ECONSTOR
Make Your Publications Visible.

A Service of

ZBW Leibniz-Informationszentrum Wirtschaft
Leibniz Information Centre for Economics

Jung, Niklas

Research Report

Abolition of the Safe Harbor Agreement: Legal situation and alternatives

EIKV-Schriftenreihe zum Wissens- und Wertemanagement, No. 17

Provided in Cooperation with:
European Institute for Knowledge & Value Management (EIKV), Hostert (Luxembourg)

Suggested Citation: Jung, Niklas (2016) : Abolition of the Safe Harbor Agreement: Legal situation and alternatives, EIKV-Schriftenreihe zum Wissens- und Wertemanagement, No. 17, European Institute for Knowledge & Value Management (EIKV), Rameldange

This Version is available at:
https://hdl.handle.net/10419/148370

Standard-Nutzungsbedingungen:

Die Dokumente auf EconStor dürfen zu eigenen wissenschaftlichen Zwecken und zum Privatgebrauch gespeichert und kopiert werden.

Sie dürfen die Dokumente nicht für öffentliche oder kommerzielle Zwecke vervielfältigen, öffentlich ausstellen, öffentlich zugänglich machen, vertreiben oder anderweitig nutzen.

Sofern die Verfasser die Dokumente unter Open-Content-Lizenzen (insbesondere CC-Lizenzen) zur Verfügung gestellt haben sollten, gelten abweichend von diesen Nutzungsbedingungen die in der dort genannten Lizenz gewährten Nutzungsrechte.

Terms of use:

Documents in EconStor may be saved and copied for your personal and scholarly purposes.

You are not to copy documents for public or commercial purposes, to exhibit the documents publicly, to make them publicly available on the internet, or to distribute or otherwise use the documents in public.

If the documents have been made available under an Open Content Licence (especially Creative Commons Licences), you may exercise further usage rights as specified in the indicated licence.

WWW.ECONSTOR.EU

Mitglied der Leibniz-Gemeinschaft

EIKV European Institute for Knowledge- and Value-Management A.s.b.l.

EIKV-Schriftenreihe zum
Wissens- und Wertemanagement

Abolition of the Safe Harbor Agreement – Legal situation and alternatives

Niklas Jung

Band 17

IMPRESSUM
EIKV-Schriftenreihe zum Wissens- und Wertemanagement
Herausgeber: André Reuter, Heiko Hansjosten, Thomas Gergen

© EIKV Luxemburg, 2016

European Institute for Knowledge & Value Management (EIKV)
c/o M. André REUTER - 27d, rue du Scheid
L-6996 Rameldange - GD de Luxembourg
info@eikv.org
www.eikv.org

Table of Contents

I. Table of Contents 1

1. Introduction 2

2. Glossary 4

3. Personal Data Transfer to the outside of the EU – Limitations and Restrictions ... 6

3.1. EU General Data Protection Directive 95/46/EC 8

3.2. EU General Data Protection Regulation (EU) 2016/679 10

4. Personal Data Transfer for Law Enforcement 17

4.1. Framework decision 2008/977/JHA and directive (EU) 2016/680 17

4.2. Umbrella Agreement 18

4.3. Judicial Redress Act 20

5. Personal Data Transfer for Commercial Use 21

5.1. The Safe Harbor Agreement 21

5.1.1. Emergence of the Safe Harbor Agreement 21

5.1.2. Definition and Procedure of the Safe Harbor Agreement 24

5.1.3. Abolition of the Safe Harbor Agreement 28

5.1.4. Impacts of the Abolition 33

5.2. Alternatives to the Safe Harbor Agreement 37

5.2.1. Agreement of Data Subject 38

5.2.2. EU-U.S. Privacy Shield Agreement 39

5.2.3. Binding Corporate Rules 45

5.2.4. EU Model Contract Clauses 48

5.2.5. Exceptional statement of facts and single contracts 52

5.2.6. Technical solutions 53

5.2.6.1. Tokenization & Pseudonymisation 54

5.2.6.2. Encryption 55

5.2.6.3. Data Center resides in the EU 56

6. Conclusion 57

II. Sources 60

1. Introduction

"I want my government to do something about my privacy
I don't want to just do it on my own." [1]

Evgeny Morozov
(Belarusian publicist)

This thesis functions as an analysis of the abolition of the Safe Harbor Agreement: a main data privacy agreement that has been in place from 26th July 2000 until 06th October 2015 between the member states of the European Union and the U.S. as a third party country, outside the European Economic and Monetary Union. The impact of the dissolution of this agreement and possible alternatives to this decision are given based on both a legal and practical standpoint concerning transatlantic data transfer, done mainly for commercial use by companies.

The goal of this analysis is to dissect the abolition of the Safe Harbor Agreement and to synthesize the actual status in regards of the alternatives and upcoming decisions regarding the legal and regulatory situation. This analysis should reflect the opinions of the different stakeholders such as governmental and European institutions as well as working parties and law experts. Solutions on how to circumvent the current problem of a missing legal basis regarding transatlantic data transfers will be highlighted throughout this analysis.

In the first chapters of the thesis the Safe Harbor Agreement as a whole will be discussed. Further the emergence and procedures of the agreement will be taken into consideration. On the other hand, corresponding directives and agreements made by the European Commission will be reviewed.

After the Safe Harbor Agreement and its procedures are discussed, an in-depth analysis of the impact of the abolishment of this agreement and its effect on both legal and economic matters is conducted. For this analysis, research will mainly be concerned with the transfer of personal data of EU individuals to U.S. companies, an act that was formerly covered by the Safe Harbor Agreement.

[1] http://www.datagovernance.com/quotes/privacy-security-quotes/

Furthermore, alternatives of the Safe Harbor Agreement – already in place or in negotiation – will be reviewed. The final abstract will outline possibilities of continuous transatlantic data transfers according to data privacy regulations complying to EU law.

2. Glossary

To understand the issues discussed in this thesis, further clarification of several terms is required; these terms will be explained below. In addition, several authorities will be listed in combination with their function.

Data subject: An individual or group from whom data is collected with the purpose of transferring it for governmental purposes or for commercial use.

Data owner: The Corporation or data processor that collects data about a data subject.

Data processor: A company or organization that processes or stores data about a data subject. For the scope of this thesis, the data processor resides in the U.S. to receive data about the data subject or through a data transmitter.

Data privacy: To protect the data subject of access to personal data by third parties.

Data protection: To protect the integrity of data, mostly performed on a company level in regards of business continuity concerns.

EU Commission: The European Commission is the EU's executive body. It represents the interests of the European Union as a whole (not the interests of individual countries). The term 'Commission' refers to both the College of Commissioners and to the institution itself. [2]

EU Parliament: The European Parliament is the EU's law-making body. It is directly elected by EU voters every 5 years. The last elections were in May 2014.[3]

EU Council: The Council of the EU is the institution representing the member states' governments. Also known informally as the EU Council, it is where national ministers from each EU country meet to adopt laws and coordinate policies.[4]

Article 29 Working Party: Conglomerate of the 28 national data privacy authorities of the European member states. The Article 29 Data Protection Working Party was set up under the Directive 95/46/EC of the European Parliament and of the Council on the 24th October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. It has advisory status and acts independently.[5]

---

[2] Comp. European Commission: About the European Commission, (2016). Internet.
[3] Comp. European Union: European Parliament, (2016). Internet.
[4] Comp. European Council: The Council of the European Union, (2015). Internet.
[5] Comp. European Commission: Article 29 Working Party, (2015). Internet.

General Data Protection Directive 95/46/EC: Data protection directive of the EU regulating data privacy principles companies need to comply with for transferring or storing of personal data of EU citizens for commercial purposes outside the EU.

GDPR: The General Data Protection Regulation is a EU regulation and the replacement of the directive 95/46/EC. The regulation contains the new data privacy principles companies need to comply with for transferring or storing of personal data of EU citizens for commercial purposes outside the EU.

Framework decision 2008/977/JHA and directive (EU) 2016/680: Pendant to the Directive 95/46/EC and the GDPR for data transfers for legal and law enforcement purposes.

