 EUR. DATA PROT. LAW REV. 287–289 (2016).

Gerrit Hornung, *Regulating privacy enhancing technologies: seizing the opportunity of the future European Data Protection Framework*, 26 EUR. J. SOC. SCI. RES. 1351–16101 (2017).

Francois Mestre, THE UGLY TRUTH BEHIND THE PRIVACY SHIELD, https://ciolawsdotcom.wordpress.com/2016/08/21/the-ugly-truth-behind-the-privacy-shield/ (last visited Dec 14, 2017).

Roderick B. Mathews & Juan Carlos Botero, *Access to Justice in the United States*, 59 VIRGINIA LAWYER 24–25 (2010).

Martin A. Weiss & Kristin Archick, U.S.-EU Data Privacy: From Safe Harbor to Privacy Shield (2016).

Danny O'brien & Rainey Reitman, THE PRIVACY SHIELD IS RIDDLED WITH SURVEILLANCE HOLES | ELECTRONIC FRONTIER FOUNDATION (2016), https://www.eff.org/deeplinks/2016/03/privacy-shield-riddled-surveillance-holes (last visited Dec 24, 2017).

GARY CLYDE HUFBAUER & EUIJIN JUNG, PB 16-12 THE US-EU PRIVACY SHIELD PACT : A WORK IN PROGRESS (2016), at 5.

Shedding Light on the Foreign Intelligence Surveillance Court (FISC): Court Findings from Our 2007-2008 Case, https://yahoopolicy.tumblr.com/post/97238899258/shedding-light-on-the-foreign-intelligence (last visited Dec 24, 2017).

Gert Vermeulen, *The paper shield: on the degree of protection of the EU-US privacy shield against unnecessary or disproportionate data collection by the US intelligence and law enforcement services* (2016).

Xavier Tracol, *EU–U.S. Privacy Shield: The saga continues*, 32 COMPUT. LAW SECUR. REV. 775–777 (2016).

Peter Margulies, *Global Cybersecurity, Surveillance, and Privacy: The Obama Administration's Conflicted Legacy* (2017).

Estelle Masse & Amie Stepanovich, THREE FACTS ABOUT US SURVEILLANCE THE EUROPEAN COMMISSION GETS WRONG IN PRIVACY SHIELD - ACCESS NOW, https://www.accessnow.org/three-facts-us-surveillance-european-commission-gets-wrong-privacy-shield/ (last visited Dec 24, 2017).

Elspeth Guild, Didier Bigo & Sergio Carrera, *Harvesting personal data and requiem for the EU-US Privacy Shield* (2017).

Anastasia Agamalova & Ksenia Boletskaya, Roskomnadzor prigrozil Facebook blokirovkoi Vedomosti (2017), http://rodina.news/roskomnadzor-prigrozil-facebook-blokirovkoi-2018-godu-17092614153034.htm (last visited Dec 14, 2017).

Nicola Lucchi, *Access to network services and protection of constitutional rights: Recognising the essential role of internet access for the freedom of expression*, 19 CARDOZO J. INT. COMP. LAW 645–678 (2011).

W. Gregory Voss, *The Future of Transatlantic Data Flows: Privacy Shield or Bust?*, 19 J. INTERNET LAW 1 (2016).

Lingjie Kong, *Data Protection and Transborder Data Flow in the European and Global Context*, 21 EUR. J. INT. LAW EJIL 441–456 (2010).

WORKING PARTY ON THE PROTECTION OF INDIVIDUALS & WITH REGARD TO THE PROCESSING OF PERSONAL DATA, TRANSFERS OF PERSONAL DATA TO THIRD COUNTRIES : APPLYING ARTICLES 25 AND 26 OF THE EU DATA PROTECTION DIRECTIVE (1998).

Jens Henrik Jeppesen, CJEU GENERAL ADVOCATE OPINION IN SCHREMS CASE A WAKE-UP CALL | CENTER FOR DEMOCRACY & TECHNOLOGY, https://cdt.org/blog/cjeu-general-advocate-opinion-in-schrems-case-a-wake-up-call/ (last visited Dec 24, 2017).

Paul de Hert & Vagelis Papakonstantinou, *The new General Data Protection Regulation: Still a sound system for the protection of individuals?*, 32 COMPUT. LAW SECUR. REV. 179–194 (2016).

Shannon Gross, *A Mystery Wrapped in an Encryption : Surveillance and Privacy in the Encrypted Era in the Encrypted Era*, 15 NW. J. TECH. INTELL. PROP. 73 (2017).

EUROPEAN COMMISSION, COM(2017) 611 FINAL, COMMISSION STAFF WORKING DOCUMENT ACCOMPANYING THE DOCUMENT REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL ON THE FIRST ANNUAL REVIEW OF THE FUNCTIONING OF THE EU–U.S. PRIVACY SHIELD (2017).

COURT CASES

Amann v. Switzerland, No. 27798/95, (ECtHR, Feb. 16, 2000).

Roman Zakharov v. Russia, No. 47143/06, (ECtHR, Dec. 4, 2015).

Shimovolos v. Russia, No. 30194/09, (ECtHR, June 21, 2011).

Malone v. the United Kingdom, Series A no. 82, (ECtHR, Aug. 2, 1984).

Leander v. Sweden, Series A no. 116, (ECtHR, Mar. 26, 1987).

Huvig v. France, Series A no. 176-B, (ECtHR, Apr. 24, 1990).

Kennedy, v. the United Kingdom, No. 26839/05, (ECtHR, May 18, 2010).

Valenzuela Contreras v. Spain, no. 27671/95, (ECtHR, Jul. 30, 1998).

Prado Bugallo v. Spain, no. 58496/00, (ECtHR, Feb. 18, 2003).

Klass and Others v. Germany, Series A no. 28, (ECtHR, Sep. 6, 1978).

Weber and Saravia v. Germany, No. 54934/00, (ECtHR, June 29, 2006).

Kvasnica v. Slovakia, no.72094/01, (ECtHR, Jun. 9, 2009).

Maximillian Schrems v. Data Protection Commissioner, C-362/14, (CJEU Oct. 6, 2015).

Olmstead v. United States 277 U.S. 438 (1928).

Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, Case C-131/12 (May 13, 2014, CJEU).

Digital Rights Ireland v. Commission, C. T-670/16, (2016, CJEU).

La Quadrature du Net and Others v. Commission, C. T-738/16, (2017, CJEU).

Digital Rights Ireland and Seitlinger and Others, Joined Cases C-293/12 and C-594/12 (CJEU, Apr. 8, 2014).

Yahoo v. United States, No.08-01. (May 29, 2008, FISC).

James R. Clapper, Jr., Director of National Intelligence, et al., Petitioners v. Amnesty International USA, et al. 568 U.S. 398 (February 26, 2013), I.

Yassin Abdullah Kadi and Al Barakaat International Foundation v. Council of the European Union and Commission of the European Communities, C-402/05 P, (Sep. 3, 2008, CJEU).

STATUTES

15 U.S.C. §§7701-7713.

18 U.S.C. §§1037.

47 U.S.C. §227.

18 U.S.C. §2510.

18 U.S.C. §1030.

15 U.S.C. §§41-58.

15 U.S.C. § 57.

15 U.S.C. § 45.

49 U.S.C. § 41712.

Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008, H.R. 6304.

USA FREEDOM Act of 2015, Pub. L. No 114-23, § 401, 129 Stat. 268.