The EU-US Privacy Shield
An insufficient level of data protection under EU Fundamental Rights Standards

Antonia Lantz

Thesis in Examensarbete, 30 HE credits
Examiner: Cecilia Magnusson Sjöberg
Stockholm, Autumn term 2016
Abstract
Because of its deep commitment to the protection of human rights, the EU affords a very high level of protection to the personal data of its citizens. This protection also plays an important role in light of the right to respect of private life, also enshrined in the EU. The European Commission decided, after negotiations with the US, on a framework called the EU-US Privacy Shield. This framework will legitimate data flows between the EU and the US and protect the EU citizens’ data, and thus their privacy. The Privacy Shield contains general principles that organizations in the US must adhere to, as well as a summary of the US law that will be applicable to and protect the EU-citizens. The framework sets out the various mechanisms through which the US authorities will ensure effective legal protection.

The Commission must, when making a decision like the Privacy Shield Decision, find and decide that the US, by reason of its domestic law or its international commitments, ensures a level of protection that is “essentially equivalent” to that ensured in the EU. In this thesis, the central question explored is whether the US provides for such a level of data protection and further whether the Privacy Shield would withstand scrutiny in the Court of Justice of the European Union. The ones that are about to transfer personal data to the US need to get an answer to whether they can rely on the Privacy Shield Decision, or if they should rely on alternative existing data transfer mechanisms instead.

The conclusion that will be presented in the thesis is that there are several reasons to be critical of the EU-US Privacy Shield. The conclusion is logically based on the fact that the Commission has not made an assessment of the protection provided in the US that is sufficient to state that the protection is “essentially equivalent” to the protection guaranteed within the EU legal order. The regulations in the US are spread out in different types of regulations. The regulations contain many limitations and exceptions to the protection which is why it is difficult to determine the scope of the protection in advance. It is therefore necessary that the Commission analyzes the actual level of protection taking these limitations and exceptions into consideration. Some kind of guarantee that the EU is informed of all regulations that might have an effect on the EU citizens’ data protection is needed.

Further, the effective exercise of the data subject’s fundamental rights might be undermined because of the complexity and the lack of clarity of the Privacy Shield Framework, and it seems like EU-citizens will have limited access to redress mechanisms in the US. The im-
Improvements made in the US since the invalidity of the previous adequacy decision does not seem to be sufficient, and what impact the new administration will have on these improvements, as well as the Privacy Shield in general, is not clear. In addition, the Privacy Shield Principles will have to get modified before the new data protection regulation will enter into application in the EU year 2018.
1 ABBREVIATIONS.................................................................................................................. 6

2 INTRODUCTION .................................................................................................................. 7
  2.1 BACKGROUND AND PURPOSE................................................................................. 7
  2.2 SUBJECT ....................................................................................................................... 8
  2.3 DELIMITATIONS......................................................................................................... 8
  2.4 MATERIAL AND METHOD......................................................................................... 9
  2.5 DISPOSITION/OUTLINE .............................................................................................. 11

3 CRITERIA FOR LEGAL TRANSFERS OF DATA UNDER THE EU REGULATION... 12
  3.1 THE CHARTER OF FUNDAMENTAL HUMAN RIGHTS ........................................... 12
  3.2 THE EU DATA PROTECTION REFORM .................................................................. 12
    3.2.1 The Regulation .................................................................................................. 13
    3.2.1.1 Stronger enforcement of data protection rules ............................................. 13
    3.2.1.2 Adequacy decisions by the Commission .................................................. 14
    3.2.1.3 Alternative existing data transfer mechanisms ......................................... 15
      3.2.1.3.1 Binding corporate rules ................................................................. 15
      3.2.1.3.2 Contractual clauses ................................................................. 16
      3.2.1.3.3 Approved codes of conduct and approved certification mechanisms .......... 16
      3.2.1.3.4 Derogations ............................................................................. 17
  3.3 THE SAFE HARBOR SCHEME AND ITS INVALIDITY – A LESSON TO LEARN? .... 17
    4.1 MR. SCHREMS V. DATA PROTECTION COMMISSIONER .................................... 17
      4.1.1 Introduction ..................................................................................................... 17
        4.1.1.1 Edward Snowden revelations .................................................................. 18
      4.1.2 Is the DPA absolutely bound by a European Commission Decision? ........ 18
      4.1.3 Annullment of the Safe Harbor Decision ..................................................... 19
        4.1.3.1 “Essentially equivalent” ........................................................................ 20
        4.1.3.2 Protection of fundamental rights ......................................................... 20
        4.1.3.2.1 EU legislation involving interference with the fundamental rights .......... 21
        4.1.3.2.2 Access to personal data by the US Government ................................ 22
        4.1.3.2.3 Legal protection ............................................................................. 22
        4.1.3.2.4 Periodically check ........................................................................... 23
  4 EU-US PRIVACY SHIELD – A STRENGTHENED FRAMEWORK? ............................... 23
    5.1 TRANSPARENCY ...................................................................................................... 24
    5.2 PRIVACY SHIELD PRINCIPLES ............................................................................ 26
      5.2.1 Choice Principle ............................................................................................... 26
      5.2.2 Security Principle and Data Integrity and Purpose Limitation Principle ........ 27
      5.2.3 Notice Principle and Access Principle ............................................................ 28
      5.2.4 Recourse, Enforcement and Liability Principle ............................................ 29
      5.2.5 Accountability for Onward Transfer Principle .............................................. 31
    5.3 NON-COMPLIANCE WITH THE PRINCIPLES .................................................... 31
      5.3.1 Complaint handling within the organization ................................................. 31
      5.3.2 Independent dispute resolution body ............................................................ 32
      5.3.3 National data protection authority ................................................................. 32
      5.3.4 US Department of Commerce ....................................................................... 33
      5.3.5 US Federal Trade Commission .................................................................... 33
      5.3.6 Privacy Shield Panel ..................................................................................... 35
    5.4 DEROGATIONS FROM THE PRINCIPLES ........................................................... 36
    5.5 ACCESS BY US PUBLIC AUTHORITIES ............................................................... 36
      5.5.1 National security ............................................................................................. 37
        5.5.1.1 Presidential Policy Directive 28 ............................................................. 38
        5.5.1.2 Foreign Intelligence Act – Section 702 .................................................. 39
        5.5.1.3 National security letter statutory provisions ........................................... 40
        5.5.1.4 Freedom Act ....................................................................................... 40
      5.5.2 Law enforcement and public interest purposes .............................................. 41
      5.5.3 Effective legal protection ................................................................................. 42
        5.5.3.1 National security area ............................................................................ 43
          5.5.3.1.1 Oversight ...................................................................................... 43
          5.5.3.1.2 Individual redress ........................................................................ 44
6 SCRUTINY BY THE CJEU AND GENERAL CONCLUSIONS

6.1 ESSENTIALLY EQUIVALENT? ................................................................. 49
   6.1.1 Transparency .............................................................................. 50
   6.1.2 Derogations from the Principles .................................................. 50
   6.1.3 Access by US public authorities ................................................... 51
       6.1.3.1 National security area .......................................................... 52
       6.1.3.2 Law enforcement and public interest ........................................ 53
   6.1.4 Redress mechanisms, complaint handling and enforcement ............. 54
       6.1.4.1 If non-compliance with the Principles ...................................... 54
       6.1.4.2 If unlawful access by the public authorities ............................ 55
       6.1.4.3 Need for a DPA in the US ..................................................... 56
   6.1.5 The legal status of the Annexes .................................................... 58
   6.1.6 Need to modify the Privacy Shield Framework? ............................... 59
       6.1.6.1 The Privacy Shield Principles ................................................. 59
       6.1.7 The qualified guess ................................................................. 60

7 TABLE OF CASES .................................................................................. 63
   7.1 CJEU ............................................................................................ 63
   7.2 ECtHR ........................................................................................... 64
   7.3 United States of America ............................................................... 64

8 TABLE OF STATUTES AND CONVENTIONS ........................................ 64
   8.1 The United States of America ....................................................... 64
   8.2 European Union ...................................................................... 65
   8.3 Argentina .................................................................................... 65
   8.4 Canada ....................................................................................... 65
   8.5 Switzerland .................................................................................. 65
   8.6 The European Commission Documents ......................................... 66

9 OTHER DOCUMENTS ........................................................................... 67

10 BIBLIOGRAPHY .................................................................................. 67

11 WEB MATERIAL .................................................................................. 67

12 JOURNALS .......................................................................................... 69
1 Abbreviations

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Full Form</th>
</tr>
</thead>
<tbody>
<tr>
<td>CJEU</td>
<td>Court of Justice of the European Union</td>
</tr>
<tr>
<td>DoC</td>
<td>US Department of Commerce</td>
</tr>
<tr>
<td>DPA</td>
<td>Data Protection Authority</td>
</tr>
<tr>
<td>FADAP</td>
<td>The Federal Act of Data Protection</td>
</tr>
<tr>
<td>FAQ</td>
<td>Frequently Asked Questions</td>
</tr>
<tr>
<td>FBI</td>
<td>Federal Bureau of Investigation</td>
</tr>
<tr>
<td>FISA</td>
<td>Foreign Intelligence Surveillance Act</td>
</tr>
<tr>
<td>FISC</td>
<td>Foreign Intelligence Surveillance Court</td>
</tr>
<tr>
<td>FISCR</td>
<td>Foreign Intelligence Surveillance Review</td>
</tr>
<tr>
<td>FOIA</td>
<td>Freedom of Information Act</td>
</tr>
<tr>
<td>FTC</td>
<td>US Federal Trade Commission</td>
</tr>
<tr>
<td>GDPR</td>
<td>General Data Protection Regulation</td>
</tr>
<tr>
<td>NIPF</td>
<td>National Intelligence Priorities Framework</td>
</tr>
<tr>
<td>NSA</td>
<td>US National Security Agency</td>
</tr>
<tr>
<td>NSL</td>
<td>National Security Letter</td>
</tr>
<tr>
<td>PCLOB</td>
<td>Privacy and Civil Liberties Oversight Board</td>
</tr>
<tr>
<td>PD</td>
<td>Personal Data</td>
</tr>
<tr>
<td>PPD</td>
<td>Presidential Policy Directive</td>
</tr>
<tr>
<td>PIPEDA</td>
<td>Personal Information Protection and Electronic Documents Act</td>
</tr>
<tr>
<td>TEU</td>
<td>Treaty on European Union</td>
</tr>
<tr>
<td>TFEU</td>
<td>Treaty on the Functioning of the European Union</td>
</tr>
<tr>
<td>US</td>
<td>United States of America</td>
</tr>
</tbody>
</table>
2 Introduction

2.1 Background and purpose

A constant challenge for the European Union (hereafter: the EU) is to guarantee the fundamental right to data protection in relation to new technologies and services. The EU needs to find a balance between the fundamental rights of personal data protection and the policy objective of promoting innovation within society. In other words, the fundamental challenge is to make the EU market attractive, without giving up on the high level of data protection that is afforded to European citizens.

Global data flows are part of the modern communications, as well as of the everyday commercial and social interactions. The Decision 2000/520/EC of 26 July 2000 (hereafter: The Safe Harbor) was adopted by the European Commission (hereafter: The Commission) in order to legitimate data flows between the EU and the United States (hereafter: the US). The Court of Justice of the European Union (hereafter: CJEU) determined this scheme invalid in 2015 since it believed it was an unsatisfactory tool for EU-US data transfers. Alternative tools authorizing data flows from the EU could still be used by companies when transferring data to the US, even though their validity has been questioned as well. Hence the decision to invalidate the Safe Harbor Scheme resulted in an upheaval and uncertainty for businesses that transfer personal data to the US on a regular basis.1 However, the Commission and the US agreed on a new framework in 2016, the so called EU-US Privacy Shield.

A new regulation in the EU about protection of natural persons with regard to the processing of personal data, but also the free movement of such data, will enter into application 25 May 2018. Since the data protection requirements will be further restricted, and new requirements will be introduced, it is not only of crucial importance for all companies in the EU and the US that the reliability of the new agreement is determined in the light of the current regulation, but also in the light of the applicable regulation in 2018 when the new regulation has entered into application. This must be done before personal data is transferred to the US under the Privacy Shield. The affected companies need an answer about whether they can fully depend upon the Privacy Shield or whether other alternatives such as Binding Corporate Rules (hereafter: BCR) or Model Clauses are more reliable. The aim of this thesis is to make a qualified guess of whether the CJEU, in the light of this new General Data Protection Regulation, the

1 Deighton, The EU-US Privacy Shield – is it strong enough?
Charter of Fundamental Human Rights and the criteria laid out by the CJEU in its case law, would uphold the validity of the EU-US Privacy Shield in the likely event the Court is asked to examine it.

2.2 Subject

The fundamental right to protection of personal data plays an important role in the light of the fundamental right to respect for private life enshrined in the Charter of Fundamental Rights of the European Union (hereafter: the Charter). The right to data protection is highly valued in the EU and the requirements on such protection will be extended with the introduction of a new regulation governing data protection within the EU. The questions to be answered and thus the central research in this thesis are: Does the EU-US Privacy Shield provide for a level of data protection in the US that is “essentially equivalent” to that of the EU? Or are other alternatives more reliable?

2.3 Delimitations

The specific laws in the US will not be described exhaustively if not necessary. The aim of the thesis is not to describe and investigate the US legal system in detail. Rather, the aim is to get a fair understanding of the relevant legislation in the US in order to be able to follow the assessment of the adequacy of the level of protection made by the Commission and thus be able to answer the central research. The national regulations in the Member States regulating data protection will not be described at all, e.g. the Swedish Personal Data Act (1998:204) (sw: Personuppgiftslag 1998:204). The thesis will be kept on a EU level since the agreement is between the EU and the US. The Privacy Shield Decision will have the same effect in every Member State. The national regulations in the Member States are therefore not relevant for the central research.

The differences between the processing of different kinds of data, e.g. human resources data or data about pharmaceutical and medical products will not be described. This in order to keep the thesis on a general level and to be able to cover all the fundamental areas and issues. Hence, the Directive (EU) 2016/680 of the European Parliament and the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of
such data, and repealing Council Framework Decision 2008/977/JHA (hereafter: The Police and Criminal Justice Authority Directive) will not be investigated at all. The difference between the controller and the processor will not be described in detail either since it is not necessary to determine the split of the responsibilities between these two entities in order to answer the central research questions.

2.4 Material and Method

A legal dogmatic methodology will be applied in this thesis. The thesis will therefore emanate from a concrete and formulated problem, in this case the unclarity around whether the EU-US Privacy Shield Decision fulfill the requirements set out in the law as it exists (de lage lata). Therefore, as an initial step, the law as it exists needs to be determined; to be described, and systemized.²

As is characteristically for the legal dogmatic methodology, the relevant questions in the thesis will be answered by an analysis of the law as it exists, even though the method does not prevent a broader perspective.³ The legal dogmatic methodology can be used to criticize or critically review the result of the analysis of the law as it exists, e.g. through arguments that are based on the purpose of the law.⁴ This will be done in this thesis. To do this, the purpose of the regulation needs to be determined, as well as the criteria of relevance that will be crucial for the legal analysis.⁵ Further, the probable function of the Privacy Shield in practice must be investigated in order to determine whether the Privacy Shield is formulated in an appropriate way in order to meet the intended purpose.

The traditional sources like the General Data Protection Regulation, as well as the Data Protection Directive, US regulations and EU and US case law, will be used and valued together.⁶ The wording of the traditional sources is relevant for the interpretation of it, but also the context and the purpose behind it.⁷ However, the traditional sources will not be sufficient enough to answer the questions presented above. Soft law, with an authoritative position within the EU legal order, as well as commitments from US authorities and recommendation by the Pri-

---

² Korling, Zamboni, Juridisk Metodlära, p. 23f.
³ Jareborg, Rättsdogmatik som vetenskap, p. 4.
⁴ Korling, Zamboni, Juridisk Metodlära (1.3 u.), p 35.
⁵ Korling, Zamboni, Juridisk Metodlära (1.3 u.), p. 36.
⁶ Sandgren, Rättsvetenskap för uppsatsförfattare, p. 43f.
vacy and Civil Liberties Oversight Board in the US (hereafter: the PCLOB) etc., will therefore also be used in addition to the traditional sources.\(^8\) EU soft law contains guidelines and codes issued by EU bodies to facilitate an effective impact of the EU regulations in the Member States.\(^9\) The soft law serves as ground for interpretation of the EU regulation.\(^10\) The soft law that will influence the analysis in this thesis are decisions from the EU Commission and statements from and opinions of the Article 29 Data Protection Working Party (hereafter: Article 29 Working Party).