Umbrella Agreement: Agreement for data transfers for law enforcement purposes between the EU and the U.S.

Judical redress act: Agreement to address the rights of citizens with EU nationality in front of U.S. courts.

Safe Harbor Agreement: Former data transfer agreement between the EU and U.S. to transfer data of the data subject lawfully to the U.S. for commercial purposes.

EU-U.S. Privacy Shield Agreement: Possible replacement for the Safe Harbor Agreement which is still under negotiation. It will contain stricter elements on the data privacy, protection and handling procedures for U.S. companies.

Binding Corporate Rules: Company agreement within corporations to ensure lawful data transfers between the different entities of the company across the globe.

EU Model Contract Clauses: Standard contractual clauses for companies released by the E.U. to amend to contracts with third parties to ensure lawful data transfers between the respective parties.

Tokenization: Method to fragment data across different lokations in combination with encryption to ensure data protection and privacy.

Pseudonymisation: Method to remove characteristics of data that can make them uniquely link to a data subject, such as name, address, etc.

3. Personal Data Transfer to the outside of the EU – Limitations and Restrictions

In today's globalized world companies as well as individuals want and need to share their private data across the globe with others in order to exploit a huge range of benefits. There can be several data-information flows within and between entities, internally within horizontal and vertical company-levels (for HR reasons), externally between the company and its partners, outsourcing firms or to third-party entities that offers a service offshore or at a more attractive place. This data, that is shared within commercial- and official entities, will contain personal information of individuals with different confidentiality level. These types of data transfer to third party countries outside the European Union is the central topic that shall be discussed in this paper. This thesis focuses solely on the data exchange between the European Union and the United States of America and is limited to this scenario.

The transfer of personal data outside the European Economic Alliance (EEA) has two distinctive types of transfers that are of significance to this thesis. The first type of transfer of personal data can be triggered by law enforcement to prevent and investigate in crime and terrorism.[6] These transfers are solely done between authorities of the transferring- and receiving country. The second type is when personal data is transferred with the intention to use it for commercial purposes. Companies in general are interested in a smooth and legal compliant data transfer for commercial purpose with the intention, for example to use this information to process tasks within low cost regions, or because a company's head quarter is located abroad and needs the personal data for different internal purposes such as HR calculations. Using personal data for commercial reasons is the more common data transfer type and will consequently be the type that will covered throughout this thesis within the context of the abolition of the Safe Harbor Agreement. This type of data-sharing is so common that it is encountered in various daily situations e.g. by uploading data to a cloud provider such as "Dropbox" [7].

A closer look will be taken at the German law, since it is very well aligned with the European law. Furthermore, Germany has one of the strictest data privacy implementation plans among any European based privacy laws. For this reason, German law can be applied as a best practice example for this thesis.

---

[6] Comp. European Comission: Questions and Answers on the EU-US data protection "Umbrella agreement", (2015). Internet.
[7] Comp. Dropbox Inc., (2016). Internet.

The German law permits the commercial transfer of personal data to third party counties under two circumstances - for either transmit (§ 3 IV 2 No. 3 Bundesdatenschutzgesetz) or commissioned data processing (§11 Bundesdatenschutzgesetz). The commercial transfer for either transmit or data processing will be the main focus of this paper. Therefore, both the Safe Harbor Agreement (abolished) and possible alternatives will be discussed in the chapter concerning commercial transfers.

The thesis will start out with the judicial base of data transfer outside the EEA and its legal requirements. After that, *the EU General Data Protection Directive 95/46/EC* and its replacement *the EU General Data Protection Regulation (GDPR)* will be examined. These regulations set up the requirement and the need for the different data transfer agreements and initiatives between the EU and U.S.

3.1. EU General Data Protection Directive 95/46/EC

The first requirement to transfer data outside the EEA is that the transfer needs to have the same characteristics as a data transfer within the European Union. Furthermore, valid reasons need to be given to justify the transfer outside the European Union. The receiving country, or at least the receiving company has to assure an appropriate level of data privacy for the data subject.[8] The initial directive 95/46/EC of the European Parliament and the European Council better known as the "*adequacy decision*" was the cornerstone for the framework agreement which eventually resulted in the Safe Harbor Agreement. Within this directive the EU Council and Parliament decided that there was a need for an adequate level of protection for the data that leaves the EU / EEA, as a means to protect the data subject against abuse of its data. Article 25 and 26 of the EU data directive highlight the need for the adequacy of data privacy for individuals.[9] The German law states this within §4 b II 2 BDSG.[10] According to the EU privacy law, it is forbidden to move EU citizens' data outside the EU unless the third party country has an "adequate" privacy protection-plan in place – comparable to the one in the EU.[11] In general, it is required that the privacy protection-plan in third party countries is at the same level as inside the EU.

According to the mentioned directive the "adequate" privacy protection level has to be proven on a case to case basis. As a practical approach, according to Article 25, the European Commission is able to attest a country's general data privacy status to be "adequate" to avoid time consuming and costly case to case assessments of the privacy level.[12]

This attestation is not in place for China, India and also not for the U.S. – which are the main places for today's service offerings in our data driven society. These countries do not have the same level of protection of personal data in place as the EU directive requires.[13] Therefore, the data transfer between the EU and any of the listed countries has only been possible with a larger amount of effort by the transferring and receiving companies based on individual contracts and clauses. As the U.S. will be the main focus of this thesis it is necessary to understand that the agreements of the EU with the U.S. are based on the need to assure data

[8] Comp. Borges, Georg: Datentransfer in die USA nach Safe Harbor (2015), p. 3617.
[9] Comp. European Parliament: Richtlinie 95/46/EG des Europäischen Parlaments (1995), p. 31ff.
[10] Comp. European Court: Ungültigkeit der Safe -Harbor-Entscheidung der EU betreffend die USA, (2015).
[11] Comp. Gibbs, Samuel: What is 'safe harbour' and why did the EUCJ just declare it invalid?, (2015). Internet.
[12] Comp. Borges, Georg: Datentransfer in die USA nach Safe Harbor (2015), p. 3617.
[13] Comp. Borges, Georg: Datentransfer in die USA nach Safe Harbor (2015), p. 3617.

privacy for the data subject and to find an alternative to the lack of protection of personal data in the U.S.

3.2. EU General Data Protection Regulation (EU) 2016/679

The Regulation (EU) 2016/679 - General Data Protection Regulation (GDPR)[14] is the replacement of the EU directive 95/46/EC and the EU Commission decision 2008/977/JHA (see 4.1: Framework decision 2008/977/JHA and directive (EU) 2016/680).[15] It is an "omnibus data protection law that builds upon and expands the [former EU] directive".[16] In its final state it will "ultimately replace the directive to become the single regulation for data privacy protection in the European union"[17].

Final negotiations about the concrete implementation of the GDPR started on the 24th June 2015 between the three main European governing parties (Commission, Council and Parliament) in a "trilogue". Afterwards the European Commission, the European Parliament and the European Council came to a final agreement and introduced a new era of data privacy for EU citizens' private data.[18] Discussions started in 2009 and became more concrete in 2012 with the proposal of the European Commission of the first draft of the GDPR, followed by another 3 years of formalizing the initial draft.[19] The final text of the regulation had been agreed upon on the 15th December 2015. A more than five-year discussion in politics and lobbies came to an end[20] as the final version had been released on the 14th April 2016, and will come into effect on the 25th May 2018.[21]

The EU was in a tight spot to come up with a more "modern" and enforcing underlying regulation meeting the requirements of today's digitalized economy and the need to protect EU citizens' data. The main reason for the European Union to come up with the GDPR is to have a common legal framework in regards of data protection. Until now the 28 EU member states had different implementations to comply with the EU directive 95/46/EC.[22] These different rules caused non-transparency and inconsistency for companies and countries.

---

[14] Comp. European Parliament: Regulation (EU) 2016/679 of the European Parliament and of the Council, (2016). Internet.
[15] Comp. de Hert, Paul and Papakonstantinou: The new General Data Protection Regulation: Still a sound system for the protection of individuals?, (2016) – Abstract.
[16] EYGM Limited: When is privacy not something to keep quiet about?, (2016), p.3.
[17] EYGM Limited: When is privacy not something to keep quiet about?, (2016), p.3.
[18] Comp. Long, William: EU General Data Protection Regulation comes into sharper focus, (2015), p.18.
[19] Comp. de Hert, Paul: The new General Data Protection Reulation: Still a sound system for the protection of individuals?, (2016), p.179.
[20] Comp. Ashford, Warwick: EU data protection rules will leave no organisation untouched, say legal experts, (2016), p.4.
[21] EYGM Limited: When is privacy not something to keep quiet about?, (2016), p.3.
[22] Comp. Ashford, Warwick: EU data protection rules will leave no organisation untouched, say legal experts, (2016), p.4.

Furthermore, it also had a huge economic impact as any data privacy efforts had to be set in place by the companies, and therefore this did not automatically imply compliance in all EU member states.

This new regulation will "affect every entity inside and outside the EU that holds Europeans' data" [23] and data of its citizens. Law firms and consultancies agree that the GDPR has to be taken seriously by firms even before it becomes an official law in 2018. Companies will have a grace period of two years to implement the necessary and appropriate changes to their systems to assure compliance with the GDPR. A need will arise for a complete transformation of data gathering, handling and protection of privacy as a whole.[24] Compared to the EU directive from 1995 the GDPR also applies to data processors who provide services to other organizations; this will affect especially technology provider for e.g. cloud services, etc.[25]

It is important to mention that companies residing outside of the European Union are directly affected by the GDPR and need to comply to the regulation as well this is handled under Article 3 "Territorial scope" of the regulation.[26]

The first scenario according to article 3 (1) of the GDPR would be a e.g. Swiss company processes data of a data subject residing in the EU as a part of an outsourcing arrangement.

The second scenario according to article 3 (2) a) would be on one hand a e.g. Swiss company offers goods to individuals in the EU and stores and processes data e.g. the shipping details of a data subject residing in the EU. On the other hand, a e.g. Swiss company has a subsidiary or branch in the EU offering goods or services to individuals in the EU.

The third scenario according to article 3 (2) b) would be companies that undertake a wide range of data collecting and monitoring activities of EU citizens, without really offering goods or services, e.g. Facebook or Google; this third category is also required to comply with this new regulation.[27]

---

[23] Comp. Ashford, Warwick: EU data protection rules will leave no organisation untouched, say legal experts, (2016), p.4.
[24] Comp. Ashford, Warwick: EU data protection rules will leave no organisation untouched, say legal experts, (2016), p.5.
[25] Comp. Ashford, Warwick: EU data protection rules will leave no organisation untouched, say legal experts, (2016), p.6.
[26] Comp. European Parliament: Regulation (EU) 2016/679 of the European Parliament and of the Council, (2016), Article 3. Internet.
[27] Comp. European Parliament: Regulation (EU) 2016/679 of the European Parliament and of the Council, (2016), Article 3. Internet.

This shows that mainly all third party companies and countries which do business with EU citizens fall under the GDPR regulation and need to comply to this regulation with all of its penalties and enforcement rules – not only the U.S. However, companies stay passive and wait the local governments to adjust their data protection laws (e.g. Switzerland which will obtain a data protection law draft rework by the end of October 2016).

The GDPR will have a major impact on how personal data of EU citizens will be treated.[28] In combination with the abolition of the Safe Harbor Agreement there will be a double threat to companies handling data, as on one hand the framework for free data flow has been abolished and on the other hand the data privacy laws of the EU will be enforced in stricter manner. Law firm partner Ross McKean from Olswang outlines that the GDPR will introduce the "most stringent data laws in the world" [29]. Which means costly and time consuming measures and safeguards need to be implemented by the firms to comply the GDPR.

The main aspects of the GDPR is that it comes with "increased compliance requirements" [30] towards the data processor and outlines "heavy financial penalties" [31] in case of noncompliance. These penalties can go up to 20 Million Euro or 4% of the world-wide turnover of the company groups.[32] Especially larger firms will take these fines seriously as for them the penalties easily reach a 7- to 8-digit monetary amount. The introduction of the GDPR is a step towards increasing data privacy and treatment of data of EU citizens. It will may provide data subjects with increased privacy and with better control of their personal data. Compared to the former EU directive 95/46/EC the new GDPR focuses on the strict enforcement of its requirements and regulations. As seen in the past, the regulations as well as the controlling and enforcement of these regulations, had not been taken seriously – especially in the context of the Safe Harbor Agreement, data privacy regulations have been violated by the U.S. government.

Regarding the impacts of the GDPR on companies and data subjects, an expert interview was conducted with the person responsible for this topic at Ernst & Young Switzerland: Adrian

[28] Comp. Ashford, Warwick: EU data protection rules will leave no organisation untouched, say legal experts, (2016), p.4.
[29] Ashford, Warwick: EU data protection rules will leave no organisation untouched, say legal experts, (2016), p.5.
[30] Ashford, Warwick: EU data protection rules will leave no organisation untouched, say legal experts, (2016), p.4.
[31] Ashford, Warwick: EU data protection rules will leave no organisation untouched, say legal experts, (2016), p.4.
[32] Comp. Ashford, Warwick: EU data protection rules will leave no organisation untouched, say legal experts, (2016), p.5.

Rogg (FSO). According to him, the impact of the GDPR on companies will begin even before the regulation comes into effect in 2018. Currently, companies already have to prepare and get ready to comply to the regulations set out by the GDPR. However, companies are in a more passive position at the moment, as complying to a lot of these regulation requirements will leave a huge financial impact - especially on mid-size firms. These companies are currently waiting for the final outcome of the regulation, in order to avoid unnecessary financial cost. According to Rogg, it is now up to the European Governing bodies, but also up to management consultancies like Ernst & Young to inform the firms about the potential outcomes and especially potential penalties they might suffer for noncompliance with the new regulation.

In general, Ernst & Young identifies 12 major impact points for companies and data subjects in terms of what the GDPR will mean to both of these parties after it comes into effect in 2018: [33]

1. EU residents will gain more control of their personal data.
2. Everyone has to follow the same rules.
3. Organizations will report to one supervising authority.
4. More organizations will need a data protection officer.
5. Rules advocate a risk-based approach.
6. Privacy by design becomes an enshrined requirement.
7. Organizations have 72 hours to report a breach.
8. Fines for violations are substantially higher.
9. Security is tied to risks.
10. The definition of “consent” has been significantly restricted.
11. Cross-border transfers are allowed, under certain conditions.
12. The restrictions on “profiling” is more narrow than proposed.

This new EU regulation will have a significant impact on the effort that companies need to put in, to comply with the new ruleset. Extra work required for carrying out rules such as mandatory privacy impact assessments; these assessments in particular will be costly and time consuming for companies.[34] Ernst & Young identified on one hand a big potential on consulting on the GDPR but also the need of the companies to help them conducting privacy assessment and data flow analysis as they do not have the expertise and manpower by themselves.[35]

[33] Comp. EYGM Limited: When is privacy not something to keep quiet about?, (2016), p. 3ff.
[34] Comp. EYGM Limited: When is privacy not something to keep quiet about?, (2016), p. 8.
[35] Comp. EYGM Limited: When is privacy not something to keep quiet about?, (2016), p. 11.

The Partner Stewart Room of the consultancy PwC sees three major components for companies to comply with the GDPR. "Compliance process, transparency framework and an enforcement, sanctions and remedies framework" [36]. The transparency framework will need a rework when it comes to engaging with people, especially in terms of contracting and permissions. Companies need to come up with an open door information strategy on what is happening with the personal data of the data subjects.[37] As the requirements towards compliance and legal regulations rise compared to the old directive, massive cost can occur for companies.[38] The internal and external compliance need to be built up and additional effort is needed to oversee the overall requirements of the new GDPR. Therefore, the contracting of law counsels is needed to assure legal compliance as well. A well-conceived compliance monitoring strategy needs to be put in place to assure long term compliance with the framework. Additionally, remediation measures have to be put in place as a third pillar to remediate possible noncompliance. Eduardo Ustaran, partner and European head of data protection at Hoan Lovells law firm, states that the "GDPR is loaded with requirements to make business more accountable for their data practices." [39] It is obvious that through this new regulation, companies have to change their ways of working when it comes to personal data. Concepts such as data privacy by design[40], meaning by implementing controls, even IT Systems compliance and data privacy will be the main consideration of the control / IT System design.