The EU soft law, as well as the commitments and recommendations from the US bodies, do not have the same value as the traditional sources\(^11\), but nevertheless have a large impact in practice and could give an indication on how the CJEU will make their decisions. These sources will therefore not be used to determine the law as it exists, but rather to help us get a deeper understanding of the practical application of the agreement, as well as the effects and the results of such. The Article 29 Working Party, as an example, has an advising competence only. Their opinions do not hold the force of law, but they are nevertheless considered important in interpreting the data protection framework.\(^12\)

The EU legal order is built on a distribution of competence between the EU and the Member States. This distribution of competences is expressed through the principle of conferral that is stated in Article 5 of the Treaty on European Union (hereafter: TEU). The factual competence for the Member States and the EU is unique for every single area according to Article 5.2 TEU. Regarding the Treaty on the Functioning of the European Union (hereafter: TFEU), and in particular Article 16 thereof, the European Parliament and the Council of the European Union had the competence to adopt the General Data Protection Regulation that will enter into application in May 2018.

The General Data Protection Regulation will have general application in the EU. That is, the regulation will be binding in its entirety and directly applicable in all Member States according to Article 288 in TFEU. It is therefore not necessary that the Member States implement

---

\(^8\) Korling, Zamboni, *Juridisk Metodlära*, p.128.
\(^9\) Korling, Zamboni, *Juridisk Metodlära* (1.3 u.), p. 127.
\(^10\) Korling, Zamboni, *Juridisk Metodlära* (1.3 u.), p. 127 f.
\(^12\) Krisch, *Do-not-track: Revising the EU’s data protection framework to require meaningful consent for behavioural advertising*, p. 9.
the Regulation in their national regulations. The data protection area will in 2018 be harmonized within the EU. The current Data Protection Directive on the other hand is, according to Article 288 TFEU, binding as to the result to be achieved. The Member States had to implement the directive.

The Member States need to consider the fundamental principles that are acknowledged by the EU as well, e.g. the principle of loyal cooperation, proportionality, legal certainty and subsidiarity etc. The principle of loyal cooperation, stated in Article 4.3 TEU, could be applied by the CJEU in order to ensure the effective application of the EU regulations and is a fundamental ground for other principles, e.g. the primacy of European law. It is sometimes possible that the EU Member States’ national regulations create a conflict with the EU regulations. The EU regulations will in that case have priority before national regulations.

In the light of the sources mentioned above, this thesis will include a qualified guess based on an analysis of what the most probable outcome of the agreement between the US and the EU. All conclusions presented will be built on relevant material that has been presented already, the law as it exists, and the analysis will be separated from the description of the law as it exists. The thesis will not be influenced by personal appraisals, even though the choice of method allows the thesis to include parts for criticism and proposed amendments. The choice of methodology also permits a comparison with other third countries and their agreements with the EU. This will be done shortly in this thesis in order to demonstrate the relevance of the arguments presented in the conclusion.

2.5 Disposition/Outline

The material content has been divided into 5 sections. Section 3, following the introduction section, will describe the criteria for the legal transfers of data under the EU regulation. Section 4 will present the reasons for the invalidity of the Safe Harbor Scheme. Section 5 will present the new adequacy decision between the EU and US replacing the Safe Harbor, the

---

13 Hettne, Otken Eriksson, EU-rättlig metod: Teori och genomslag i svensk rättsstillämpning, p. 177.
14 See Article 4.3 TEU.
15 Bernitz, Kjellgren, Europarättsens grunder, chapter 6.
16 Hettne, Otken Eriksson, EU-rättlig metod: Teori och genomslag i svensk rättsstillämpning, p. 82f.
17 Lerhberg, Praktisk juridisk metod, p. 95.
18 Sandgren, År rättsdogmatiken dogmatisk?, section 3.
19 Sandgren, Rättsvetenskap för uppsatsförfattare, p. 44.
20 Korling, Zamboni, Juridisk Metodlära, p. 24 and Sandgren, År rättsdogmatiken dogmatisk?, section 5.
21 Sandgren, Rättsvetenskap för uppsatsförfattare, p. 45 ff.
EU-US Privacy Shield. The question whether the Privacy Shield decision can withstand scrutiny by the CJEU will be discussed in section 6.

3 Criteria for legal transfers of data under the EU regulation

3.1 The Charter of Fundamental Human Rights

The EU recognizes and sets out the rights, freedoms and principles that will be common to the Member States in the Charter. Article 7 of the Charter sets out the right to respect for private life and Article 8 of the Charter provides for the right to protection of personal data. These two articles play an important role in the light of each other. Further, Article 47 of the Charter states the right to an effective remedy before a tribunal for everyone whose rights and freedoms guaranteed by the law of the EU have been violated. Article 52 of the Charter states that any limitation on the rights and freedoms recognized in the Charter must be provided for by law. These limitations must respect the essence of those rights and freedoms.

3.2 The EU Data Protection Reform

The European Commission put forward a Data Protection Reform package (hereafter: the reform) in January 2012 in order to strengthen the EU-internal rules and to provide individuals with more control over their personal data. The reform package comprises out a common EU framework for data protection, namely the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (hereafter: GDPR). That will enter into application 25 May 2018 and will replace the Data Protection Directive 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 (hereafter: The Data Protection Directive, or the Directive). The aim of the GDPR is to establish one common data protection standard for all Member States and thereby eliminate the differences in the level of protection amongst them. The GDPR is a comprehensive framework with 99 articles and 173 paragraphs. In addition to this, the Police and Criminal Justice Authority Directive sets the rules for processing of personal data within the Police and Criminal Justice Authority.

---

3.2.1 The Regulation

The GDPR applies, according to Article 3 GDPR, to the processing of personal data “in the context of activities of an establishment of a controller or a processor in the Union...”. How to transfer personal data to a country outside the EU, a so called third country, is regulated in chapter V. The provisions in that chapter shall, according to the general principle for data transfers in Article 44, be applied in order to ensure that the level of protection of natural persons guaranteed by this regulation is not undermined in case of a transfer. Article 44 covers all personal data that are undergoing processing, or are intended for processing after transfer to a third country or an international organization. Such a transfer shall only take place if it is complied with the conditions laid down in chapter V. The same principles are applicable for onward transfers of personal data from the third country or an international organization to another third country or to another international organization. The various solutions authorizing international transfers are essentially the same in the GDPR as in the current Data Protection Directive, such as Binding Corporate Rules and Contractual Clauses. However, the reform clarifies and simplifies those rules, as well as introduces some new tools for international transfers.23

3.2.1.1 Stronger enforcement of data protection rules

The GDPR, as well as the Data Protection Directive, require the Member States to provide for one or more independent Supervisory Authorities (hereafter: Data Protection Authority, DPA) to be responsible for monitoring the application of this data protection regulation.24 The GDPR strengthens the powers of the national DPAs in Article 58 and provides them with more tasks in Article 57, as well as spells out their independence in Article 52, in order to provide a stronger data protection.25 The authority must be able to examine a complaint from a data subject with complete independence.26 The authority shall remain free from external influence, and should not take instructions from anybody.27

The Article 83 GDPR states that a two-tiered sanctions regime will apply. The breaches the law makers have deemed to be most important from a data protection perspective could lead to fines up to 20 million euros or 4% of the total worldwide annual turnover of a company,

---

23 e.g. Article 46(1)(e) GDPR.
24 Article 51 GDPR.
25 e.g. Article 51 and 52 GDPR.
26 Schrems v. Data Protection Commissioner, C-362/14, paragraph 57.
27 C-518/07, Commission v. Germany, paragraph 25.
whichever is greater. For other breaches, the DPAs could impose fines on companies of up to 10 million euros or 2% of global annual turnover, once again, whichever is greater.\textsuperscript{28} What the DPA must consider when deciding on the amount of the administrative fine in each individual case are listed in Article 83(2) GDPR. The DPA will be empowered to impose fines up to 20 million euros or the 4% of the total worldwide annual turnover in case of non-compliance with an order made by the DPA, as referred to in Article 58(2)(i) GDPR, pursuant to Article 83(6) GDPR.

3.2.1.2 Adequacy decisions by the Commission

Personal data can be transferred on the basis of an adequacy decision according to Article 45 GDPR without any specific authorization being required. This decision is made by the Commission who may find that a third country, a territory or one or more specified sectors within that third country, or an international organization ensures an “adequate level of protection”. The GDPR provides for a more precise and detailed catalogue of elements that the Commission must take into account when assessing the level of data protection provided in the legal order of a third country, compared to the current Data Protection Directive. What the Commission should take into account is followed by Article 45(2) GDPR, e.g. respect for human rights and fundamental freedoms, relevant legislation and the existence and effective functioning of one or more independent supervisory authorities.\textsuperscript{29}

The Commission is also required to, on an ongoing basis, monitor developments in the third countries and the international organizations that might affect the decision adopted in accordance to Article 45(3) GDPR or Article 25(6) in the Data Protection Directive, according to Article 45(4) GDPR. It is also regulated in Article 45(3) GDPR that the Commission shall, in the adequacy decisions, provide for a periodic review every four years. The Commission must repeal, amend or suspend the decision without retro-active effects if they find that the adequate level within the meaning of paragraph 2 no longer is ensured, according to Article 45(5) GDPR. Decisions adopted on basis of the Data Protection Directive shall, according to Article 45(9) GDPR, remain in force until the opposite is decided through a new Commission Decision that is in accordance with Article 45(3) and 45(5) GDPR. A list of the third countries, territories and specified sectors within a third country and international organizations for which, according to a decision made by the Commission, ensure an “adequate level of protec-

\textsuperscript{28} Article 83(4) and (5) GDPR.
\textsuperscript{29} Article 45(2) GDPR.
tion” shall be published by the Commission in the *Official Journal of the European Union* and on its website, according to Article 45(8) GDPR.\(^{30}\)

### 3.2.1.3 Alternative existing data transfer mechanisms

A controller or processor may, according to Article 46(1) GDPR, transfer personal data to a third country or an international organization if the controller or the processor has provided appropriate safeguards. The GDPR recognizes the same appropriate safeguards as the current Data Protection Directive that legitimate transfers of personal data to a third country that has not been found to ensure an adequate level of protection, e.g. standard contractual clauses and BCRs. The GDPR introduces new alternative mechanisms such as approved codes of conduct and approved certification mechanisms as well.\(^ {31}\) The GDPR also clarifies the situation when so-called derogations can be used, e.g. a transfer may take place if the data subject has consented to the purposed transfer.\(^ {32}\) These alternatives are not necessarily confined to a specific country hence they might have a broader coverage than the adequacy decisions. However, they might only apply to specific data flows hence they might, in that manner, have a more limited scope.\(^ {33}\)

#### 3.2.1.3.1 Binding corporate rules

Appropriate safeguards referred to in Article 46(1) GDPR may be provided by BCRs according to Article 46(2)(b) GDPR. Article 47(1) GDPR sets out the requirements for the BCR that can be adopted by different multinational companies. Article 47(2) GDPR states what the rules shall specify. It is, according to Article 47(3) GDPR, the role of the Commission, with assistance from the Committee\(^ {34}\), to specify the format and the procedures for the BCR they which to be in place when information between controllers, processors and DPAs is being exchanged. Before the BCR can be adopted, the competent supervisory authority shall assess the adequacy of the rules and further approve the rules.

---

\(^{30}\) Andorra, Argentina, Canada, Switzerland, Faroe Islands, Guernsey, State of Israel, Isle of Man, Jersey, New Zealand, United States and Eastern Republic of Uruguay. Available at: European Commission, *Commission decisions on the adequacy of the protection of personal data in third countries.*

\(^ {31}\) Article 46(2)(c) and (f) GDPR.

\(^ {32}\) Article 49(1)(a) GDPR.

\(^ {33}\) Article 49 GDPR.

\(^ {34}\) The Committee shall be within the meaning of Regulation (EU) NO 182/2011 according to Article 47(1) and 93(2) GDPR.
The BCR are internal rules that define an agreed standard of how to transfer personal data within a corporate group, when one entity is located in a third country that does not provide an adequate level of protection of personal data. The BCR ensure that the transfer benefits from an adequate level of protection once approved under the EU cooperation procedure. No specific authorization from a supervisory authority is needed according to article 46(2) GDPR.

The BCR must designate an entity within the EU that will be responsible for breaches of the rules by the entity located outside the EU and that will be liable for such. All individuals have the right to enforce compliance with the rules in the EU by lodging a complaint before a DPA and bringing an action before a Member State Court, when their data is being processed by an entity within the group.

### 3.2.1.3.2 Contractual clauses

Appropriate safeguards referred to in Article 46(1) GDPR may be provided by standard data protection clauses according to Article 46(2)(c) and (d) GDPR. The clauses shall be adopted by the Commission, or by a DPA if approved by the Commission. Both options shall be pursuant to Article 93(2) GDPR, hence be adopted with assistance from the Committee. The Commission has approved sets of model clauses already. Each of these lays down obligations of data exporters and importers.

### 3.2.1.3.3 Approved codes of conduct and approved certification mechanisms

The GDPR introduces, in Article 46(2)(e) and (f), the “approved code of conduct” and “approved certification mechanism” as sufficient safeguards required in 46(1) GDPR for transfers of personal data. These alternatives should be pursuant to Article 40 or 42 GDPR, the primary sources of authority for establishing approved codes of conduct, together with binding and enforceable commitments of the controller or processor in the third country. Associations and other bodies should be encouraged to draw up codes of conduct within the limits of this Regulation. They should, when doing so, “consult relevant stakeholders, including data

---

35 Article 46(1) GDPR and European Commission, *Overview on Binding Corporate rules.*
36 European Commission, *Overview on Binding Corporate rules.*
38 The Committee shall be within the meaning of Regulation (EU) 182/2011, according to Article 93(2) GDPR.
39 e.g. Commission Decision 2001/497/EC, Commission Decision 2002/16/EC.
40 Recital 98 GDPR.
subjects where feasible, and have regard to submissions received and views expressed in re-
response to such consultations”. 41

3.2.1.3.4 Derogations

Derogations from the general prohibition of transferring personal data to entities established
in a third country without an adequate level of protection are listed in letters (a) to (g) in Arti-
cle 49(1) GDPR as alternative grounds on which a transfer nevertheless may take place. A
transfer may also take place, according to the second subparagraph in Article 49(1), if the
transfer “is not repetitive, concerns only a limited number of data subjects, is necessary for
the purposes of compelling legitimate interests pursued by the controller”. It is necessary that
the relevant controller has assessed all the circumstances surrounding the data transfer. The
controller must provide suitable safeguards with regard to the protection of personal data. The
data subject must be informed about the transfer. 42

4 The Safe Harbor Scheme and its invalidity – a lesson to learn?

The Commission found in Decision 2000/520/EC of 26 July 2000, the Safe Harbor Decision,
adopted by the Commission on the basis of Article 25(6) of the Data Protection Directive, that
the US ensured an adequate level of protection by reason of the Safe Harbor agreement. The
Safe Harbor Principles were issued by the US Department of Commerce on 21 July 2000 to
“foster, promote and develop international commerce”. 43

4.1 Mr. Schrems v. Data Protection Commissioner

4.1.1 Introduction

The fundamental right to data protection, enshrined in the Charter, is reaffirmed in the case C-
362/14 44 (hereafter: the Schrems Case) by the CJEU. The request sent to the CJEU was essen-
tially about how to interpret Articles 25(6) and 28 of the Data Protection Directive, in the
light of Article 7, 8 and 47 of the Charter, i.e. whether a supervisory authority of a Member
State is absolutely bound by a European Commission Decision or whether it has the authority
to suspend a data transfer in contravention. However, the CJEU answered more than just the

41 Recital 99 GDPR.
42 Article 49(1) GDPR.
specific questions posed by the Irish Court, and declared the EU-US Safe Harbor agreement to be invalid.