However, the new regulation does not only cause burdens to companies, it can help companies by being a clear simplification measure for them. The GDPR is, after the abolition of the Safe Harbor Agreement, a helpful solution and guidance tool to ensure the right measures and actions for overseas data transfer of the personal data of EU citizens. The GDPR sees "standard contractual clauses and Binding Corporate Rules (see below) as legitimate frameworks for transferring EU citizens' data out of the EUR" [41]. This framework could be a breakthrough towards a real alternative to the former Safe Harbor Agreement. Therefore, the

[36] Ashford, Warwick: EU data protection rules will leave no organisation untouched, say legal experts, (2016), p.6.
[37] Comp. Ashford, Warwick: EU data protection rules will leave no organisation untouched, say legal experts, (2016), p.6.
[38] Comp. de Hert, Paul: The new General Data Protection Reulation: Still a sound system for the protection of individuals?, (2016), p.180.
[39] Ashford, Warwick: EU data protection rules will leave no organisation untouched, say legal experts, (2016), p.6.
[40] Ashford, Warwick: EU data protection rules will leave no organisation untouched, say legal experts, (2016), p.6.
[41] Ashford, Warwick: EU data protection rules will leave no organisation untouched, say legal experts, (2016), p.7.

options companies have to transfer data in a legal manner outside of the EU in a compliant way will broaden. This will have the effect, that noncompliance to the new regulation will become harder to justify[42] by the data processors, and thereby give the data subject more security and opportunities for action in regards of transferring its personal data towards authorities and data owners.

Furthermore, Eduardo Ustaran concludes that privacy will become a standard agenda point on company's board meetings.[43] This highlights how important the topic will become as the impact of noncompliance could harm the business operations within and outside the EU.

Criticism and limitations were raised by Iheanyi Samuel Nwankwo, a research associate at the Institute for Legal Informatics in Hannover. He took a closer look of the events surrounding a disaster like natural catastrophes, epidemics or other special situations such as terroristic attacks. He concluded that there still seemed to be a lack of responsibility and guidance in events of an occurring disaster. Meaning that he feels that the data protection of individuals should be lowered when a disaster occurs in order to "protect the vital interest of the different data subjects" [44]. He feels that guidance on how to handle data processing and the extension of data processing during disasters is flawed – especially if the data subject is not able to give its agreements in these types of situations.

However, the GDPR, compared to the Data Protection Directive, does in fact consider the aspect of disaster events. According to Nwankwo, a concept of a disaster manager could be introduced. This concept would have offer special training and obligation to handle the subject's data and assure compliance to the GDPR in disaster situations.[45] Only a few countries, Australia and New Zealand as examples, adjusted their laws in regards of data processing for disaster situations. For now, it seems in the EU, only SMS alerts are used during natural disasters. According to Nwankwo, the specification of disaster situations in detail as well as respective actions and safeguards need to be defined on an EU level.[46]

---

[42] Ashford, Warwick: EU data protection rules will leave no organisation untouched, say legal experts, (2016), p.7.
[43] Comp. Ashford, Warwick: EU data protection rules will leave no organisation untouched, say legal experts, (2016), p.7.
[44] Nwankwo, Iheanyi S.: The Proposed Data Protection Regulation and its Limitations in Disaster Situations, (2016), p.05061.
[45] Comp. Nwankwo, Iheanyi S.: The Proposed Data Protection Regulation and its Limitations in Disaster Situations, (2016), p.05061.
[46] Comp. Nwankwo, Iheanyi S.: The Proposed Data Protection Regulation and its Limitations in Disaster Situations, (2016), p.05061.

Further criticism had been given during the early draft phase of the GDPR in 2015 by Article 29 Working Party. Within the initial draft, the purpose limitation of the data gathered by companies had been completely eliminated. This meant that the same data processor could use a subject's personal data for other purposes which the data subject originally did not agree to. The Article 29 Working Party found clear arguments against the absence of the purpose limitation as the control of data would be blurred this would cause further weakening of the high data protection standard within the EU and further weakening of the rights of the data subject.[47]

According to the Article 29 Working Party, as stated in their program for 2016 till 2018, their way of working will fundamentally change with the introduction of the GDPR. Their main field of work will be to act as an advising governing body and to be part of the newly formed European Data Protection Board.[48] After the introduction of the GDPR, a transitional period is set for two years, starting in April 2016. During the transition phase to the new role of the Working Party, regulations and guidance will need to be provided by all subgroups of the Article 29 Working Party. These Subgroups are dedicated to certain topics such as technology, international data transfer, the future of privacy, etc. Subgroups will help to develop the topics under the supervising authority of the Article 29 Working Party. The subgroups themselves will advise the Working Party on specific questions within their area of obligation as subject matter experts.[49]

The Working Party itself will continue to be subject matter experts on the broader data protection topics within the EU but also increase the interaction with the international data protection authorities. Furthermore, in the final regulation published on the 27th April 2016, several articles still state draft regulations and work in progress certifications. The Article 29 Data Protection Working Party will help to fill these gaps until the regulations become effective in 2018.[50] The general recommendation to companies is to conduct assessments on the data of subjects and their flows within the company. A next step within 2017 would be to data-inventory, minimize and clean inventory as well as remediate gaps for systems in which the data is stored or processed. Only then can compliance to the GDPR be assured when the regulation becomes effective in 2018.

[47] Comp. Revolidis, Ioannis and Dahi: Further Processing of Personal Data, (2015), p. 04618.
[48] Comp. Article 29 Data Protection Working Party: Work Programme 2016 – 2018, (2016), p.2.
[49] Comp. Article 29 Data Protection Working Party: Work Programme 2016 – 2018, (2016), p.3.
[50] Comp. Article 29 Data Protection Working Party: Work Programme 2016 – 2018, (2016), p.2.

4. Personal Data Transfer for Law Enforcement

4.1. Framework decision 2008/977/JHA and directive (EU) 2016/680

With the decision 2008/977/JHA from the 27th November 2008 better known as the "Framework Decision" the amendment within Article 13 of the EU General Data Protection Directive has been made. Article 13 states the legalization to transfer personal data to other EU member states for the purpose of further transfer to third party countries outside the EFA under the condition that the data is used as a means of investigation, prevention or support in criminal offense cases.

On the 27th April 2016 the European Parliament and the European Council the directive (EU) 2016/680 came into place and renewed the Council Framework Decision 2008/977/JHA from 2008.[51] The renewal can be seen as pendant to the Regulation (EU) 2016/679 also known as the General Data Protection Regulation repealed the Directive 95/46/EC for the law enforcement data transfer cases.

[51] Comp. European Commission: Reform of EU data protection rules, (2016). Internet.

4.2. Umbrella Agreement

The Umbrella Agreement was initiated to put in place a "high-level data protection framework for EU-U.S. law enforcement cooperation" [52]. The agreement gives the possibility for data-sharing between the European Union and the U.S. in regards of criminal and terror investigation. It "covers all personal data (for example names, addresses, criminal records) exchanged between the EU and the U.S." [53]. The negotiations for this agreement began officially in 2011 and concluded at the end of 2015. The negotiations resulted in an agreement about the content and a draft version of the agreement between the European Union and the U.S. had been published.[54] The Umbrella Agreement could be seen as the counterpart to the former Safe Harbor Agreement, or the later mentioned "Privacy Shield Agreement" (see Chapter 5.2.2) for the transfer of personal data for commercial purposes. While the Umbrella Agreement addresses personal data in the context of law enforcement and terror defense.