4.1.1.1 Edward Snowden revelations
Revelations made by the Edward Snowden, a former American National Security Agency subcontractor, demonstrated that the existence of large-scale information-gathering programs in the US that provided the US intelligence agencies with broad access to personal data about Europeans. Mr. Snowden had been working for the US National Security Agency (hereafter: NSA) and could therefore reveal, thanks to thousands of highly classified NSA files in his possession, “the interception and surveillance of internet and telecommunications systems by the NSA on a massive, global scale”.

One program used is code-named PRISM, and is aimed to protect public security. This program makes it possible for the NSA to collect personal data such as emails or photographs from “major us service providers” such as Microsoft, Google or Facebook. The NSA program X Keyscore enabled the NSA to, as it is formulated in the Guardian Newspaper dated 31st July 2013, “collect nearly everything a user does on the internet”. The surveillance systems are targeted at non-US persons located outside the US.

4.1.2 Is the DPA absolutely bound by a European Commission Decision?
Initially, Mr. Schrems, representing the Austrian non-profit organization Europe-Versus-Facebook, made a complaint to the Irish DPA in the wake after Edward Snowden’s revelations. Mr. Schrems asked the DPA to examine the validity of the Safe Harbor as he alleged that it did not guarantee a level of protection of his personal data in the US that is required in the Charter and the Data Protection Directive. He meant that his data would be subject to mass surveillance under US law. The Data Protection Officer in turn refused to investigate the complaint made by Mr. Schrems. The Officer meant that he was bound by the decision that the data protection regime in the US was adequate and effective when the transfer of data was with a company who had self-certified its adherence to the Principles implemented in the

45 Greenwald and MacAskill, *Boundless Informant: the NSA's secret tool to track global surveillance data.*
47 Greenwald, MacAskill, *NSA Prism program taps in to user data of Apple, Google and others.*
48 Greenwald, MacAskill, *NSA Prism program taps in to user data of Apple, Google and others.*
49 Greenwald, MacAskill, *NSA Prism program taps in to user data of Apple, Google and others.*
50 Schrems v. Data Protection Commissioner, C-362/14, paragraph 28.
51 Commission Decision 2000/520/EC.
decision. The case was brought for judicial review in the High Court of Ireland which in turn sent the question whether a DPA is absolutely bound by a European Commission decision, or whether the DPA may conduct its own investigations of the matter, to the CJEU.

The guarantee of independence of national DPA, according to Article 28(1) of the Data Protection Directive as well as Article 8(3) of the Charter, was designed to ensure the effectiveness and reliability of the monitoring of the protection of individuals as follow in Article 7, 8 and 47 of the Charter as well as the Directive. As stated in paragraph 42 in the Schrems case, the national supervisory authority must have, and has, a wide range of powers to ensure a fair balance between observance of the fundamental right to privacy and the interest requiring free movement of personal data in order to guarantee that protection. Article 28(3) of the Data Protection Directive lists those powers.

It is also stated that each DPA shall hear claims concerning the protection of the rights about data protection in Article 28(4) of the Data Protection Directive. The power of the Commission to make adequacy decisions according to Article 25(6) of the Directive cannot prevent a person, whose personal data could be or has been transferred to a third country, from lodging a complaint to the DPA within the meaning of Article 28(4) of the Directive. The Court found that a Commission Decision cannot eliminate the powers expressly accorded to the DPA by the Charter and the Directive. Article 28 of the Data Protection Directive applies to any processing of personal data regardless of if the Commission has adopted a decision pursuant to Article 25(6) of the Directive. Hence the Court found that the Safe Harbor decision unlawfully limited the powers of the DPAs authority stated in Article 28 of the Data Protection Directive and Article 8(3) of the Charter.

4.1.3 Annulment of the Safe Harbor Decision

The DPAs do not have authority to declare a Commission Decision invalid. Although the Court found that DPAs have the authority to suspend a specific data flow to an organization in a third country that has self-certified its adherence to the decision. It is well-established that

---

52 Schrems v. Data Protection Commissioner, C-362/14, paragraph 29.
53 Schrems v. Data Protection Commissioner, C-362/14, paragraph 36.
54 Schrems v. Data Protection Commissioner, C-362/14, paragraph 53.
55 Schrems v. Data Protection Commissioner, C-362/14, paragraph 57 and 66.
56 Schrems v. Data Protection Commissioner, C-362/14, paragraph 104.
57 Foto-Frost, C-314/85, paragraph 14 and 15.
58 Schrems v. Data Protection Commissioner, C-362/14, paragraph 101.
the only authority that can declare a Commission Decision as invalid is the CJEU. The CJEU did examine, in its judgement, whether the Safe Harbor Decision was in accordance with the Data Protection Directive. The CJEU declared the Safe Harbor decision invalid in its judgement of 6 October 2015.

4.1.3.1 “Essentially equivalent”
The CJEU explained the fact that there is no definition of “an adequate level of protection” in the Data Protection Directive. However, Article 25(2) of the Directive states that the adequacy of the level of protection shall be determined with consideration to all circumstances surrounding the transfer of data. According to Article 25(6) of the Directive, the Commission may find that a third country ensures an adequate level of protection by reason of its domestic law or of the international commitments for protection of the basic freedoms and rights of individuals.

The CJEU found that the term “adequate level of protection” does not mean that the third country is required to ensure a level of protection that is identical to the protection that is guaranteed in the EU or that the third country needs to have a regulation in place that is a mere and exhaustive copy of the EU regulation. Rather, the Court found that the article require the third country to ensure a level of protection of fundamental rights and freedoms “essentially equivalent” to that guaranteed within the EU. Since the Commission must consider all the circumstances surrounding the transfer, the Commission must assess the content of the regulations in the third country “resulting from domestic law or international commitments and the practice designed to ensure compliance with those rules”.

4.1.3.2 Protection of fundamental rights
The Commission must find “duly stating reasons” that the third country ensures an adequate level of protection of the fundamental rights when receiving personal data from the EU. This is an essential formal requirement pursuant to the Article 25(6) of the Data Protection Directive that is the article that gives the Commission the power to decide that the legal order

---

59 Melki and Abdeli, C-188/10 and C-189/10, paragraph 54.
60 Schrems v. Data Protection Commissioner, C-362/14, paragraph 106.
61 Schrems v. Data Protection Commissioner, C-362/14, paragraph 71.
62 Schrems v. Data Protection Commissioner, C-362/14, paragraph 73.
63 Schrems v. Data Protection Commissioner, C-362/14, paragraph 96.
in the third county ensure such a level of protection. Nevertheless, such an assessment was never made with a sufficient level of detail in the Safe Harbor Decision, the CJEU merely examined the Safe Harbor scheme. The Commission did not indicate that the US in fact ensured an adequate level of protection, by reason of its domestic law or its international commitments, in Article 1 of the Decision. Article 1 was therefore declared to be invalid.\(^{65}\)

4.1.3.2.1 EU legislation involving interference with the fundamental rights

It was followed by the Safe Harbor Decision that the applicability of the Safe Harbor Principles could be derogated. The Decision provided that national security, public interest and law enforcement considerations had primacy over the Safe Harbor Principles. Hence the decision allowed disclosures of personal data in instance of such interests. The applicability of the principles could also be derogated when statues, government regulations or case law created conflicting obligations or explicit authorizations, as long as the organization could demonstrate the non-compliance was “limited to the extent necessary to meet the overriding legitimate interest further by such authorizations”.\(^{66}\)

It has been stated by the CJEU that any EU-legislation enabling interference with the fundamental rights and freedoms that is guaranteed within the EU to privacy must lay down clear and precise rules governing the scope and application of a measure, as well as impose minimum safeguards.\(^{67}\) The persons whose personal data are affected must be guaranteed that their data is effectively protected against the risk of abuse and other unlawfully use. The right to respect for private life requires that derogations to such a protection must apply only in so far as is strictly necessary.\(^{68}\) The CJEU has found that a general derogation from the Principles, without limit or effective legal protection, enabled interference with the fundamental rights of European Citizens.\(^{69}\) There are not sufficient findings stated in the Safe Harbor Decision regarding rules adopted by the US that intended to limit any interference with fundamental rights of the individual whose data is transferred from the EU to the US.\(^{70}\)

\(^{64}\) Schrems v. Data Protection Commissioner, C-362/14, paragraph 97.
\(^{65}\) Schrems v. Data Protection Commissioner, C-362/14, paragraph 83, 96 and 97.
\(^{66}\) Schrems v. Data Protection Commissioner, C-362/14, paragraph 84 to 86.
\(^{67}\) Digital rights Ireland and others, C-293/12 and C-594/12, paragraph 54 and Schrems v. Data Protection Commissioner, C-362/14, paragraph 91.
\(^{68}\) Digital rights Ireland and others, C-293/12 and C-594/12, paragraph 52 and Schrems v. Data Protection Commissioner, C-362/14, paragraph 92.
\(^{69}\) Schrems v. Data Protection Commissioner, C-362/14, paragraph 87
\(^{70}\) Schrems v. Data Protection Commissioner, C-362/14, paragraph 93.
4.1.3.2.2 Access to personal data by the US Government

The CJEU stressed the lack of sufficient findings in the Safe Harbor Decision about rules adopted by the US that intended to limit the public authorities access to the individual’s data that was transferred from the EU to the US and thus the interference with their fundamental rights. The public authorities were not covered by the Safe Harbor Principles. The Safe Harbor Principles were applicable solely to self-certified United States organizations receiving personal data from the European Union. The CJEU stated that access to EU citizens’ personal data on a general basis, by intelligence agencies and US law enforcement, would mean that the data are not adequately protected since they are able to access the personal data that has been transferred from the EU “in a way incompatible, in particular, with the purpose for which it was transferred, beyond what was strictly necessary and proportionate to the protection of national security”.

To summarize, in order to provide a level of protection that is essentially equivalent to the one ensured in the EU, the US must provide for a regulation that lays down clear and precise rules governing the scope and application of a measure and impose minimum safeguards, as well as ensure that interference with the fundamental rights is limited to what is strictly necessary. The CJEU stated that the Commission has not presented duly stated reasons that the US provide for such.

4.1.3.2.3 Legal protection

The CJEU stated that there must be legislation in place allowing the individual to pursue legal remedies in order to have access to personal data relating to her, as well as in order to obtain rectification or erasure of such data. The lack of such possibilities would mean that the Article 47 of the Charter would not be respected. Article 47 of the Charter require everyone whose rights and freedoms guaranteed within the EU have the right to effective remedy before a tribunal. The Commission has not found duly stated reasons for how the US ensures a level of protection that is essentially equivalent with this requirement.

71 Schrems v. Data Protection Commissioner, C-362/14, paragraph 88.
72 Schrems v. Data Protection Commissioner, C-362/14, paragraph 82.
73 Schrems v. Data Protection Commissioner, C-362/14, paragraph 90.
74 Digital rights Ireland and others, C-293/12 and C-594/12, paragraph 52, 54 and Schrems v. Data Protection Commissioner, C-362/14, paragraph 91-92.
75 Schrems v. Data Protection Commissioner, C-362/14, paragraph 93, 97.
76 Schrems v. Data Protection Commissioner, C-362/14, paragraph 95.
77 Schrems v. Data Protection Commissioner, C-362/14, paragraph 95.
78 Schrems v. Data Protection Commissioner, C-362/14, paragraph 97.
The CJEU found that the Safe Harbor Decision did not refer to any existence of legal protection against interference of the fundamental rights, caused by the public authorities. The recourse procedure before the Federal Trade Commission (hereafter: the FTC) sets out in FAQ 11 Annex II of the Decision were limited to commercial disputes. The private dispute resolution mechanism, concerned compliance by the US undertakings with the Safe Harbor Principles, were limited to disputes about “the legality of interference with fundamental rights that results from measures originating from the state”. The data subjects had no administrative or judicial means of redress enabling access to the data relating to them that was being used by intelligence agencies or US law enforcement, or to get it rectified or erased.

4.1.3.2.4 Periodically check

The CJEU has stated that the Commission has, after making an adequacy decision, a duty to check periodically if such standard in the third country still persists. The protection of personal data plays an important role in order to ensure the fundamental right to respect for private life. The decision must continue to be factually and legally justified. Such a review needs to be done when evidence indicates a doubt in that regard as well. The Commission needs to take into account all the circumstances that might have arisen after that decision’s adoption. Many individuals’ personal data rights are threatened when data is transferred to a third country that does not ensure an adequate level of protection. Hence the review should be strict.

5 EU-US Privacy Shield – a strengthened framework?

The Commission implemented a new decision, the Commission Decision 2016/4176/EC of 12 June 2016 pursuant to the Data Protection Directive of the European Parliament and of the Council on the adequacy of the protection provided by the EU-US Privacy Shield (hereafter: The Privacy Shield). This decision seeks to replace the previous Safe Harbor agreement that was determined as invalid by the CJEU in 2015. The Commission states in paragraph 13 as well as in Article 1 of the Privacy Shield Decision “that the privacy Principles issued by the US Department of Commerce as a whole ensure a level of protection of personal data that is essentially equivalent to the one guaranteed by the basic principles laid down in Directive

79 Schrems v. Data Protection Commissioner, C-362/14, paragraph 89.
80 Schrems v. Data Protection Commissioner, C-362/14, paragraph 90.
81 Schrems v. Data Protection Commissioner, C-362/14, paragraph 76 to 78.
The Commission has assessed the level of protection in the US, the US law and practice including these official representations and commitments, in the light of 13 recommendations issued by the Commission given after the invalidity of the Safe Harbor and the Schrems case. The US organizations self-certify to the EU-US Privacy Shield Principles issued by US Department of Commerce (hereafter: the DoC), contained in Annex II to the Privacy Shield Decision. Supplementary information about the self-certification can be found in Annex II, section III.6.

5.1 Transparency

The DoC will maintain a list over all US organizations that have self-certified their adherence to the Privacy Shield Principles, the so called Privacy Shield List. The DoC will make this list available in order to make it easy to identify the organizations that are adhering to the Principles. The list of adhering companies serves as a public notice. It is now stated in the Privacy Shield that all self-certified organizations must include the Department's web address for the Privacy Shield List in the organization's privacy policy. That was one of the 13 recommendations that the Commission, on the basis of that Safe Harbor Framework in the Communication from the Commission to the European Parliament and the Council 27 November 2013, set out.

The Commission found in its communication in 2013 that it is not sufficient that organizations only provide the DoC with a description of their privacy policies. Another recommendation from the Commission was therefore that self-certified companies should be obliged to publicly disclose their privacy policies on their website in a consumer friendly and easily readable way. That recommendation is taken in consideration. The Privacy Shield Decision states that the self-certified organizations must do so, as well as to publicize their commitment to comply with the Privacy Shield Principles. They must demonstrate that their privacy policies, which they fully have implemented, are in line with the principles. Transparency of the

---

82 COM(2016)4176 final, paragraph 137.
organizations that has self-certified to the Privacy Shield is a fundamental principle to a framework like this.\textsuperscript{91}

Problems that impact on the credibility of a scheme like the Privacy Shield will have a negative impact on the fundamental rights of the EU citizens’ and create a disadvantage for the EU organizations compared to the ones in the US who are operating under the schemes, but do not actually apply to the principles in practice. The Commission, in its communication from 2013\textsuperscript{92}, stressed the importance of that all organizations that have certified comply with the transparency requirement. The DoC will, according to the Privacy shield, systematically verify that the organization’s policies conform to the Privacy Shield Principles in order to keep the list updated.\textsuperscript{93} The DoC will also, both \textit{ex officio} and when an organization does not provide satisfactory response to its enquiries, conduct reviews of all self-certified organization in order to ensure that companies that initially self-certify with the scheme actually follow the mandates set forth therein. Such a review will also be conducted as a result of a specific complaint or if there is sufficient evidence in place to suggest that an organization does not comply with the Principles.\textsuperscript{94} The DoC will assess periodically the administration and supervision of the Privacy Shield to ensure that there are monitoring procedures in place in order to address new issues that may arise.\textsuperscript{95}

The DoC will remove an organization from the Privacy Shield list in response to any notification about the organization’s persistent failure to comply with the Principles, regardless of if it is received from the organization itself, from a privacy self-regulatory body or another independent dispute resolution body, or from a government body. The DoC will first provide the organization with a 30 days’ notice and an opportunity for the organization to respond.\textsuperscript{96} It is now stated in the Privacy Shield that the DoC will keep an updated and informative list of organizations that are no longer part of the Privacy Shield Framework as well. The reason for the removal must be stated. The organizations that have been removed from the list because of “persistent failure to comply” do no longer have the right to retain information collected under the Privacy Shield. The organization must verify to the DoC whether they will return or

\begin{footnotesize}
\textsuperscript{91} COM(2016)4176 final, paragraph 31 and Annex II, section I.3.
\textsuperscript{92} COM(2013)847 final.
\textsuperscript{93} COM(2016)4176 final, paragraph 32 and COM(2016)4176 final, Annex I.
\textsuperscript{94} COM(2016)4176 final, paragraph 33 and COM(2016)4176 final, Annex I.
\textsuperscript{95} COM(2016)4176 final, Annex I.
\textsuperscript{96} COM(2016)4176 final, Annex II, section III.11(g)(iii).
\end{footnotesize}
delete the information, or continue to apply the Principles.\textsuperscript{97} It is mandatory for the organizations to continue to apply to the Principles if they will retain the information received.\textsuperscript{98}

The DoC will search for false claims of participations in the framework. Any misleading statements or practices will be subject to an enforcement action by the FTC, Department of Transportation or other relevant US enforcement authority. The DoC will monitor any false claims \textit{ex officio} or when referred from a DPA.\textsuperscript{99} The DoC will also conduct a review to verify that an organization, in relevant published privacy policies, removes references that imply that the organization continues to actively participate in the Privacy Shield even though the organization is removed from the Privacy Shield list for any reason.\textsuperscript{100}

\section*{5.2 Privacy Shield Principles}

The DoC, in consultation with the European Commission and with industry and other stakeholders, developed and issued the Privacy Shield Principles in order to “foster, promote and develop international commerce”.\textsuperscript{101} They must ensure the higher level of protection of data protection that will be offered by the GDPR when that regulation will enter into application in 2018, and consequently replace the current framework, the Data Protection Directive. The principles must be applied to by the organizations regardless of what personal data that are being transferred in reliance on the Privacy Shield.\textsuperscript{102} The principles are stated in part II of Annex II.

\subsection*{5.2.1 Choice Principle}

The data subject must be provided with a clear and readily available mechanism that makes it possible for her to choose to avoid, or, when sensitive information\textsuperscript{103}, to choose to expressly consent to\textsuperscript{104}, that her personal data is to be transferred to a third party\textsuperscript{105} or that the data is

\textsuperscript{97} COM(2016)4176 final, Annex I.
\textsuperscript{98} COM(2016)4176 final, paragraph 31, 33.
\textsuperscript{100} COM(2016)4176 final, Annex I.
\textsuperscript{101} COM(2016)4176 final, Annex I, section I.1.
\textsuperscript{103} i.e. personal information 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, according to COM(2016)4176 final, Annex II, section II.2(c).
\textsuperscript{104} An organization is not required to obtain affirmative express consent with respect to sensitive data in the cases listed in Annex II, section III.1.
\textsuperscript{105} A third party is someone other than an agent acting on behalf of the organization. An agent should always be acting under a contract with the organization, according to COM(2016)4176 final, Annex II, section II.2(b).
used for a purpose that is incompatible with the purpose for which it was originally collected or subsequently authorized by the individual.\textsuperscript{106} The GDPR introduce an enhanced protection for children’s data in Article 8 GDPR. If the child is under 16 years old, processing of that child’s data requires consent from the holder of parental responsibility over the child. Such a requirement is not phrased in the Privacy Shield.

\textbf{5.2.2 Security Principle and Data Integrity and Purpose Limitation Principle}

The self-certified organization must protect the information it is creating, maintaining, using or disseminating from “loss, misuse and unauthorized access, disclosure, alteration and destruction”.\textsuperscript{107} The organization must take into account the risks involved in the processing material and the nature of the material.\textsuperscript{108} The information that is being processed must also be limited to the information that is relevant. All processing must be compatible with the purpose for which it has been collected or subsequently authorized by the data subject. The organizations must ensure that the data is reliable for its intended use, accurate, complete and current. The data may be retained only for as long as it servers the purpose(s) for which it was initially collected or subsequently authorized.\textsuperscript{109}

The Privacy Shield does not recognize the concept of “automated individual decision making”, i.e. a decision based solely on automated processing. An explicit right not to be subject to such a decision is followed by Article 22 GDPR. There are three exceptions to this right followed by subparagraph (2), namely when it is necessary for entering a contract between the data subject and the data controller; when the Member State to which the controller is subject authorize the processing and if the Member State lays down “suitable measures to safeguard the data subject’s right and freedoms and legitimate interests”; or if the data subject has consented.

The explicit recognition of the principles “privacy by design” and “privacy by default” are a requirement due to be implemented under the GDPR.\textsuperscript{110} “Privacy by design” means that the controllers will be required to implement appropriate technical and organizational measures designed to implement data-protection principles in order to ensure privacy. The IT systems

\textsuperscript{106} COM(2016)4176 final, Annex II, section II.2.
\textsuperscript{107} COM(2016)4176 final, Annex II, section II.4(a).
\textsuperscript{110} Article 25 GDPR.
must ensure privacy during the whole life cycle of the system or process development. “Privacy by default” means that the controllers are required to implement appropriate technical and organizational measures to ensure that, by default, only personal data which are necessary for each specific purpose of the processing are processed. The Privacy Shield Principles do neither require that the self-certified organizations have IT systems in place, nor another solution, ensuring a level that is essential equivalent with the level of protection such a system would guarantee.

5.2.3 Notice Principle and Access Principle

This principle states the organization responsibility to, in a “clear and conspicuous language”, inform the data subject about the elements relating to the processing of their personal data, as well as the timing of such a notice. The data subject needs, e.g. to be informed about its right to access the information held by the organization about them. The right to access makes the data subject able to correct, amend or delete inaccurate information about them or information that has been processed in violation of the Principles. The right to access may be restricted in exceptional circumstances.

The GDPR requires that the legal basis for the processing must be determined in advance since Article 13 and 14 GDPR require that the controller inform the data subject about that basis. This is a new requirement and is not listed in the Notice Principle in the Privacy Shield. The organizations must also determine the planned time period for retention of the data since the data subject must be informed about such according to Article 13-15 GDPR as well. Such an information requirement is not included in the “Notice principle” in the Privacy Shield either.

The GDPR introduces the requirement to provide information to the data subject when the purpose of the processing of its personal data no longer require identification of the data subject, and the controller is not in the position to identify her. It is stated in Article 11(2) GDPR that the controller is not obliged to maintain, acquire or process additional information in order to identify the data subject in such case. This requirement is not stated in the EU-US Privacy Shield.

114 Article 6 GDPR.
The GDPR explicitly recognizes the data subject’s right to be forgotten, the right to obtain erasure of personal data concerning her, if any of the grounds in Article 17 GDPR are applicable. This right was recognized already in the Google Spain case in 2014. In addition to that, the GDPR details the liability for the controller to, after taken account to available technology and the cost of implementing, and if the controller has made the personal data public, inform other controllers processing personal data about the data subject’s request to erase the data, including links to, copies and replication of such data. Article 19 GDPR states that the controller should communicate any erasure carried out in accordance with Article 17(1) GDPR to each recipient the data has been disclosed to. This means that the US organizations need to have full control over who they have sent the information to and what information that have been sent in order to meet this level of protection.

It is followed by the “Access Principle” in the EU-US Privacy Shield that a data subject shall have access to personal information an organization hold about her in order to be able to delete information that is inaccurate. It is also stated in the Privacy Shield that the data must be reliable for its intended use, accurate, complete and current. However, there are no current requirements to erase data when the purpose for which it was collected is obsolete, nor when the data subject claims erasure or when the data are inaccurate, in the Privacy Shield.

The right to data portability is introduced in Article 20 GDPR. This means that the data subject must have the right to receive the personal data concerning her and to transmit those data to another controller than the one to which the personal data had been provided, if it is provided directly to a controller in a way described in the article. Nothing in the article indicates that it is only the first controller that the data subject had provided it to that will be covered by this requirement. This right improves the data subject’s right to access of the data about her. Nothing in the Privacy Shield indicate that this right is considered.

5.2.4 Recourse, Enforcement and Liability Principle
The self-certified organization will be responsible for the processing of the personal information it receives under the Privacy Shield, and that are subject to an onward transfer. The organization shall remain liable if an agent processes the personal information about the data

---

115 Google Spain Case, C-131/12.
subject in a manner inconsistent with the principles. An exception from this main principle is when the organization proves that it “is not responsible for the event giving rise to the damage”.

The organizations must provide mechanisms that ensure compliance with the effective privacy protection requirements in the other Privacy Shield Principles. There must be a follow-up procedure within the organization in place for verifying that the privacy practices have been implemented as presented, and for verifying that assertions organizations make about such practices are true. The organization must also make the retained records on the implementing of the Privacy policies available upon request in the context of an investigation or a complaint. The organization must re-certify its participation under the EU-US Privacy Shield annually. The organization must serve the DoC with all information relating to the Privacy Shield they require, and they must respond to all inquiries and request by the DoC, and to the DPAs they have chosen to cooperate. The data subjects shall have a number of possibilities to enforce their rights, lodge complaints and to have their complaints resolved as well. Effective remedies shall be included.

Article 37 GDPR introduces the requirement to designate a so called data protection officer if any of the three cases mentioned in the article are applicable, such as when the processing is carried out by a public authority or body or when the processing operation require regular and systematic monitoring of data subjects on a large scale. The data protection officer shall be involved in all issues which relate to the protection of personal data according to Article 38 GDPR. The role of the officer is to oversee the data protection responsibilities within the organization, ensure compliance with them and to cooperate with the national DPAs. The data subject may contact the officer directly regarding all issues relating to the processing of her personal data. The Privacy Shield framework does not provide for such a mechanism.

---

120 COM(2016)4176 final, Annex II, section II.7(b) and section III.11(c).
123 Article 39 GDPR.
5.2.5 Accountability for Onward Transfer Principle

Any transfer of personal information from an organization to a third party acting like a controller or processor can take place only for limited, and in a contract specified, purpose. A contract must guarantee that the organization complies with the Privacy Shield Principles. The self-certified organization must take reasonable steps to ensure that the third party effectively process the personal information consistent with the principles, and must stop and remediate unauthorized processing. Supplementary information about obligatory contracts for Onward transfers can be found in Annex II, section III.10.

5.3 Non-compliance with the Principles

The Privacy Shield Framework provides the data subject with means to enforce their rights and to lodge complaints regarding the self-certified companies’ non-compliance with the principles. The framework includes letters from The DoC (Annex I and Annex II), the FTC (Annex IV) and the US Department of Transportation. The letters do not carry the force of law, but set out the various mechanisms through how these authorities ensure effective legal protection. The letters clarify the Privacy Shield Principles the self-certified organizations have to commit to comply with, as well as the relevant US law and the representations made by the FTC and the Department of Transportations.

5.3.1 Complaint handling within the organization

The self-certified organizations must, according to the Recourse, Enforcement and Liability Principle, provide a redress mechanism within the organization for complaints from EU data subjects whose personal data might have been processed in a non-compliant manner. Each individual’s complaints and disputes must be investigated and resolved, hereafter at no cost to the individual. The organization must within a period of 45 days provide a response to the data subject. The response must include information about how the organization will rectify the potential problem. The organization must arbitrate claims delivered to the organization in accordance with the procedure set forth in Annex 2 of Annex I, “Annex I: Arbitral Model”. This option is only available for claims that the organization has violated its obligations under the Principles.

---

5.3.2 Independent dispute resolution body

One independent dispute resolution body, either in the US or the EU, must be designated by the organization in order to investigate and resolve complaints from the data subject about non-compliance with the privacy Shield Principles, and to provide recourse that hereafter will be free of charge for her. The organization must inform the data subject about the body designated and whether it is the panel established by DPAs, described in more detail below, an alternative dispute resolution provider based in the EU, or an alternative dispute resolution provider based in the US.

Its independence depends on the mechanisms impartiality, transparent composition and financing, and track record. If the organization fails to comply with the ruling of a dispute resolution, the dispute resolution body will notify such non-compliance to the DoC and the FTC, or a competent court if appropriate. The independent dispute resolution body is required to provide the data subject with information about the procedure and about the services they provide under the Privacy Shield. The remedies provided must ensure that the effects of non-compliance are reversed or corrected, the future processing will be compliant with the principles and, where appropriate, the processing of the data subject’s data will cease. There must be rigorous sanctions that can ensure compliance with the principles in place. What the sanctions may include vary, as well as the degree of severity, e.g. publicity for findings of non-compliance combined with the requirement to delete the data, suspension and removal of a seal, compensations for individuals for losses.

5.3.3 National data protection authority

The organizations can designate a DPA panel as the organization’s dispute resolution and therefore commits to cooperate with EU DPAs. Hence when a complaint is addressed to the DPA, the informal panel of DPAs established at a Union level will deliver an advice in order to help to ensure a harmonized and coherent approach. Both sides in the dispute will be able to provide evidence before the advice is delivered.