The framework itself contains certain warrants on data privacy and safeguards to ensure protection for the data subject, such as retention periods or high restrictions on onward transfers from the U.S. to other countries.[55]

The newly announced European Data Protection Supervisor (EDPS) supports the intention of the European Union and U.S. to find a common framework for law enforcement data. The institution is assigned for a five-year period from December 2014 onwards.[56] The institution is an "independent supervisory authority with responsibility for monitoring the processing of personal data by the EU institutions and bodies" [57]. The EDPS, Giovanni Buttarelli, recommends, however, on essential improvements and certain clarification for the draft version.[58]

---

[52] European Commission: Questions and Answers on the EU-US data protection "Umbrella agreement", (2015).
[53] European Commission, Questions and Answers on the EU-US data protection "Umbrella agreement", (2015).
[54] Comp. European Commission: Statement by EU Commissioner Věra Jourová on the finalisation of the EU-US negotiations on the data protection "Umbrella Agreement", (2015).
[55] Comp. European Commission: Questions and Answers on the EU-US data protection "Umbrella agreement", (2015).
[56] Comp. European Data Protection Supervisor: EDPS welcomes EU-US "Umbrella Agreement" and stresses need for effective safeguards, (2016).
[57] European Data Protection Supervisor: EDPS welcomes EU-US "Umbrella Agreement" and stresses need for effective safeguards, (2016).
[58] Comp. European Data Protection Supervisor: EDPS welcomes EU-US "Umbrella Agreement" and stresses need for effective safeguards, (2016).

The main reason the agreement is restrained is that it will not "come into force until the U.S. Judicial Redress Bill (see below) has become law in the U.S." [59]. The agreement finally broke down after U.S. government refused to grant EU citizens the right to address legal matters in U.S. Courts accordingly.[60] In 2016, the Judicial Redress Act has been signed and the topic has been revisited and it needs to be looked into how negotiations will continue.

[59] Comp. Long, William and Blythe: EU-US Data Protection "Umbrella Agreement" Finalised, (2015). Internet.
[60] Comp. DeGraw, James et al.: Worldwide: The U.S.-EU Safe Harbor Framework Is Invalid: Now What?, (2015). Internet.

4.3.Judicial Redress Act

The Judicial Redress Act is an agreement to address the rights of citizens with EU nationality in front of U.S. courts. [61] On the 24th February 2016, U.S. President Obama signed the Judicial Redress Act and it became a law.[62]

The Judicial Redress Act has been a base for the "EU General Data Protection Regulation" as the European Commission was not willing to sign the contracts with U.S. authorities until EU passport holders could redress judicial in front of U.S. courts, either if data had been collected for commercial purposes or for law persecution.

The EDPS, Giovanni Buttarelli, criticized that the Judicial Redress Act only grants EU passport holders and member states the right to judicial redress. This leaves a gap for non EU-nationals, having a EU residence, to have the right "to challenge how their data is handled in the U.S.".[63]

[61] Comp. Spies, USA: Judicial Redress Act verabschiedet, (2016), p.05005.
[62] Comp. Sidley Austin LLP: President Obama Signs Judicial Redress Act, (2016). Internet.
[63] Stupp, Catherine: Commission's 'Umbrella Agreement' with US under fire from MEPs, (2015). Internet.

5. Personal Data Transfer for Commercial Use

5.1. The Safe Harbor Agreement

The following chapter will first cover the description of the Safe Harbor Agreement and the reason for its initial emergence. It will then give an overview of what the Safe Harbor Agreement contains, including its principles and coverage from a data privacy perspective for the data subject.

5.1.1. Emergence of the Safe Harbor Agreement

The Safe Harbor Agreement was put in place to ensure a general way within the European Union and across its member states to share personal data of individual data subjects for business purposes with the U.S. As individual case by case contracts or agreements had been very costly and time consuming, an interstate level agreement was the only way to ensure the accuracy of data transfer to third party countries such as the U.S. in general. This transatlantic agreement should provide the possibility of a free data flow of personal data from the European Union to the U.S. with no need for further paper work. The Safe Harbor Agreement was seen as a "one stop shop"[64] as no individual contracts or agreements had to be made e.g. with individual member states of the EU or on a company level.[65]

Until the Safe Harbor Agreement came into effect, the data flow was limited to the data interchange between the EU member states and countries that had an adequate level of data privacy in regards of personal data and their protection. The adequacy is commonly defined as the same level of protection and safeguards guaranteed within the European Union.

The economic need of a data exchange, increased by the emergence of a data driven society and business models, required the European Commission in coordination with the U.S. government and its counterpart also known as the U.S. Department of Commerce set up an agreement. Through the missing agreement between the EU and the U.S. became a main agenda point for both governments to reinsure that the data transfers to U.S. companies will be lawful again. The EU wants to ensure that U.S. companies comply to the EU data privacy

[64] Gibbs, Samuel: What is „safe harbour" and why did the EUCJ just declare it invalid, 2015. Internet.
[65] Comp. Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit: Safe Harbor – Datenschutz-Wiki, (2016). Internet.

standards where the U.S. wants again a free data flow without additional need for single contracts.

The discussion about a specific framework filling this gap took place on the 26th July 2000, resulting in the EU decision 2000/520/EC known as the "Safe Harbor Agreement". This decision was pursuant to the directive 95/46/EC.[66] The European Commission accepted, with the decision based on Article 25 VI of the directive 95/46/EC – the EU data privacy standard – the Safe Harbor principles, published by the U.S. Department of Commerce.[67] The U.S. published Further Asked Questions (FAQ) about the Safe Harbor Agreement in the publication of the Official Journal 215 from the 28th August 2000, p.7.[68] These FAQ gave guidelines to companies in regards to the principles and how data transfer, storage, and processing had to be conducted in order to comply to the EU data privacy law. With help of the FAQs companies had guidelines on implementing the safeguards and controls in order to comply to the Safe Harbor standards while conducting business.

Several adjustments and reviews for the possibilities of data transfer were made to the original directive from 2000. However, the 15-year-old agreement on the transatlantic data transfer earned critique from different sides. On the 27th November 2013 the EU Commission published their report regarding the Safe Harbor Agreement with a collection of thirteen recommendations to restore the trust in the EU-U.S. data flows. The EU Commission campaigned for the retention of the Safe Harbor Agreement.[69]

This retention could only be possible with adjustments to the current Safe Harbor Agreement that was drawn up by the EU Commission at the time. Therefore, three recommendations, that were hard to accept by the U.S. Department of Commerce, should be in focus: [70]

- Transparency: "All contracts with subcontractor need to be published"
- Enforcement: "A certain percentage of Safe Harbor Certified companies should be reviewed in regards of complying with the Safe Harbor Principles (see below)"
- Access through U.S. authorities: "Companies have to publish information about the extend U.S. authorities can access data and under which circumstances"

[66] Comp. Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit: Safe Harbor, 2016. Internet.
[67] Comp. Grau, Timon and Granetzny: EU-US-Privacy Shield, (2016), p.405 – Paragraph I.
[68] Comp. ARTICLE 29 DATA PROTECTION WORKING PARTY: Working Document on Functioning of the Safe Harbor Agreement, (2002), p.2.
[69] Comp. Spies: EU-Kommission äußert sich zu EU/US-Safe Harbor – 13 Empfehlungen, (2013), p.03837.
[70] Comp. Spies: EU-Kommission äußert sich zu EU/US-Safe Harbor – 13 Empfehlungen, (2013), p.03837.

Several years the Safe Harbor Agreement functioned as a more or less effective safeguard and framework for the transfer of the personal data for commercial purpose from the EU to the U.S. However, this agreement contained several gaps, which were also caused by its age and the data practices that U.S. authorities have in place; this introduced a wave of criticism against the framework, which will be discussed further in the next chapter.

5.1.2. Definition and Procedure of the Safe Harbor Agreement

The Safe Harbor Agreement, as mentioned in the previous chapter, should fill the gap of the missing data privacy laws in the U.S. which would prevent the legal transfer of personal data from the EU to U.S. The participation to the agreement as a firm was on basis of a self-certification of the companies in the U.S.