The national DPAs will investigate complaints regarding non-compliance with the Privacy Shield framework. The organizations have to respond to inquiries from the DPAs, comply with the advice given by the DPAs and provide the DPAs with written confirmation that action has been taken, when the respective organization has voluntarily submitted to the oversight by the DPA. If the organization fails to comply with the advice and do not offer a satisfactory explanation for the delay, the panel will choose whether to notify the FTC or other competent US enforcement authority, or, when the breach is considered as serious, the DoC.\textsuperscript{133} The DPAs has the power to suspend personal data transfer if necessary considered that the data are not afforded an adequate level of protection.\textsuperscript{134} In situations where an organization does not rely on a DPA panel, if no DPA panel has been designated as an organization’s dispute resolution body, the DPA receiving a complaint may refer the complaint either to the DoC or the FTC.\textsuperscript{135}

5.3.4 US Department of Commerce
The DoC is the U.S. authority administering the EU-U.S. Privacy Shield. The DoC shall review and undertake best effort to resolve complaints they have received about the organizations non-compliance with the Privacy Shield Principles. The DoC will make it possible for the DPAs to refer complaints to them in order to facilitate a resolution. The DoC will remove the organization from the Privacy Shield list if it is determined that the organization has persistently failed to comply. The data subjects will not be able to submit a complaint directly to the DoC.\textsuperscript{136}

5.3.5 US Federal Trade Commission
The FTC is a federal agency in the US\textsuperscript{137} that will ensure compliance with the Privacy Shield Principles in the commercial sphere with help from its investigatory and enforcement powers. The FTC has powers to prevent organizations from “using unfair methods of competition in or affecting commerce and unfair or deceptive acts or practices in or affecting commerce”.\textsuperscript{138} The FTC has the power to sanction these acts.\textsuperscript{139}

\textsuperscript{133} COM(2016)4176 final, Annex II, section III.5(b).
\textsuperscript{134} COM(2016)4176 final, paragraph 142.
\textsuperscript{135} COM(2016)4176 final, paragraph 51.
\textsuperscript{136} COM(2016)4176 final, Annex I and COM(2016)4176 final, paragraph 52.
\textsuperscript{137} Federal Trade Commission, \textit{Submit a Consumer Complaint to the FTC}.
\textsuperscript{138} FTC Act, 15 U.S.C § 45.
The FTC has committed, as a result of the Schrems Case and the invalidity of the Safe Harbor, rigorously enforce the new framework in order to strengthen the privacy protection provided to the EU citizens.\textsuperscript{140} The FTC provides stronger monitoring and enforcement, including an increased cooperation with individual EU DPAs. However, the scope of the FTC’s investigative and Law Enforcement Authority is still limited the commercial sphere. The FTC does not have jurisdiction over national security matters, nor other governmental actions. In addition to that, banks, savings and loan institutions\textsuperscript{141}, Federal credit unions\textsuperscript{142} and common carriers subject to the Federal Trade Commission Act (hereafter: FTC Act) to regulate commerce, and its relation to other persons, partnerships, and corporations are excluded from the types of organizations the FTC can investigate.\textsuperscript{143}

The FTC will undertake Privacy Shield investigations on its own initiative or when receiving complaints from the individuals. EU citizens will take their complaints to the national DPAs who in turn will refer the complaint to the FTC. The FTC will also investigate complaints they have received from the DoC or dispute resolutions or self-regulatory bodies. The FTC has a standardized process in place in order to do so.\textsuperscript{144} The FTC will give ‘priority consideration’ to referrals from the DoC, the dispute resolutions bodies and the DPAs,\textsuperscript{145} in particular the referrals from the DoC regarding organizations that falsely claim adherence to the principles, holding them out to be current members of the Privacy Shield Framework.\textsuperscript{146}

It is also important to mention that the FTC does not resolve or mediate individual consumer complaints,\textsuperscript{147} even though the FTC encourages the consumers to submit their complaints to FTC’s Consumer Sentinel Database. The FTC uses this database to identify trends, determine enforcement priorities and identify potential investigation targets. EU citizens may use this system in the same way as US citizens.\textsuperscript{148} Neither the EU-US Privacy Shield nor the FTC Act define a consumer. However, according to the EU, a “Consumer” means a natural person who are acting outside their trade, business, craft or profession.\textsuperscript{149}

\textsuperscript{140} COM(2016)4176 final, Annex IV.
\textsuperscript{141} FTC Act, 15 U.S.C. section 57a(f)(3).
\textsuperscript{142} FTC Act, 15 U.S.C. section 57a(f)(4).
\textsuperscript{143} FTC Act, 15 U.S.C. section 43.
\textsuperscript{144} COM(2016)4176 final, Annex IV, section II and COM(2016)4176 final, paragraph 54.
\textsuperscript{145} COM(2016)4176 final paragraph 54 and COM(2016)4176 final, Annex II, II.7(e).
\textsuperscript{146} COM(2016)4176 final, Annex IV, section II.
\textsuperscript{147} COM(2016)4176 final, Annex IV, n. 14 and Federal Trade Commission, \textit{Submit a Consumer Complaint to the FTC}.
\textsuperscript{149} e.g. Directive 2011/83/EU, Article 2(1), Directive 2005/29/EC, Article 2(1).
The FTC has a range of actions to address the issues raised. They may review the organizations privacy policies and obtain information directly from the organization or from a third party, follow up with the referring company etc. It may also initiate enforcement proceeding when appropriate. Therefore, called “consent orders” are administrative orders that the FTC uses to enforce compliance with the Privacy Shield Principles. If the organization fails to comply with these orders, the FTC may refer the case to a competent court that can impose penalties and other remedies.

The FTC will, in addition to the consultation with referring DPAs on case-specific matters, cooperate with the EU DPAs in an increased way. In order to make the cooperation more effective, and in order to improve the enforcement cooperation, the FTC commits to participate in meetings with representatives of the Article 29 Working Party to discuss the matter, and annually discuss the implementation of the framework with the DoC, the Commission and the Article 29 Working Party as well. The Global Privacy Enforcement Network is a system launched in 2015 for sharing information about investigations and promote enforcement coordination.

5.3.6 Privacy Shield Panel

If none of the above mentioned recourse mechanisms has satisfactorily resolved a complaint from a data subject, the Privacy Shield Panel is the last recourse mechanism where the EU data subject may invoke arbitration. This panel will be based in the US and will be subject to review by US courts. The panel will impose “individual-specific, non-monetary equitable relief” in order to remedy non-compliance with the Privacy Shield framework. Their decisions against the US self-certified organizations are binding hence they are enforceable in US courts according to Federal Arbitration Act chapter 2. Individuals should be able to use that legal remedy if a company fails to comply.

---

150 COM(2016)4176 final, Annex IV, section II.
152 COM(2016)4176 final, Annex IV, section V.
154 i.e. correction, deletion, or return of the individual’s data in question, according to COM(2016)4176 final, Annex I of Annex II, section B.
5.4 Derogations from the Principles

It is stated in the introduction to the Privacy Shield Principles, issued by the DoC, that adherence to the Privacy Shield principles may be limited when it is necessary to meet national security, public interest or law enforcement requirements; when statute, government regulation, or case law creates a conflicting obligations or explicit authorizations; or “if the effect of the Directive or Member State law is to allow exceptions or derogations, provided such exceptions or derogations are applied in comparable contexts”.157 The same exceptions were stated in the Safe Harbor and it was found in the Schrems case that such a exception of general nature enable interference with the fundamental rights of the EU-citizen whose personal data is or could be transferred to the US.158

A limited adherence that is permitted when statute, government regulation, or case law creates a conflicting obligations or explicit authorizations is acceptable provided that the organization can demonstrate that “its non-compliance with the principles is limited to the extent necessary to meet the overriding legitimate interests furthered by such authorization”.159 The organizations are now, according to the Privacy Shield framework, required to indicate in their privacy policies where such exceptions to the Principles may be permitted. The organizations must also inform the data subject about the requirement to disclose personal information in response to lawful requests by the public authorities when it is necessary to meet national security, public interest or law enforcement requirements.160 The possibilities for a public authority to access personal data that has been transferred from the EU to the US, as well as the limitations on and the protections against such an access, will be described below.

5.5 Access by US public authorities

The limitations on the US government access to the data transferred from the EU to the US are not mentioned in the Privacy Shield Principles since they are not subject to the framework. The principles are only, just like the Safe Harbor161, applicable to commercial organizations, and the means to legal protection and redress described previously is not applicable in

158 Schrems v. Data Protection Commissioner, C-362/14, paragraph 87.
161 Schrems v. Data Protection Commissioner, C-362/14, paragraph 82.
disputes relating to the legality of interference with fundamental rights that result from measures originating from the government.

Limitations have nevertheless been acknowledged as an essential component of the Privacy Shield to limit the access rights of the US government to transferred personal data, as well as redress possibilities. The framework includes letters from The Office of the Director of National Intelligence (Annex VI), the US Secretary of State (the Ombudsperson Letter, Annex III) and the Department of Justice (Annex VII). These letters shall ensure that there are meaningful and effective limitations on the US government’s access to data that has been transferred from the EU in place, as well as that safeguards applicable in the US law will ensure that the data subject’s personal data are effectively protected against unlawful interference and the risk of abuse.

### 5.5.1 National security

There is a framework in place in the US that regulates the intelligence agencies access to data for national security purposes. That framework includes procedures, rules and guidelines, e.g. the Foreign Intelligence Surveillance Act (hereafter: FISA), Presidential Directives, National Security Letters (hereafter: NSL) and the USA Freedom Act (hereafter: the Freedom Act). It is the Congress in the US that has the power to impose limitations within the national security area, but it is the President of the US who has the power to direct activities of the US intelligence Community through Executive Orders or Presidential Directives.\[^{162}\]

The US intelligence agencies can seek data that has been transferred to from the EU the US.\[^{163}\] They submit a request for collection to the National Signals Intelligence Committee (hereafter: SIGCOM) who in turn reviews the request to determine whether it is consistent with the FISA or the National Intelligence Priorities Framework (hereafter: NIPF).\[^{164}\] The NIPF states the intelligence priorities of the US that are determined by the president annually,\[^{165}\] and do not present an unwarranted risk to privacy and civil liberties.\[^{166}\] SIGCOM oper-

---

\[^{162}\] COM(2016)4176 final, paragraph 68.
\[^{163}\] COM(2016)4176 final, Annex VI, section I(a).
\[^{164}\] COM(2016)4176 final, Annex VI, section I(a).
\[^{165}\] COM(2016)4176 final, Annex VI, section I(b).
\[^{166}\] COM(2016)4176 final, Annex VI, section I(b).
ates under the NSA who in turn are responsible for overseeing an coordinating signals intelligence across the Intelligence Community.\textsuperscript{167}

5.5.1.1 Presidential Policy Directive 28

The Presidential Policy Directive 28 (hereafter: PPD-28) imposes a number of principles and requirements that apply to all US signals intelligence activities, as well as limitations for “signals intelligence” operations.\textsuperscript{168} The directive is a policy document that not intend to alter the rules in the applicable law.\textsuperscript{169} This directive is relevant for non US-persons because it stipulates, among other things, that the US signals intelligence activities must include appropriate safeguards.\textsuperscript{170} This directive is an improvement made in the US after the invalidity of the Safe Harbor. Signal intelligence is “intelligence derived” from e.g. communications systems, radars and weapons systems, e.g. from electronic signals and systems used by foreign targets. This is in order to gather information about international terrorists and foreign powers, organizations or persons.\textsuperscript{171} The PPD-28 states that all persons should be treated with dignity and respect\textsuperscript{172} and privacy and civil liberties shall be integral considerations in the planning of the US signals intelligence activities. That is regardless of the persons nationality or where they reside.\textsuperscript{173}

It is stated in case law from the CJEU that the principle of proportionality requires that “acts of the EU institutions be appropriate for attaining the legitimate objectives pursued by the legislation at issue and do not exceed the limits of what is appropriate and necessary in order to achieve those objectives”.\textsuperscript{174} The PPD-28 states that US signals intelligence activity shall be as “tailored as feasible”.\textsuperscript{175} This means that signal intelligence shall be conducted in a targeted manner. This target will have impact on what is actually collected.\textsuperscript{176} What “feasible” is, is subject to the policies that agencies have issued under PPD-28. These policies are public.\textsuperscript{177}

\textsuperscript{167} COM(2016)4176 final, Annex VI, section I(b).
\textsuperscript{168} COM(2016)4176 final, Annex VI, section I and PPD-28, section 1 and 2.
\textsuperscript{169} PPD-28, section 4(9).
\textsuperscript{170} PPD-28, section 4.
\textsuperscript{171} NSA, Signals Intelligence.
\textsuperscript{172} PPD-28, section 4.
\textsuperscript{173} PPD-28, section I(b).
\textsuperscript{174} Digital rights Ireland and others, C-293/12 and C-594/12, paragraph 46.
\textsuperscript{175} PPD-28, section I(d).
\textsuperscript{176} COM(2016)4176 final, Annex VI, section I(b).
\textsuperscript{177} Office of the Director of National Intelligence, \textit{STRENGTHENING PRIVACY \\ & CIVIL LIBERTIES PROTECTIONS} and COM(2016)4176 final, Annex VI, section I(b).
The intelligence Community might collect so called “bulk signals intelligence” under certain circumstances. That means that “authorized collection of large quantities of signals intelligence data which, due to technical or operational considerations, is acquired without the use of discriminants”. That will be done in order to identify new or emerging threats that are hidden within the system of global communications. Such a collection can only be used for six specific purposes, e.g. espionage. However, the Intelligence Community elements should conduct targeted signals intelligence collection activities when practicable. That is the main rule. The Intelligence Community elements will have to balance their efforts to protect legitimate privacy and civil liberties interests with the practical necessities of signals intelligence activities. That is the principle of reasonableness. When determining whether to collect the information, the Intelligence Community must consider the availability of other information from e.g. public sources, and prioritize collection through those means. The PPD-28 stipulates that the collection of signals intelligence must be based on statue or Presidential Authorization.

5.5.1.2 **Foreign Intelligence Act – Section 702**

Section 702 of the FISA Amendment Act of 2008 allows the government to target, on the basis of annual certifications prepared by the Attorney General and the Director of National Intelligence, for foreign intelligence purposes, communications of foreign persons. US person located anywhere in the world are not included. These certifications identify specific categories of foreign intelligence to be collected, and are submitted to the Foreign Intelligence Surveillance Court (hereafter: FISC). The FISC authorizes surveillance programs, e.g. PRISM and UPSTREAM, rather than individual surveillance measures. Section 702 permits the programs PRISM and UPSTREAM to provide searches carried out in a targeted manner through the use of individual selectors that identify specific communications facilities. It is not possible to search for key words or the names of targeted individuals, but it is possible to search for the target’s email address or telephone number. However, it is not necessary that

---

178 PPD-28, section 2(5).
179 COM(2016)4176 final, Annex VI, section I(b).
180 PPD-28, section 1(a).
181 Public Law 110-261.
182 Public Law 110-261.
183 50 U.S.C. § 1881(a) and (b).
184 FISA, 50 USC. § 1881(a).
185 PCLOB, section 702 report, p. 32 to 35.
the government has any reasonable belief that the target of surveillance has a connection to criminal or terrorist activities, only that non-US target might communicate foreign intelligence information.\textsuperscript{186}

The collection is authorized by law, and is subject to multiple levels of review, judicial supervision and oversight.\textsuperscript{187} The Attorney General and the Director of National Intelligence verify the compliance. The agencies have the obligation to report any incidents of non-compliance to the FISC.\textsuperscript{188} It reviews the applications requesting the electronic surveillance, and it needs to certify that the acquisition fulfill the criteria stated in the FISA.\textsuperscript{189}

5.5.1.3 National security letter statutory provisions

The NSLs are authorized by different statues and allow the Federal Bureau of Investigation (hereafter: FBI) to collect information contained in credit reports, financial records and electronic subscriber and transaction records from certain kinds of companies. This is done in order to protect against international terrorism or clandestine intelligence activities only.\textsuperscript{190} One legal authorization appears in the ECPA which requires that any request for subscriber information or transactional records uses a "term that specifically identifies a person, entity, telephone number, or account".\textsuperscript{191}

5.5.1.4 Freedom Act

The USA Freedom Act modified the US surveillance and other national security authorities when it was signed into law in June 2015. The USA Freedom Act amended the FISA.\textsuperscript{192} It also increased public transparency.\textsuperscript{193} The number of the FISA orders and directives sought and received, as well as an estimation of the number of persons targeted by surveillance, both US persons and non-US persons, shall be disclosed to the US Congress and the public by the US government. In addition to that, the act requires public reporting about the number of NSL issued.\textsuperscript{194} The Freedom Act prohibits bulk collection of any records even of non-US persons,

\textsuperscript{186}FISA, 50 U.S.C. §§ 1881(g)(4).
\textsuperscript{187}COM(2016)4176 final, Annex VI, section I(d).
\textsuperscript{188}COM(2016)4176 final, paragraph 109.
\textsuperscript{189}FISA, 50 U.S.C. §§ 1881a(d), (e), (g) and (h).
\textsuperscript{190}Patriot Act, 18 USC § 2709, section (a)(1).
\textsuperscript{191}ECPA, 18 U.S.C. § 2709.
\textsuperscript{192}Freedom Act, 50 U.S.C., chapter 36.
\textsuperscript{194}Freedom Act, H.R. 2048, section 602(a) and 603.
pursuant to various provisions of the FISA or through the use of the NSL.\textsuperscript{195} The government must base any application for collection under these authorizations on a “specific selection term”. This term shall specifically identify the relevant person, account, address or personal device. This shall limit the scope of information and the collection is precisely focused and targeted.\textsuperscript{196}

### 5.5.2 Law enforcement and public interest purposes

The US Department of Justice provides an overview of the tools that can be used to obtain data from companies in the US for criminal law enforcement or public interest purposes in Annex VII. All law enforcement and regulatory activities in the US must conform to applicable law and policies. The legal framework sets out limitations of the ability of US law enforcement and regulatory agencies to collect information from organizations in the US.\textsuperscript{197}

Searches and seizures by law enforcement authorities principally require court-ordered warrant upon a showing of probable cause that a crime was committed or is about to be committed.\textsuperscript{198} Once law enforcement no longer needs the seized items as evidence, they should be returned. That is followed by the Fourth Amendment of the US Constitution, which also guarantees privacy, dignity and protects against arbitrary and intensive acts by officers of the Government.\textsuperscript{199} Non-US persons do not have protection under the Fourth Amendment.\textsuperscript{200} They will however benefit from this right to protection indirectly if the data are held by US organizations with the effect that law enforcement authorities in any event have to seek judicial authorization before obtaining access to it.\textsuperscript{201} That requirement is a fundamental safeguard against abuse by the law-enforcement authorities. It needs to be ensured that proper authorization is obtained in all cases of interception.\textsuperscript{202}

Authorities, with civil and regulatory responsibilities, may only seek access to data that is relevant to matters within their scope of authority to regulate.\textsuperscript{203} The authorities may, within that limitation, issue subpoenas, criminal or administrative, to corporations for e.g. electroni-
cally stored information. The corporations have a few legal bases to use in order to challenge these requests. The administrative subpoenas are limited to specific cases and will be subject to independent judicial review at least where the government seeks enforcement in court.