Mainly the Safe Harbor Agreement has seven underpinning principles which companies had to fulfill for their self-certification.[71] These principles should mainly govern the data treatment and data privacy within U.S. territory.

Following the seven principles published by the U.S. Department of Commerce: [72]

***NOTICE**: An organization must inform individuals about the purposes for which it collects and uses information about them, how to contact the organization with any inquiries or complaints, the types of third parties to which it discloses the information, and the choices and means the organization offers individuals for limiting its use and disclosure. This notice must be provided in clear and conspicuous language when individuals are first asked to provide personal information to the organization or as soon thereafter as is practicable, but in any event before the organization uses such information for a purpose other than that for which it was originally collected or processed by the transferring organization or discloses it for the first time to a third party.*

***CHOICE**: An organization must offer individuals the opportunity to choose (opt out) whether their personal information is (a) to be disclosed to a third party or (b) to be used for a purpose that is incompatible with the purpose(s) for which it was originally collected or subsequently authorized by the individual. Individuals must be provided with clear and conspicuous, readily available, and affordable mechanisms to exercise choice.*

For sensitive information (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), they must be given affirmative or explicit (opt in) choice if the information is to be disclosed to a third party or used

[71] Comp. Borges, Georg: Datentransfer in die USA nach Safe Harbor, (2015), p.3617 – Paragraph III.
[72] U.S. DEPARTMENT OF COMMERCE: SAFE HARBOR PRIVACY PRINCIPLES, (2009). Internet.

for a purpose other than those for which it was originally collected or subsequently authorized by the individual through the exercise of opt in choice. In any case, an organization should treat as sensitive any information received from a third party where the third party treats and identifies it as sensitive.

***ONWARD TRANSFER**: To disclose information to a third party, organizations must apply the Notice and Choice Principles. Where an organization wishes to transfer information to a third party that is acting as an agent, as described in the endnote, it may do so if it first either ascertains that the third party subscribes to the Principles or is subject to the Directive or another adequacy finding or enters into a written agreement with such third party requiring that the third party provide at least the same level of privacy protection as is required by the relevant Principles. If the organization complies with these requirements, it shall not be held responsible (unless the organization agrees otherwise) when a third party to which it transfers such information processes it in a way contrary to any restrictions or representations, unless the organization knew or should have known the third party would process it in such a contrary way and the organization has not taken reasonable steps to prevent or stop such processing.*

***SECURITY**: Organizations creating, maintaining, using or disseminating personal information must take reasonable precautions to protect it from loss, misuse and unauthorized access, disclosure, alteration and destruction.*

***DATA INTEGRITY**: Consistent with the Principles, personal information must be relevant for the purposes for which it is to be used. An organization may not process personal information in a way that is incompatible with the purposes for which it has been collected or subsequently authorized by the individual. To the extent necessary for those purposes, an organization should take reasonable steps to ensure that data is reliable for its intended use, accurate, complete, and current.*

***ACCESS**: Individuals must have access to personal information about them that an organization holds and be able to correct, amend, or delete that information where it is inaccurate, except where the burden or expense of providing access would be disproportionate to the risks to the individual's privacy in the case in question, or where the rights of persons other than the individual would be violated.*

***ENFORCEMENT**: Effective privacy protection must include mechanisms for assuring compliance with the Principles, recourse for individuals to whom the data relate affected by non-compliance with the Principles, and consequences for the organization when the Principles are*

not followed. At a minimum, such mechanisms must include (a) readily available and affordable independent recourse mechanisms by which each individual's complaints and disputes are investigated and resolved by reference to the Principles and damages awarded where the applicable law or private sector initiatives so provide; (b) follow up procedures for verifying that the attestations and assertions businesses make about their privacy practices are true and that privacy practices have been implemented as presented; and (c) obligations to remedy problems arising out of failure to comply with the Principles by organizations announcing their adherence to them and consequences for such organizations. Sanctions must be sufficiently rigorous to ensure compliance by organizations.

The seven principles mainly introduced the concept of informing data subjects, thereby giving them the choice to decide what their data can be used for and to give them the ability to restrict the onward transfer of their data to third parties. The companies need to assure the security of the data and that the integrity of the data is assured. Furthermore, the data subject should be able to raise complaints against the processing companies in regards of their personal data and the treatment of this data.[73]

The U.S. Department of Commerce in cooperation with the European Commission developed and published these principles.[74] Companies could review the principles on the governmental website export.gov[75]. This website collects all kind of export and trade relevant information from different U.S. government departments and market researches[76]. Moreover, the site contains a list of the companies that have complied to the previously mentioned principles and thereby signed up for self-certification.

The list of self-certified companies identifies the companies and their corresponding current status. The status for certified companies that complied to the Safe Harbor Agreement were listed with the flag “current”. This means those companies declare to comply to the principles and had undergone their current recertification. However, there were also companies that were listed with the status “not current” meaning that recertification had been missed.[77]

---

[73] Comp. Die Bundesbeauftragte für den Datenschutz und die Infromationsfreiheit: Safe Harbor, (2015). Internet.
[74] Comp. Borges, Georg: Datentransfer in die USA nach Safe Harbor, (2015), p.3617 – Paragraph III.
[75] US Government: SAFE HARBOR PRIVACY PRINCIPLES, (2009). Internet.
[76] US Government: Export.gov Helps American Companies Succeed Globally, (2015). Internet.
[77] Comp. European Commission: Communication from the Commission to the European Parliament and the Council on the functioning of the Safe Harbour from the perspective of EU Citizens and Companies Established in the EU, (2013), p.4 – Paragraph 2.2 and foot note 13.

This act of self-certification had been a declaration of the companies that they comply to the Safe Harbor principles. Furthermore, the companies had to apply a privacy policy, which was required to be publicly available on their corporate website. The self-certification process had to be repeated annually.[78]

The main problem about the self-certification had been the self-accreditation and the principles themselves. They had a wide scope of interpretation which did not fully ensure safeguarding according to an expert's opinion.[79] There were no control mechanisms in place in order for companies to complete the self-certification process and to comply to the principles. No authority or independent third party did a verification of the data practices of the companies that wanted to be certified. The European Commission's decision states that in order "to meet the verification requirements of the Enforcement Principle, an organization may verify such attestations and assertions either through self-assessment or outside compliance reviews".[80] This self-certification with a control mechanism to assess applying companies, based on a self-assessment, seems to be inefficient and ineffective from an EU standpoint in regards of enforcement or oversight. The question left open is, if the companies were self-certified, did they then really comply with the principles of the Safe Harbor Agreement?

[78] Comp. Borges, Georg: Datentransfer in die USA nach Safe Harbor, (2015), p.3617 – Paragraph III.
[79] Comp. Borges, Georg: Datentransfer in die USA nach Safe Harbor, (2015), p.3617 – Paragraph III.
[80] European Comission: Offical Journal of the European Communities, (2000), p.L 215/16 FAQ 7.

5.1.3. Abolition of the Safe Harbor Agreement

This section will canvas the abolition of the Safe Harbor Agreement as a result of the European Court's decision on the 06th October 2015. With this decision the European Court precipitated a fundamental change in regards of material data privacy regulations, as the requirements of international data transfer were intensified and became a main topic of attention.[81]

Several circumstances led to this final decision for abolition taken by the court. The main topic that the court questioned was, from an overall standpoint, if the Safe Harbor Framework, how it functioned at the time, had ever been effective in its methods of assurance of compliance and verification of self-certified companies. This concern was also raised by the data protection commissions of the EU member states. Therefore, the doubts concerning the validity of an adequate data protection level and the self-certification of companies as valid proof of compliance to this level could be seen as a main reason for the abolition of the framework.

The self-certification itself had been topic in several conferences of the highest German data privacy authority. In a first conclusion they stated that European companies have to ensure, before any data transfer of personal data outside of the EU is conducted, that the receiving company completely ensures an "adequate" and comparable data privacy level similar to the one of the European Union. They came to this conclusion as neither the EU nor the American authorities have an effective system in place that enforces and controls the compliance towards the Safe Harbor principles. The authority further stated that the companies cannot only rely on the Safe Harbor Certification.[82] This shows how deeply the data privacy authorities within the European Union distrusted the Safe Harbor Agreement and it shows indirectly how the whole situation with the agreement began to unravel.

The protocol of the conference additionally stated that the companies would have to demand proof from the data receiver about the adequacy of their data privacy principles and to verify if their Safe Harbor certification was still valid. Another very important point is that the information obligation had to be conducted by the receiving company towards

[81] Comp. Borges, Georg: Datentransfer in die USA nach Safe Harbor, (2015), p.3617 – Paragraph I.
[82] Comp. Düsseldofer Kreis: Beschluss der obersten Aufsichtsbehörden, (2010), p.1.

the data subject.[83] This meant that any information about the purpose of the data transfer and gathering, and how complaints against the company and the data transfer itself could be pointed out should've been made clear to the data subject before any personal data could be transferred. Onward transfers to third parties needed to be disclosed as well, according to this obligation.[84] This highlights how the data privacy authorities tried to ensure compliance to the Safe Harbor principles by the certified companies and the missing control over the principles of EU or U.S. authorities, by making the transmitting companies perform the controls for them. This meant that whenever transmitting companies observed any noncompliance or irregularities, they were obligated to report this to the appropriate data privacy authorities.[85]

Another inconsistency of the Safe Harbor Agreement was shown by a study conducted by the European Commission in 2004; this study addressed the high amount of implementation deficiencies the Safe Harbor Agreement had.[86] These deficiencies mostly refer to the inability for the data subject to access information through the corporate website to find out about the treatment and ability to dispose of their personal data. Another common deficiency was the absence of a link or the use of misleading links to the company's privacy policies by refraining from referring to the Federal Trade Commission's List (DOC certification page) so the data subject could not sufficiently verify if the company in question was really on the Safe Harbor list of self-certified companies.[87] Other points of criticism were the different labeling schemes used by companies, that made it impossible for the data subject of the corporate sites to identify adequate privacy policies.[88] Another study from 2008 concludes that only 348 of the 1109 registered companies with the status current fulfill the criteria to be safe harbor certified.[89] These deficiencies are clear offenses against the seven Safe Harbor Principles and highlight the ineffectiveness of the entire framework.

The grievances of the Safe Harbor Agreement come to an extend shown in the communique of the European Commission to the European Parliament about the

[83] Comp. Düsseldofer Kreis: Beschluss der obersten Aufsichtsbehörden, (2010), p.1.
[84] Comp. Düsseldofer Kreis: Beschluss der obersten Aufsichtsbehörden, (2010), p.1 – Foot note 2.
[85] Comp. Düsseldofer Kreis: Beschluss der obersten Aufsichtsbehörden, (2010), p.2.
[86] Comp. Dhont, Jan et al.: Safe Harbour Decision Implementation Study, (2004), p.62ff.
[87] Comp. Dhont, Jan et al.: Safe Harbour Decision Implementation Study, (2004), p.63.
[88] Comp. Dhont, Jan et al.: Safe Harbour Decision Implementation Study, (2004), p.62f.
[89] Comp. Borges, Georg: Datentransfer in die USA nach Safe Harbor, (2015), p.3618 – Paragraph III.

functioning of the Safe Harbor Agreement.[90] The most grave circumstance had been the fact, that around 10% of the companies claiming membership within the Safe Harbor Agreement are not even listed in the Department of Commerce's list of Safe Harbor self-certified companies.[91] This false statement of membership had been reviewed by an Australian consultancy, which concluded that the number of false claims from 2008 to 2013 had more than doubled.[92] These false claims had a serious impact on the trustworthiness of the Safe Harbor Agreement and shows once again the inefficient - or not existing - control mechanisms and safeguards. Neither had there been an effective method implemented to sanction infringements against the Safe Harbor principles by the U.S. authorities nor were companies actually sanctioned.[93] The framework had not been actively policed neither had there been audits of the certified companies in regards of correctness or false claims. Neither the U.S. Federal Trade Commission nor the European Data Privacy Authorities actively conducted any reviews.[94]

Another topic raised by the European Commission was the exponential increase in data flow and the critical importance of the transatlantic data flows for the economy. This fact made the European Commission review the Safe Harbor Agreement and the rapid growth of companies which applied for the Safe Harbor Agreement which resulted in even more attention of the European Commission in the self-certification issue.[95]

A main reason that the whole Safe Harbor Framework suffered shipwreck is mainly the circumstance that, through the Whistleblower Eduard Snowden, the practices of the U.S. government in regards of governmental access to personal data of EU citizens, had been disclosed.[96]

---

[90] Comp. European Commission: Communication on the Functioning of the Safe Harbour [Agreement], (2013), p.6ff.
[91] Comp. European Commission: Communication on the Functioning of the Safe Harbour [Agreement], (2013), p.7.
[92] Comp. European Commission: Communication on the Functioning of the Safe Harbour [Agreement], (2013), p.7 – Footer 24.
[93] Comp. Borges, Georg: Datentransfer in die USA nach Safe Harbor, (2015), p.3618 – Paragraph III.
[94] Comp. DeGraw, James et al.: Worldwide: The U.S.-EU Safe Harbor Framework Is Invalid: Now What?, (2015). Internet.
[95] Comp. European Commission: Communication on the Functioning of the Safe Harbour [Agreement], (2013), p.3.
[96] Comp. European Commission: Communication on the Functioning of the Safe Harbour [Agreement], (2013), p.3.

The problem resides here within the U.S. law and data privacy act as it appears to have major deficiencies compared to the European data privacy law.[97] From an American standpoint the data privacy principles reside on the systematic "right to be let alone"; this means for the individual that on a case based decision this right is either given or not.[98] This expresses the fundamental difference with European Privacy law. The U.S. government possesses the right to obtain mass access to private data for processing and gathering.[99] The basis of these laws are the Patriot Act and the Foreign Intelligence Surveillance Act.[100] Borges further questions the fact if the Freedom Act from the 02nd June 2015 should restrict the rights of U.S. authorities to access personal data by mass surveillance.[101]

The disclosure of the U.S. data privacy practices made Mr. Maximilian Schrems, an Austrian data privacy activist, rise complaints against Facebook transferring personal data of its users to the U.S.[102] Mr. Schrems first rose the complaints at the Irish data protection commissioner, as Facebook's European subsidiary is based in Ireland. The Irish data protection commissioner reacted by dismissing the complaints, arguing that according to the Safe Harbor Agreement all data flows and its compliance was assured.[103]

This dismissing of the issue caused Mr. Schrems to go in front of court against the commissioner and Facebook. The case is known as C-362/14 Maximilian Schrems vs. Data Protection Commissioner[104] at Irish High Court. The Court rose two questions: whether the actions Facebook took, especially participation in the National Security Agency's (NSA) PRISM Program, comply with the Safe Harbor Framework and whether the framework in general is "functioning as intended".[105]

---

[97] Comp. Borges, Georg: Datentransfer in die USA nach Safe Harbor, (2015), p.3618 – Paragraph III.
[98] Comp. Borges, Georg: Datentransfer in die USA nach Safe Harbor, (2015), p.3618 – Paragraph III.; Comp. Warren, Samuel and Brandeis: Das Recht auf Privatheit The Right to Privacy, (2011). Internet.
[99] Comp. Borges, Georg: Cloud Computing, (2016), p.512f.
[100] Comp. Borges, Georg: Datentransfer in die USA nach Safe Harbor, (2015), p.3618 – Paragraph III.
[101] Comp. Borges, Georg: Datentransfer in die USA nach Safe Harbor, (2015), p.3618 – Paragraph III.
[102] Comp. DeGraw, James et al.: Worldwide: The U.S.-EU Safe Harbor Framework Is Invalid: Now What?, (2015). Internet.
[103] European Court: InfoCuria - Rechtsprechung des Gerichtshofs - ECLI:EU:C:2015:650, (2015), Paragraph 28.
[104] Comp. DeGraw, James et al.: Worldwide: The U.S.-EU Safe Harbor Framework Is Invalid: Now What?, (2015). Internet.
[105] DeGraw, James et al.: Worldwide: The U.S.-EU Safe Harbor Framework Is Invalid: Now What?, (2015). Internet.