5.5.3 Effective legal protection

The Commission found that safeguards provided under US law mostly are available for US Citizens or legal residents. The right to an effective judicial remedy was highlighted strongly by the CJEU in the Schrems case as well. The opportunity for the EU citizens to pursue legal remedies, and to seek judicial redress in order to obtain access, rectification or erasure of their personal data taking place under the US surveillance programs, was absent. However, the Judicial Redress Act of 2015 gives the EU citizens, when data has been transferred to the US limited access to US Courts to enforce privacy rights when the US government are guilty for Privacy Act violations.

The Judicial Redress Act extends the right to judicial redress that US-persons enjoy to the EU citizens. Civil actions against certain US government agencies may be brought for purposes of “accessing, amending, or redressing unlawful disclosures of records transferred from a foreign country to the United States to prevent, investigate, detect, or prosecute criminal offenses.” The act only applies to records transferred from public or private entities directly to the US public authorities, and the rights granted by the Act may be enforced only if the data subject has sufficient resources to bring an action in the US. There are thresholds to meet before an individual could bring an action before the US Courts, and redress is only available under limited circumstances and for some classes of data.

The Privacy Act regulates the government’s use of personal data. It ensures a protection of the privacy of their personal data. However, the Privacy Act is limited in its scope. It

---

204 COM(2016)4176 final, Annex VII.
205 e.g. The Bank Secrecy Act, Fair Credit Reporting Act and Right to Financial Privacy Act.
206 COM(2016)4176 final, Annex VII.
207 COM(2013)847 final, section 7(2).
208 Schrems v. Data Protection Commissioner, C-362/14, paragraph 90 and 95.
210 H.R 1428, Public Law No: 114-126 (02/24/2016), section 2.
211 Judicial Redress Act, section 2(h)(4).
212 H.R 1428, Public Law No: 114-126 (02/24/2016), section 2(a) and (b).
213 The Privacy Act, 5 U.S.C § 552a(a)(2).
only applies to data processing conducted by the US federal government, the public sector, and does not apply to state government or the private sector.\textsuperscript{214} In addition to this, law enforcement agencies like FBI and CIA are, in different cases, exempted from the Act.\textsuperscript{215} The NSA is able to claim exemptions to the Privacy Act based on the national security interest.\textsuperscript{216} Despite these significant limitations, this act is an improvement made after the invalidity of the Safe Harbor agreement.

5.5.3.1 National security area

5.5.3.1.1 Oversight

The US intelligence community is subject to various oversight mechanisms from within the executive branch.\textsuperscript{217} Additionally, the US Congress has oversight responsibilities regarding all US foreign intelligence activities.\textsuperscript{218} The tribunal\textsuperscript{219} FISC is responsible for oversight and compliance of any signals intelligence collection activities conducted pursuant to the FISA, and in some cases prior authorization of the measures. Their decisions can be challenged before the Foreign Intelligence Court of Review (hereafter: FISCR)\textsuperscript{220} and, ultimately, the Supreme Court of the United States.\textsuperscript{221}

The Freedom Act requires the FISC to demand that data collection meets certain standards for minimization, such as limits the amount of non-pertinent data collected. The FISC is also required to appoint a panel of advocates on behalf of privacy in important cases. These advocates shall make arguments that advance privacy and civil liberties interests.\textsuperscript{222} To increase the efficient oversight by the FISC, the FISC will be provided with documentation of Section 702 targeting decisions and “US Person Queries” and shall assess how the foreign intelligence purpose requirement is being met in practice. The FISC will therefore be provided with some insight into whether the government is in fact satisfying the “foreignness” and “foreign intelligence purpose” requirement. It could also signal to the FISC that changes to the target-

\textsuperscript{214} Colonna, \textit{LEGAL IMPLICATIONS OF DATA MINING}, p. 232.
\textsuperscript{215} The Privacy Act, 5 U.S.C. § 552a(j) and (k).
\textsuperscript{216} The Privacy Act, 5 U.S.C. § 552a(b)(7).
\textsuperscript{217} PPD-28, section 4(a)(iv), COM(2016) 4176 final, section 3(1)(2).
\textsuperscript{218} National Security Act, §3091(a), COM(2016)4176 final, paragraph 102 and COM(2016)4176 final, Annex VI, section I(d).
\textsuperscript{219} FISA, 50 U.S.C. § 1803 (b).
\textsuperscript{220} FISA, 50 U.S.C. §§ 1801 to 05.
\textsuperscript{221} FISA, 50 U.S.C. 1881a(H) and COM(2016)4176 final, paragraph 105.
\textsuperscript{222} Freedom Act, 50 U.S.C., chapter 36.
ing procedures may be needed.\textsuperscript{223} The NSA must hereafter also document the foreign intelligence reasons for targeting decisions.\textsuperscript{224}

Further, the Intelligence Community employs oversight personnel\textsuperscript{225} and has its own independent Office of the Inspector General responsible for the oversight. The Department of Justice and the Department of Defense provides extensive oversight of intelligence activities, as well as the ODNI Civil Liberties and Privacy Office, the PCLOB and the President's Intelligence Oversight Board.\textsuperscript{226} The intelligence Community, as well as relevant Inspector Generals and the Attorney General also have numerous mechanisms to ensure that they are complying with the limitations on collection, e.g. checks and reviews.\textsuperscript{227}

\textbf{5.5.3.1.2 Individual redress}

In case a data subject has a complaint about that collecting and further processing of her personal data is taking place under the US Surveillance programs, the data subject has different individual redress mechanisms to choose from within the national security area.\textsuperscript{228} These relate to interference under the FISA, unlawful intentional access to personal data by government officials and access to information under Freedom of Information Act (hereafter: FOIA). The FISA provides for a number of available remedies to non-US persons, the right to seek relief in the US courts are not limited to US persons.\textsuperscript{229} The remedies available are e.g. to sue government officials in their personal capacity for money damages\textsuperscript{230}, to bring a civil cause of action for money damages against the US\textsuperscript{231}, to challenge the legality of surveillance in the event the US government intends to use or disclose information obtained.\textsuperscript{232} Additional avenues that EU data subjects could use can be found in e.g. the Computer Fraud and Abuse Act, Electronic Communications Privacy Act and Right to Financial Privacy Act\textsuperscript{233}, as well as in

\begin{footnotes}
\item[224] COM(2016)4176 final, paragraph 110.
\item[225] For instance, the NSA employs more than 300 compliance staff in the Directorate for Compliance according to Annex VI, section I(d).
\item[226] COM(2016)4176 final, paragraph 95.
\item[227] COM(2016)4176 final, Annex VI, section I(d) and COM(2016) 4176 final, paragraph 103.
\item[228] COM(2016)4176 final, paragraph 111 to 113.
\item[229] COM(2016)4176 final, paragraph 111 and Annex VI, section V.
\item[230] FISA, 50 U.S.C. § 1810.
\item[231] FISA, 18 U.S.C. § 2712.
\end{footnotes}
the Administrative Procedure Act\textsuperscript{234}. However, the governmental agencies might be able to withhold information from the data subjects under certain circumstances.\textsuperscript{235}

It can be concluded that non-US citizens have judicial redress possibilities in the US, but the available causes of action are limited. The individual needs to be able to demonstrate the existence of damage\textsuperscript{236} or show that the government intends to use obtained information in judicial or administrative courts.\textsuperscript{237} The individuals who bring claims to the courts will be declared inadmissible where they cannot demonstrate “standing”.\textsuperscript{238} To establish ”standing” in the Supreme Court\textsuperscript{239} the applicant must be able to show an injury that is “concrete, particularised, and actual or imminent; fairly traceable to the challenged action; and redressable by a favorable ruling”.\textsuperscript{240} These factors restrict access to ordinary courts.

5.5.3.1.2.1 EU-US Privacy Shield Ombudsperson

The US has established a new redress mechanism in the area of national security in order to provide for additional redress avenue accessible for non-US data subjects.\textsuperscript{241} A so called Ombudsperson, independent from the national security authorities\textsuperscript{242}, will follow up on complaints and enquiries by EU citizens about national security access. The Ombudsperson will deal with complaints from data subjects in the EU who believe that their personal data has been used in an unlawful way by any public authority in the US. The request will initially be submitted to the DPA in the Member State who in turn will send the request to the Ombudsperson. The Ombudsperson will make further communication directly to these bodies. It is the DPA that will be responsible for the communication with the individual submitting the request.\textsuperscript{243} Hence the process for the individual will be simplified, e.g. the individual will be able to communicate in their own language.

The Ombudsperson will confirm whether relevant laws, statutes, executive orders, presidential directives and agency policies have been complied with, and if the matter has been properly

\textsuperscript{234} The Administrative Procedure Act, 5 U.S.C. § 702.
\textsuperscript{235} COM(2016) 4176 final, paragraph 115.
\textsuperscript{237} 50 U.S.C. § 1806.
\textsuperscript{238} COM(2016)4176 final, paragraph 115.
\textsuperscript{239} US Constitution, Article III.
\textsuperscript{240} Clapper v. Amnesty International USA, p.10.
\textsuperscript{241} COM(2016)4176 final, paragraph 116.
\textsuperscript{242} ECtHR, Zakharov, paragraph 275.
\textsuperscript{243} COM(2016)4176 final, Annex III, section 3(a) and(f).
investigated. In order of non-compliance, the Ombudsperson will inform the complainant that it has been remedied. There must be mechanisms available for the Privacy Shield Ombudsperson in order for her to be able to ensure that the data subject will get an appropriate response. These mechanisms are listed in Annex III of the Privacy Decision, e.g. the possibility to effectively use and coordinate closely with the oversight bodies, and the possibility to refer matters related to requests to the PCLOB for consideration. All the written commitments will be published in the US federal register.

5.5.3.2 Law enforcement and public interest area

There are a number of judicial redress avenues available for individuals in the US law that can be used against US public authorities, e.g. in the Administrative Procedure Act, the Freedom of Information Act, the Electronic Communications Privacy Act. These avenues are available for all individuals regardless of their nationality. The Administrative Procedure Act states that "any person suffering legal wrong because of agency action, or adversely affected or aggrieved by agency action", is entitled to seek judicial review. The data subject has the right to obtain access to federal agency records and to enforce such right in court. This right is limited since such records could be protected from public disclosure by an exemption or special law enforcement exclusion. The Electronic Communications Privacy Act provides recourse for an affected individual to file a civil action in US federal court for "actual and punitive damages as well as equitable or declaratory relief" against a government official, or against the US.

The Commission lists other alternative acts in the Privacy Shield Decision that provide the data subject with a right to bring suit against a US public authority, e.g. the Computer Fraud and Abuse Act, the Federal Torts Claim Act, the Right to Financial Privacy Act, and

---

244 COM(2016)4176 final, Annex III, section 3(e).
248 COM(2016)4176 final, paragraph 130.
the Fair Credit Reporting Act255.256 However, nothing indicates that the Commission has assessed further the efficiency of these acts, nor the possibilities for the EU citizens to use them.

5.6 Periodic review of adequacy finding

It was stated in the Schrems case that the Commission, after it has adopted an adequacy decision, is required to check periodically whether the adequacy decision is still factually and legally justified.257 The requirement of a periodic review of, on an ongoing basis, an adequacy decisions adopted pursuant to the Directive, are stated in Article 45(4) GDPR as well. This requirement is met in the Privacy Shield Decision where it is stated that the Commission periodically must monitor whether the findings relating to the adequacy of the level of protection that the Privacy Shield ensures are still factually and legally justified. The Commission will monitor the decision, as well as the compliance by the US authorities.258

To facilitate this process, the US will provide the Commission with relevant material about the developments in the US law. The adequacy findings may also be influenced by legal developments in Union Law, e.g. the GDPR. The Commission will also request that the DoC provides information on relevant aspects of the functioning of the EU-US Privacy Shield, and seek explanations concerning any questions or matters concerning the Privacy Shield, including transparency reports allowed under the US regulations.259

If the Commission concludes that the level of protection that is offered in the Privacy Shield framework cannot be regarded as “essentially equivalent” to the one in the EU, it will inform the DoC and request that appropriate measures are taken in order to continue to guarantee effective compliance and an adequate level of protection. If sufficient measures are not taken within a reasonable and given timeframe, if the US Authorities fail to demonstrate satisfactorily that the EU-US Privacy Shield will continue to guarantee effective compliance and an adequate level of protection, the Commission will initiate the procedure leading to the partial or complete suspension, or repeal of the decision. The Commission may alternatively purpose to amend the decision.260

256 COM(2016)4176 final, paragraph 134.
257 COM(2016)4176 final, paragraph 145-146.
258 COM(2016)4176 final, paragraph 145-146.
259 COM(2016)4176 final, paragraph 145-146.
260 COM(2016)4176 final, paragraph 150.
5.7 Action of Data Protection Authorities

It is clarified by the CJEU that the Commission, through an adequacy decision, has no competence to restrict the powers of the DPAs which are derived from Article 28 of the Directive and hereafter, Article 51 GDPR, and the Charter.261 Nothing in the Privacy Shield indicates an interference with this. It is now stated in the EU-US Privacy Shield that when a DPAs receives a complaint that questions the commission adequacy decision, national law must provide the DPA with a legal remedy to put those objections before a national court, if it seems to be well founded that adequacy decision might interfere on the fundamental right to privacy and data protection.262 This is in accordance with the GDPR which expressly empowers the DPA to order the suspension of data flows to a recipient in a third country or an international organization.263

6 Scrutiny by the CJEU and general conclusions

The CJEU has stressed the importance of the right to protection of personal data and privacy in its case law. That approach is strengthened with respect to the fact that the GDPR requires a higher level of protection than the Data Protection Directive, even though the GDPR, as well as the Directive, are having as its principal aim to ensure the free movement of personal data.264 Hence the right to the protection of personal data is not an absolute right, but must be considered in relation to its function in society.265

The processing of personal data could result in infringed fundamental freedoms, in particular the right to privacy, enshrined in Article 7 of the Charter, and the right to protection of personal data, enshrined in Article 8 of the Charter. The fundamental rights form an integral part of the general principles of law hence the court must ensure the observance of these.266 Interference with Article 7 and 8 of the Charter have been pointed out as wide-ranging and must be considered to be “particularly serious”.267 For the purposes of a valid adequacy decision by

261 Schrems v. Data Protection Commissioner, C-362/14, paragraph 40.
262 COM(2016)4176 final, paragraph 144.
263 Article 58(2)(j) GDPR.
264 The joined cases C-465/00, C-138/01 and C-139/01, paragraph 70.
265 Deutsche Telekom AG and others, C-543/09, paragraph 51.
266 Google Spain Case, C-131/12, paragraph 68, P Connolly v Commission, Case C-274/99, paragraph 37 and Österreichischer Rundfunk and Others, C-465/00, paragraph 68.
267 Digital rights Ireland and others, C-293/12 and C-594/12, paragraph 37.
the Commission, and in order to withstand scrutiny by the CJEU, the Privacy Shield Framework must be able to meet the criteria specified by the CJEU, as well as the GDPR.

6.1 Essentially equivalent?

As mentioned above, the US takes a sectoral approach when regulating the Data Protection, while the EU relies on its comprehensive legislation, the Data Protection Directive, or soon, the GDPR. The CJEU has found that the term “adequate level of protection” means that the third country must ensure a level of protection that is “essentially equivalent” with the one ensured in the EU, by reason of its domestic law or its international commitments. Any interference with fundamental rights authorized by law must be strictly necessary, personal data may not be accessed on a general basis. Further, the data subject must have right to redress. The European Commission is required to assess the content of the data protection rules in the US and the practices designed to ensure compliance with those rules. The challenge the US faces is therefore to make it clear enough how the EU-required “adequacy standard” impact on personal data transfers to the US.

Canada, Argentina and Switzerland are three countries that ensure an adequate level of protection.268 All three countries have one law which applies to all types of personal data.269 The Commission has found that these countries ensure an adequate level of protection by reason of these laws. All three Commission Decisions look very similar to the Privacy Shield Decision. All four decisions contain 6 articles, each with very similar wording. However, in addition to these articles, the US Privacy Shield Decision contains 155 paragraphs and the other three decisions approximately 15 each. In addition to that, the Privacy Shield Decision includes seven annexes, the other decisions include none. To be able to understand the scope of the Privacy Decision, it is also necessary to have a comprehensive understanding of the US legal system, in particular of all the different acts mentioned in this thesis.

The EU-US Privacy shield is a complex framework. All information is spread out in the “main” decision document as well as in the seven annexes. The documents refer to each other, as well as to US regulations, policies, websites etc. The Privacy Shield would benefit from greater precision and accessibility. The lack of clarity in the set of documents is something

---

269 PIPEDA, Swiss Data Protection Act and Personal Data Protection Act in Argentina.
Article 29 Working Party in particular stressed as a weakness in the new framework. The effective exercise of the data subject’s right might be undermined in practice because the complexity and the lack of clarity of the overall architecture of this mechanism. The protection ensured in the framework is difficult to find and use, hence it will probably have a negative impact on the data subjects rights.

6.1.1 Transparency
The Privacy Shield values the fundamental principle of transparency. The transparency approach in the Privacy Shield is in accordance with the recommendations from the Commission. The Privacy Shield demonstrates, in this matter, an important improvement in comparison to the Safe Harbor Scheme. Further, the requirement of a periodic review in both Schrems and the GDPR is met in the Privacy Shield Decision.

6.1.2 Derogations from the Principles
It is followed by the Privacy Shield Decision that the applicability of the Privacy Shield Principles may be derogated. Firstly, the Decision provides that national security, public interest and law enforcement considerations have primacy over the Privacy Shield Principles. This means that the organizations must disclose the personal data when receiving a lawful request by a public authority relying on one of these grounds. The rules governing the scope and application of measure, and the question whether the derogations will apply only in so far it is strictly necessary, will be discussed in the following section (6.1.2).

Secondly, derogations are authorized when statute, government regulation or case law create a conflicting obligation or explicit authorization. These derogations shall be limited to the extent necessary to meet an overriding legitimate interest furthered by such authorization. However, such a general derogation, enabling an interference with the fundamental rights enshrined in the Charter, must according to the Schrems Case be limited to the what is strictly necessary. The Commission might therefore need to assess the scope of this possibility a bit further. It is not clear in the Privacy Shield Decision which interest that are legitimate and therefore will get prioritization before the Principles. The Commission needs to assess the rules adopted by the US that intend to limit the interference to what is strictly necessary. This needs to be done in order for the Commission to be able to determine whether the adequate

270 WP29 Working Documents WP238, section 1.2.2.
271 WP29 Working Documents WP238, section 2.2.6(a).
level of protection of the fundamental rights enshrined in the Charter is ensured by reason of US law.\textsuperscript{273}

The fact that the organizations will be required to indicate in their privacy policies when an overriding legitimate interests will authorize a derogation from the Privacy Shield Principles might be applicable will improve the transparency and make the data subject more aware of what might happen to her data. This must be regarded as a safeguard that enables the data subject to be protected against the risk of abuse and against any unlawful access and use of the data.

\textbf{6.1.3 Access by US public authorities}

The letters attached to the framework as annexes describe, as a summation, a range of safeguards and limitations applicable on the US authorities. Collection limitations, retention and dissemination limitations and compliance and oversight mechanisms are included in this, as well as the legal protection offered. The Commission has concluded in the Privacy Shield Decision that there are rules in place in the US that guarantee that any interference with the fundamental rights for national security and law enforcement purposes are limited only to what is strictly necessary to achieve the legitimate objective in question.\textsuperscript{274}

The Commission has in its communication in 2013 recommended that the organizations in their privacy policies should include information about the extent to which US law allows public authorities to collect and process data transferred under the, by then in force, Safe Harbor Framework. The Commission believed that the individuals and the companies would be unfamiliar with what was being done with their data otherwise. That in turn could be something the Commission believed created a conflict with the transparency principle.\textsuperscript{275} However, it is now stated in the Notice Principle that the data subject must be informed of the organization’s requirements to disclose her personal information when receiving a lawful request by a public authority. The recommendation from the Commission seems to be met.

\textsuperscript{273} Schrems v. Data Protection Commissioner, C-362/14, paragraph 97.
\textsuperscript{274} COM(2016)4176 final, paragraph 88 and 125.
\textsuperscript{275} COM(2013)847 final, section 8.
6.1.3.1 National security area

There have been some changes in the US about surveillance practices since the Snowden revelations in June 2013 and the invalidation of the Safe Harbor in 2015. The PPD-28 has been introduced. It requires the access by US authorities to be targeted. The data collected in bulk may only be used for six specific national security purposes. Since 2015, the Freedom Act also limits bulk collection of data and allows companies to issue transparency reports on the approximate number of government access requests. In addition to that, the FISA has been amended and the FISC has got a strengthened role in connection to that the Freedom Act was signed into law in 2015. The FISC will be supplied with more information to use in determining whether the government’s acquisitions comply with the FISA and the Fourth Amendment. The FISC shall demand that data collection meets certain standards for minimization and the FISC is required to appoint a panel of advocates on behalf of privacy in important cases. These advocates shall make arguments that advance privacy and civil liberties interests.\(^{276}\)

Much focus and emphasis is placed on the PPD-28. The PPD-28 includes both limitations on the access and safeguards as required in CJEU case law. It can nevertheless be questioned if the requirement in the PPD-28 about that signal intelligence activities must be “tailored as feasible” also means that all data collection must be strictly necessary and proportionate. Further, this directive is not law. It is issued by the Barack Obama administration and could be superseded by subsequent policy directives issued by the next administration. This presidential policy directive might therefore not be anything the Commission should value highly as protection for the EU-citizens.

The Freedom Act does, as well as PPD-28, limit the collection of the information. It states that the collection must be “precisely focused” and targeted. It is not clear in the Commission Decision whether this means that the collection must be restricted to what is strictly necessary either. That requirement needs to be demonstrated. A balance needs to be found between the objectives for the collection\(^{277}\) and the individual’s rights.\(^ {278}\)

It is stated in the letter from ODNI that the US intelligence agencies must send a request to SIGCOM in order to seek the data that has been transferred from the EU. SIGCOM will en-

\(^{276}\) Freedom Act, 50 U.S.C., chapter 36.
\(^{277}\) Digital rights Ireland and others, C-293/12 and C-594/12, paragraph 60.
\(^{278}\) ECtHR, Zakharov, paragraph 199 and 260.
sure that their request is consistent with the FISA or NIPF. This request protects the data sub-
jects from an unlawful use of their data and limits the collection. However, it is not necessary
that the government has any reasonable belief that the target of surveillance has a connection
to criminal or terrorist activities, only that non-US target might communicate foreign intelli-
gence information. This collection of personal data could probably not be regarded as lim-
ited to what is strictly necessary. At least, the Commission has not stated that is the case.

To summarize, neither the FISA, the PPD-28 nor the Freedom Act seem to be able to guaran-
tee that the access to personal data by public authorities on the national security area is limited
to what is strictly necessary. This is an important requirement that has been stated in the
CJEU case law. These acts seem, having regard to the Commission’s assessment, to provide
an insufficient protection of the data subjects' personal data.

Further, it is not clear in the Privacy Shield how the statues authorizing the NSL also restrict
the use of them, i.e. what the criteria are. It is not stated that there are rules governing the
scope and application of a measure in place, nor whether they impose minimum safeguards. It
is not clear how the data subject are protected against the risk of abuse or any unlawful access
and use of the data beyond the fact that the Freedom Act require disclosure by the government
about the number of NSL requests they have received. The information about this authoriza-
tion is insufficient.

6.1.3.2 Law enforcement and public interest
The DoJ describes in its letter to the Commission the possibilities for a public authority to
access personal data on the purposes of law enforcement. These activities must comply with
law and policies that contain limitations. However, the DoJ mentions the possibility to access
personal data on the purpose of public interest shortly and not in detail. It is stated that agen-
cies may seek access only to data that is relevant to matters within their scope of authority to
regulate, but it is not clear in the Commission Decision how the US lays down clear and pre-
cise rules governing the scope and application of such a measure. The Commission Decision
does not assess the scope of the possibility to authorize the access on the purpose of the public
interest further. The information about this authorization is insufficient.

6.1.4 Redress mechanisms, complaint handling and enforcement

The EU citizens are provided with a couple of alternatives for complaint handling. The Commission considers these alternatives as sufficient to ensure a level of protection that is essentially equivalent with the one guaranteed by the basic principles laid down in the Data Protection Directive. However, whether they are “essentially equivalent” to the forthcoming the GDPR is a separate matter entirely.

6.1.4.1 If non-compliance with the Principles

The most effective alternative for the individuals will be to submit their complaint to the national DPA. It was stated in the Schrems case that a transfer of personal data to a third country, that has been subject of a Commission decision pursuant to Article 25(6) of Data Protection Directive, is neither according to Article 8(3) of the Charter nor Article 28 of the Directive, excluded from the national supervisory authorities’ sphere of competence the oversight. The DPAs have the power to suspend personal data transfer if necessary considered that the data are not afforded an adequate level of protection. Nevertheless, the DPA will not have the power to force the data subject’s right to access the data relating to them, nor get it rectified or erased. This alternative is therefore not sufficient enough to ensure a level of protection that is essentially equivalent with the one enshrined in Article 47 of the Charter.

While it is true that the DPAs have limited authority to enforce the data subject’s access rights etc., the data subjects will nevertheless through the DPA have access to the FTC and the DoC who will prioritize their complaint. The DoC will have the power to remove the organization from the Privacy Shield list and the FTC will use administrative orders to enforce compliance with the Privacy Shield Principles. The FTC might be able to force the data subject’s right to access the data relating to them and to get it rectified or erased. The FTC will otherwise be able to refer the case to a US court. Nevertheless, the scope of the FTC is, as was established already in the Schrems case, strictly limited, partly to the fact that it only act on a limited part of the commerce area, and partly because of its limited investigation powers. Individuals may bring claims before the FTC through a DPA, but customers are excluded. The protection the FTC provides the EU-citizens is therefore not sufficient since it is not available in all possible cases.

---

280 COM(2016)4176 final, paragraph 61 and 124.
281 Schrems v. Data Protection Commissioner, C-362/14, paragraph 54.
282 COM(2016)4176 final, paragraph 142.
The efficiency of the Privacy Shield Panel, the last recourse mechanism, can be questioned. Even if the EU citizens theoretically can rely upon the privacy safeguards afforded in the US law, and hence enforce the decision from the panel in the US courts, the relevant question is if they really have the ability to enforce its right in practice. Above the potential language issues, and the need for the EU citizen to get to the US, the US privacy laws are unfamiliar to Europeans and must be able to demonstrate “standing”. Further, the legal status of the annexes might be an issue. It is definitely doubtful whether the US court will let an EU citizen to claim its rights and enforce the decision from the Privacy Shield Panel in the court based on a letter from the DoC (Annex I and II). The legal status of the Annexes will be discussed further below. The Privacy Shield Panel might therefore not be a complement to the FTC that is sufficient.

6.1.4.2 If unlawful access by the public authorities
A key element in the CJEU’s reasoning in the Schrems Case was that the EU data subjects would have no administrative or judicial means of redress in the US enabling “the data relating to them to be accessed and, as the case may be, rectified or erased” when her data was being transferred to the US, and was in the possession of intelligence agencies.\textsuperscript{283} A legislation not providing for the possibility to pursue for such does not respect the essence of the fundamental rights enshrined in Article 47 of the Charter, which mentions an effective remedy before an impartial tribunal.\textsuperscript{284}

The Ombudsperson mechanism, independent from the US intelligence services, is created in order to provide for an additional redress avenue for all EU data subjects on the national security area. It is unclear in the Privacy Shield Decision, as well as in the letter from the Secretary of State, in what way the Ombudsperson can order non-compliance to be remedied and whether it is vested with adequate powers to effectively exercise its duty, e.g. if the ombudsperson could get sufficient information to be able to state if processing of personal data is lawful, and if it ensures a satisfactory remedy in case of disagreement. The Privacy Shield only states that the Ombudsperson will “respond” to complaints. It is necessary that the Ombudsperson’s recommendations and decisions will be effectively respected and implemented by the relevant bodies. It is not clear that the Ombudsperson provides for any possibility for

\textsuperscript{283} Schrems v. Data Protection Commissioner, C-362/14, paragraph 90.
\textsuperscript{284} Schrems v. Data Protection Commissioner, C-362/14, paragraph 95.
an individual to pursue legal remedies in order to have access to personal data relating to her, or to obtain the rectification or erasure of such data. A legislation not providing for the possibility to pursue for such does not respect the essence of the fundamental rights enshrined in Article 47 of the Charter. The Ombudsperson mechanism seems therefore not to be in compliance with Article 47 of the Charter.

The new Judicial Redress Act seems, at first glance, to address the concerns raised by the CJEU about a lack of means to redress when personal data is in the possession of intelligence agencies. However, the Judicial Redress Act might be of little use because of the exemptions followed in the Privacy Act. The NSA could claim national security exemptions to the Privacy Act and continue to use the PRISM program in order to make it possible for the NSA to collect personal data from different organizations. In addition to that, the US legal system is unfamiliar to a non-US person. Once again, the question is whether an EU citizen, in practice, will be able to decide which causes of action available under the Privacy Act that is exercisable against the relevant US agency. Different actions are creating a patchwork of legal remedies and redress is only available under limited circumstances and for some classes of data. The rights granted by the Act may also be enforced only if the data subject has sufficient resources to bring an action in the US. As mentioned above, there are thresholds to meet before an individual could bring an action before the US Courts and get “standing”.

The FISA provides for a number of available remedies to non-US persons as well, e.g. to bring a civil cause of action for money damages against the US. Further, the Commission shortly mentions that the Administrative Procedure Act, the Freedom of Information Act, the Electronic Communications Privacy Act, as well as a several other statutes, that provide the data subject with judicial redress avenues that can be used against US public authorities. However, it is highly doubtful whether it is feasible for Europeans to take advantage of the tools provided in these acts, as well as the Judicial Redress Act, without a fairly knowledge of the US legal system. The Commission must therefore assess whether it is feasible for the EU citizens to use this means in practice, as well as the scope of the protection.

6.1.4.3 Need for a DPA in the US

It is obvious that the EU highly values the role of a DPA since their role, as well as their pow-

---

285 Schrems v. Data Protection Commissioner, C-362/14, paragraph 95.
ers and the requirements for independency, will be extended. As mentioned above, the Commission shall also, according to Article 45(2) of the GDPR, take account of the existence and effective functioning of one or more independent supervisory authorities in the third country when assessing the adequacy level of the protection. Argentina, Canada and Switzerland are, as mentioned above, examples of countries that the Commission has found to ensure a level of protection that is essentially equivalent with the one ensured in the EU. All three countries provide a body like the DPA. These bodies give requesting parties assistance and advise, as well as control and enforce compliance with the regulation. The US regulations do not require or provide for a single data protection agency in the same way.

The FTC in the US aims to ensure compliance with the relevant data protection regulation, it has enforcement powers through the “consent orders” and cooperate with the EU DPAs. However, the FTC will not have direct contact with the data subjects as an EU DPA will. The jurisdiction of the FTC is also strongly limited in contrast to the EU DPAs. However, the Ombudsperson could fill in some gaps that the FTC does not cover. The Ombudsperson will investigate whether the data subject’s personal data has been treated in accordance with the limitations and safeguards in the ODNI letter, Annex VI. The Ombudsperson’s jurisdiction is, on the other hand, limited to the national security area.

In addition to the FTC and the Ombudsperson mechanisms, the DoT, the DoC the PCLOB will provide accountability for oversight and enforcement as well. Their responsibilities and powers are spread out in different regulations. The DPA in the EU must be able to assist and cooperate with other DPAs in other Member States if necessary. All these US bodies will be able to do so. None of these bodies will, on the other hand, be able to communicate directly to the data subject.

The FTC, the Ombudsperson, the DoT, the DoC and the PCLOB might together provide accountability for oversight and enforcement in the EU and could therefore work together as a DPA function. Each mechanism, regarded to their limitations, do not play a role that is comparable to that of the national DPA provided in the GDPR or the Data Protection Directive on its own. Since none of the above mentioned mechanisms will be able to assist and advise the data subject directly, it needs to be assessed whether the contact with the national DPA who

---

286 Article 25(1) PIPEDA, Article 26 the Swiss Data Protection Act and Article 29 the Personal Data Protection Act in Argentina.
in turn will get in contact with these mechanisms are enough, if the subject actually will be able to get assistance and advice in practice. Further, the Commission must assess whether these mechanisms together are vested with powers and independency enough to ensure the same level of protection as a national DPA.

The Article 29 working group has questioned the independence of the US Ombudsperson to oversee redress for Europeans whose data has been misused since the Ombudsperson will be appointed and report to the Secretary of state.\textsuperscript{287} The Ombudsperson will be nominated by the President and confirmed by the Senate. The Ombudsperson can be dismissed in his role of Under Secretary in the Department of State. These factors might undermine the independence and could therefore be in non-compliance with Article 8(3) of the Charter that require that compliance with the data protection rules shall be subject to control by an independent authority. It is important that the Ombudsperson has sufficient distance from the intelligence community in order to be independent. The Commission must assess whether that is the case.

\subsection*{6.1.5 The legal status of the Annexes}

The annexes contain commitments that are fundamental for a well-functioned cooperation between the US and the EU. The annexes provide, as an example, for oversight and enforcement mechanisms in order to verify and ensure that the self-certified companies comply with the principles. If, for example, the DoC does not investigate organizations adherence to the Principles and thus not update the Privacy Shield list of organizations on a regular basis as promised in Annex I, information might be transferred to an organization that falsely claim adherence to the Principles. That transfer is not lawful. Another example is that the FTC commits in Annex IV to give priority to Privacy Shield referrals from EU Member States, to take action to address issues about US organization’s non-compliance with the Principles, as well as to exchange information on referrals with referring enforcement authority and cooperate with EU DPAs. This is also a fundamental commitment since this is one of few redress mechanisms available for the EU citizens in the US.

It is not clear whether a mere assurance from the old administration in the US could be sufficient enough to protect the right to data protection and privacy. It might be necessary that the legal status of the annexes gets questioned. What impact the change of administration in the

\textsuperscript{287}WP29 Working Documents WP238, p. 4.
US will have on the Privacy Shield and its annexes might also be a relevant issue to consider. The Privacy Shield framework does apparently not have the force of law and could easily be superseded by the new US administration.

6.1.6 Need to modify the Privacy Shield Framework?

6.1.6.1 The Privacy Shield Principles

The “Access Principle” needs to be modified in order to meet the “right to be forgotten” requirement in the GDPR. The data subject has no right to claim the data to be erased in the Privacy Shield. The Privacy Shield must also require that the organizations communicate the erasure to all recipient the data has been disclosed to. Further, there is no requirement to actually erase the data in the Privacy Shield; neither on the request of the subject, nor when the data is inaccurate or when the purpose for which it was collected is obsolete. That will be needed both in order to meet the “right to be forgotten” but also the retention principle/storage principle followed by EU regulation.

Since the GDPR introduces an enhanced protection for children’s data and requires consent from the holder of parental responsibility over the child before processing, it might be necessary that the Choice Principle in the Privacy Shield gets modified. Further, the time for the processing must be determined in advance since the data subject has the right to be informed about the retention time according to the GDPR. The “Notice Principle” in the Privacy Shield needs to be modified in order to meet that requirement, as well as the requirement in Article 11(2) GDPR.

The GDPR mentions the data minimization principle in Article 5(c). Personal data shall be processed in an adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. The Data Integrity and Purpose Limitation Principle in the Privacy Shield states that personal information must be limited to what is relevant for the purpose(s) of processing. It might be necessary to modify this sentence in order for this principle to be essentially equivalent to the minimization principle in the GDPR. The EDPS has recommended to add an “adequacy” and a “necessity” requirement.288

The organizations might have to offer “data portability” in order to benefit the data subject

with a greater access to its personal data, as well as “Privacy by Design” and “Privacy by Default” in order to benefit the data subject with a greater security of its data. They must also make sure that they ensure protection against “automated individual decisions” based solely on automated processing. The access principle and the security principles should be modified in order to meet these improvements in the GDPR.

Another improvement in the GDPR is the requirement directed to some organizations to designate a Data Protection Officer. The officer will be responsible within the organization to ensure compliance with the GDPR and to cooperate with the DPAs. They will also be someone the data subject can contact directly. The Privacy Shield framework does not provide for such a mechanism. Nevertheless, it is stated in the Privacy Shield that organizations are responsible for the processing of personal data, that effective privacy protection must include clear mechanisms for assuring compliance with the principles and that they must provide a redress mechanism within the organization for complaints from EU data subjects whose personal data might have been processed in a non-compliant manner. The Privacy Shield may formulate the data protection in a way that is different to how it is formulated in the GDPR, as long as it is essentially equivalent. Their solution must however be as good as the Data Protection Officer. The Commission should assess whether that is the case.

6.1.7 The qualified guess

The Commission must, according to the Schrems Case, find “duly stating reasons” that the US, by reason of its domestic law or its international commitments, ensures a level of protection that is essentially equivalent to that ensured in the EU. The Commission Decision must be expanded in order to fulfil this requirement. It must be expanded in order to show that the Commission actually has assessed the level of protection provided in the US in a sufficient way.

It is necessary that the Commission concludes that there are mechanisms in place to cover for the lack of a DPA in the US. Further, the Commission needs to demonstrate that derogations to the data protection apply only in so far it is strictly necessary. Firstly, the assessment of whether there are rules in place that guarantee that the public authorities will not get access to the EU citizens’ personal data on a general basis needs to be improved. Hence the Commission needs to analyze the situations where relevant exemptions to such rules may apply in order to determine the scope of the public authorities means to access, as well as the possibili-
ties for the public authorities to withhold information about the data subject. Secondly, the Commission must assess in what way the Privacy Shield Principles might be derogated in case of a conflicting obligation in statues, government regulations or case law. The Commission must provide some kind of guarantee that that the EU is informed of all regulations that might have an effect on the principles might be needed.

Article 47 of the Charter requires that everyone whose rights and freedoms guaranteed within the EU have the right to effective remedy before a tribunal. The Privacy Shield demonstrates a willingness to offer an effective redress mechanism for individual data subjects. However, the complexity of the system might have impact on the individual fundamental rights enshrined in Article 47 of the Charter. The most feasible alternative today seems to be that the individual chooses to bring a complaint to the national DPA. This alternative is not sufficient enough to ensure a level of protection that is essentially equivalent to that enshrined in Article 47 of the Charter. The DPA can only in limited cases refer the claim to FTC who in turn can refer the case to US court. The data subject will probably not have the chance in practice, even though she theoretically has the possibility, to bring a claim in the US court on her own when a public authority has processed her data in an unlawful way. The Commission should assess the effectiveness of this right in practice. The Commission has not found duly stating reasons for how the US ensures a level of protection that is essentially equivalent with Article 47 of the Charter.

EU citizens have the right to enforce compliance with BCR in the EU by lodging a complaint before a DPA in the Member State and bringing an action before a Member State Court. Maybe the same possibility should be offered regarding non-compliance with an “Adequacy Decision”, or at least that a national DPA should be able to represent the EU citizen and act on their behalf as an intermediary. This could facilitate direct access for individuals to independent redress, taking into account the complexity of the mechanisms provides.

As stated in the introduction, the EU must strive for making the market attractive, without giving up on the citizens’ rights, e.g. the right for data protection and privacy as well as the right to an effective remedy and a fair trial. The Privacy Shield might be one attempt to do that, to make it possible for organizations to transfer personal data from the EU to US. How-
ever, the framework is still untried and liable to be challenged.\textsuperscript{289} The organizations cannot be certain that the framework is reliable before it is being fully operational, and the conditions presented above makes it doubtful that the Privacy Shield would withstand scrutiny in the CJEU. What might be necessary as well is that the annexes legal status gets questioned in the court before it is possible to rely on the Privacy Shield.

The Privacy Shield will probably not be sufficient to demonstrate that the US provides a protection of personal data that is essentially equivalent to that ensured in the EU, and thus withstand scrutiny in the CJEU. The lack of an exhaustive assessment performed by the Commission was the core reason to determine the Safe Harbor Decision invalid. Other alternatives are therefore more reliable; e.g. BCR or SCC.

\textsuperscript{289} Digital Rights Ireland has challenged the adoption of the Privacy Shield pact by the EU executive in front of the second-highest EU court, arguing it does not contain adequate privacy protections, T-670/16. However, a spokesman for the European Commission said: “As we have said from the beginning, the Commission is convinced that the Privacy Shield will live up to the requirements set out by the European Court of Justice (ECJ) which has been the basis for the negotiations.” Available at: Reuters, \textit{This Privacy Group Is Challenging the U.S.-EU Data Pact}. 

62
7 Table of cases

7.1 CJEU
Judgement of 15 July 1964, C-6/64, Costa v ENEL [cit. Costa v. ENEL, C-6/64]


Judgement of 20 May 2003, the joined cases C-465/00, C-138/01 and C-139/01 [cit. The joined cases C-465/00, C-138/01 and C-139/01]

Judgement of 20 May 2003, C-465/00, Österreichischer Rundfunk and Others, EU:C:2003:294 [Cit. Österreichischer Rundfunk and Others, C-465/00]


Judgement of 22 June 2010, C-188/10 and C-189/10, Melki and Abdeli EU:C:2010:363 [cit. Melki and Abdeli, C-188/10 and C-189/10]

Judgement of 9 March 2010, C-518/07, Commission v Germany, EU:C:2010:125 [cit. C-518/07, Commission v Germany]

Judgement of 5 May 2011, C-543/09, Deutsche Telekom AG and others, EU:C:2011:279 [cit. Deutsche Telekom AG and others, C-543/09]

Judgement of 7 November 2013 IPI, C-473/12, Institut professionnel des agents immobiliers (IPI) v Geoffrey Englebert and others, EU:C:2013:715 [cit. Case IPI, C-473/12]

Judgement of 8 April 2014, C-293/12 and C-594/12, Digital rights Ireland and Seitlinger and others, EU:C:2014:238 [cit. Digital rights Ireland and others, C-293/12 and C-594/12]

Judgement of 13 May 2014, C-131/12, Google Spain v. AEPD and Mario Costeja González, EU:C:2014:317 [cit. Google Spain Case, C-131/12]

7.2 ECtHR
Judgement of 4 December 2015, Grand Chambre, Case of Roman Zakharov v. Russia, European Court of Human Rights, Application no. 47143/06 [cit. ECtHR, Zakharov]

7.3 United States of America


8 Table of statues and Conventions

8.1 The United States of America

Administrative Procedure Act of 1946 (5 U.S.C. ch. 5) [Cit. Administrative Procedure Act]

Computer Fraud and Abuse Act of 1984 (18 U.S.C. 1§ 1030) [cit. Computer Fraud and Abuse Act]

Electronic Communications Privacy Act of 1986 (18 U.S.C. §§ 2510-22) [Cit. ECPA]


The Administrative Procedure Act of 1946 (5 U.S.C. § 702) [cit. The Administrative Procedure Act]

The Bank Secrecy Act of 1970 [cit. The Bank Secrecy Act]


The Fourth Amendment of the Constitution of the United States of America (1787) [Cit. The Fourth Amendment of the U.S Constitution]


The Judicial Redress Act of 2015 (H.R 1428) [cit. The Judicial Redress Act]

The Privacy Act of 1974 (5 U.S.C. § 552a) [cit. The Privacy Act]

USA Freedom Act, H.R. 2048, Public Law 114-23 [cit. Freedom Act, H.R. 2048]

8.2 European Union


8.3 Argentina
The Personal Data Protection Act No 25.326 of 4 October 2000 [hereafter: The Personal Data Protection Act in Argentina]

The Regulation, approved by Decree No 1558/2001 of 3 December 2001 [Argentine Regulation]

8.4 Canada
Canadian Personal Information Protection and Electronic Documents Act, S.C. 2000, c. 5 [cit. PIPEDA]

8.5 Switzerland
8.6 The European Commission Documents


9 Other documents


Article 29 Data Protection Working Party Working Documents WP238, published on 13 April 2016 [cit. WP29 Working Documents WP238]


10 Bibliography

Colonna, Liane, LEGAL IMPLICATIONS OF DATA MINING, Ragulka Förlag,1 u., 2016 [cit. Colonna, LEGAL IMPLICATIONS OF DATA MINING]


Korling, Fredric, Zamboni, Mauro, Juridisk Metodlära, Studenlitteratur, 1.1 u., 2013 [cit. Korling, Zamboni, Juridisk Metodlära]

Korling, Fredric, Zamboni, Mauro, Juridisk Metodlära, Studenlitteratur, 1.3 u., 2013 [cit. Korling, Zamboni, Juridisk Metodlära (1.3 u.)]

Lerhberg, Bert, Praktisk juridisk metod, Institutet för bank- och affärsjuridik (IBA), 6. u., 2010 [cit. Lerhberg, Praktisk juridisk metod]

Sandgren, Claes, Rättsvetenskap för uppsatsförfattare, Nordstedts Juridik, 3 u., 2015 [cit. Sandgren, Rättsvetenskap för uppsatsförfattare]

11 Web material


European Commission, Commission decisions on the adequacy of the protection of personal data in third countries, http://ec.europa.eu/justice/data-protection/international-
transfers/adequacy/index_en.htm (18 October 2016) [cit. European Commission, Commission decisions on the adequacy of the protection of personal data in third countries]


FOIA.gov, What is FOIA?, https://www.foia.gov/ (16 October 2016) [cit. FOIA.gov, What is FOIA?]


Glenn Greenwald and Ewen MacAskill, NSA Prism program taps in to user data of Apple, Google and others, 7 June, 2013, https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data (22 September 2016) [cit. Greenwald, MacAskill, NSA Prism program taps in to user data of Apple, Google and others]

NSA, Signals Intelligence, https://www.nsa.gov/what-we-do/signals-intelligence/ (5 October 2016)[cit. NSA, Signals Intelligence]


12 Journals

Deighton, Alison, The EU-U.S. Privacy Shield – is it strong enough?, P. &D.P, 16(4), 8-10 (2016) [cit. Deighton, The EU-US Privacy Shield – is it strong enough?]

Sandgren, Claes, Debatt - Är rättsdogmatiken dogmatisk? Tidsskrift for Rettsvitenskap nr 04-05, s. 648-656, 2005 [cit. Sandgren, Är rättsdogmatiken dogmatisk?]


Krisch, Matthew S. Do-not-track: Revising the EU’s data protection framework to require meaningful consent for behavioural advertising, Volume XVIII Richmond Journal of Law & Technology, issue 1 [cit. Krisch, Do-not-track: Revising the EU’s data protection framework to require meaningful consent for behavioural advertising]