The EU Advocate General published his opinion on these two matters on the 23rd September 2015 in a general statement which was not binding for the European Commission.[106] He concluded that on one hand surveillance by the government is a necessary action to prevent criminal offenses and terrorism. However, the extent to which the U.S. government's agencies such as the NSA and others collected data of EU citizens "demonstrated an over-reach".[107] The Advocate General further complained that the European Commission accepted these deficiencies in 2013 and had not already suspended the Safe Harbor Agreement in 2014, while further negotiations were held with the U.S. on the malfunction of the framework.[108]

On the 06th October 2015 the European Court took a decision in the Case C-362/14 of Mister Schrems.

Looking at the final decision of the European Court the Advocate General's opinion had been carried out with certain exceptions. With this final decision the court made the invalidity of the Safe Harbor Agreement effective. In the ruling under point two the final decision can be found, where the court states that decision 2000/520 (Safe Harbor Agreement) is invalid.[109] This ruling caused all data transfer to third party in the U.S. to not be covered anymore under the umbrella of the Safe Harbor Agreement. Therefore, companies that did not have other safeguards in place would not be allowed to transfer their data across borders.

[106] Comp. BOT, ADVOCATE GENERAL: Opinion of Advocate General Bot delivered on 23 September 2015 - Case C-362/14, (2015).
[107] Comp. DeGraw, James et al.: Worldwide: The U.S.-EU Safe Harbor Framework Is Invalid: Now What?, (2015). Internet.
[108] Comp. DeGraw, James et al.: Worldwide: The U.S.-EU Safe Harbor Framework Is Invalid: Now What?, (2015). Internet.
[109] Comp. European Court: InfoCuria - Rechtsprechung des Gerichtshofs - ECLI:EU:C:2015:650, (2015).

5.1.4. Impacts of the Abolition

The first way in which the impact of the abolition can be established, is for one to have a look at the companies that used the Safe Harbor Agreement as a main legal framework to transfer personal data to the U.S. For these company's the legal basis to transfer or even store the subject's information in the U.S. had disappeared from one day to another. From an economic standpoint the abolition is a disaster, as some of the affected company's main business model is based on data gathering, data transfer and storage or the processing of this data. Especially German regulators found clear arguments in regards of the abolition and the further possibility of data transfers. They clearly stated that they will "prohibit any data transfers still based on Safe Harbor that come to their knowledge without any grace period". [110] Furthermore, the data protection authorities of the European Union will not allow new data transfers based on the Safe Harbor Agreement. The main problem resulting from this for companies is the missing grace period as they are forced to react immediately and to come up with alternative solutions and safeguards for data that is transferred to the U.S. ad hoc. Within this timeframe it was nearly impossible for these companies to react or to come up with valid alternatives.

However, it had been a two-sided coin for the 3246 Safe Harbor certified companies.[111] Not all companies fully relied on the Safe Harbor Agreement as an effective safeguard, they already had model contract clauses or other contractual frameworks in place protecting their data transfer of personal data to the U.S. As the Safe Harbor Agreement has been known as a risky solution for quite some time, as more and more critics rose, so the companies were already searching for possible solutions.

An easy transatlantic data flow is a main business driver for services offered abroad but also for EU companies that want to transfer their data to outsource services or within their companies for HR purposes. Without approved data flows business as usual would not be possible. Mainly for companies that have a high amount of personal data, a lot of data owners, a high frequency in changes and massive data relationships e.g. high number of processors or onward transfers, felt a vast impact of the missing framework. They needed to completely rethink all data flows and to immediately kick off assessments to identify their legal situation.

---

[110] Taylor Wessing LLP: Safe Harbor is invalid. Now what?, (2015). Internet.

[111] On 26 September 2013 the number of Safe Harbour organizations listed as "current" on the Safe Harbor List was 3246, as "not current" 935. (European Commission: Communication from the Commission to the European Parliament and the Council on the functioning of the Safe Harbour from the perspective of EU Citizens and Companies Established in the EU, (2013), p.4.)

The main problem without a framework agreement is the number of single contracts that companies need to have with different vendors, or transmitting- and receiving companies to ensure legal compliance. As the number of contracts and legal work is mostly not feasible or even affordable, the companies are not able to legally compliant continue with the transfer of data or even with their whole business. Efforts would occur for the analysis of each contract that is in place as well as data relations which have no contractual agreement at the moment. Furthermore, the gathering for alternative solutions would have a high cost impact as well as an intense effort by the companies is required.[112] Especially with different data relations in place, companies would need to have different safeguards in place as well. Another part of the analysis is that the companies need to conduct a second layer of assessment to identify and analyze the third parties within the data transfers they conduct, especially for the cases of onward transfers.[113] Therefore, the companies need to conduct an in-depth evaluation of the third parties and their data treatment and privacy practices. This part had been covered before by the Safe Harbor Agreement and did not needed to be conducted then. Also the law firm Ropes & Gray states that the investigation on possibilities to comply after the abolition of the framework should not be underestimated and can have a huge economical and procedural impact for the whole industry.[114]

As stated, the inheriting efforts have a huge economical and reputational impact, so the demands for a new framework agreement become higher and the finalization of the negations about such an agreement are urgently needed.[115]

Direct reactions on the stock market should be taken into consideration when analyzing the impact of the abolition. Just after the court decision about the abolition of the Safe Harbor Framework, the shares of Facebook and Google dropped about one percent before stock markets opened.[116] However, these companies did not fully rely on just the Safe Harbor Agreement and used certain alternatives that are mentioned in the chapters with the alternatives below.

---

[112] Comp. DeGraw, James et al.: Worldwide: The U.S.-EU Safe Harbor Framework Is Invalid: Now What?, (2015). Internet.
[113] Comp. DeGraw, James et al.: Worldwide: The U.S.-EU Safe Harbor Framework Is Invalid: Now What?, (2015). Internet.
[114] Comp. DeGraw, James et al.: Worldwide: The U.S.-EU Safe Harbor Framework Is Invalid: Now What?, (2015). Internet.
[115] Comp. European Commission: Communication from the Commission to the European Parliament and the Council on the functioning of the Safe Harbour from the perspective of EU Citizens and Companies Established in the EU, (2013), p.4.
[116] Comp. Reuters: Aktien von Facebook und Google nach EuGH-Urteil im Minus, (2015), p.1. Internet.

For the data subject the main impact of the abolition is the protection of the individual's data privacy, especially that there is less access by U.S. authorities. This strengthens the position of the data protection authorities in the EU and leads to an overall better situation for the data subject in regards of the safeguards of the data of the subject. However, a disadvantage for the data subject could be the missing of certain services and offerings; these services might not be provided anymore in the European Union after the abolition of the framework.

The impact of the abolition of the Safe Harbor Agreement from a law standpoint is not yet assessed in full detail. However, all data transfers relied on the Safe Harbor Agreement and to only rely on this agreement has become invalid at the moment the EU court decided to abolish the agreement.

Overall, the decision of the court could open the door to further complaints and lawsuits in regards of the data transmission of EU citizens' personal data that will be comparable to the court case of Mr. Schrems.

The data protection authorities of the EU stated that companies should stay calm and take a pragmatic approach. [117] Furthermore, they refer to the alternative solutions mentioned further down in the chapters about the different alternatives.[118] The German Data Protection Commission stated that under certain circumstances data transfers of personal data could be allowed, if these are not of a recurring nature. Furthermore, data of employees can be excluded from the transfer ban if a special agreement is made.[119]

According to Marx and Wüsthof there is "no absolute prohibition of the data transmission" [120] itself. They refer to a statement of the Article 29 Working Party, within this article it says that data transfers will still be done under the Safe Harbor Agreement anyway, even after the court's decision concerning the abolition.[121] Even though these transfers are unlawful, they cannot be prevented as companies need to figure out ways to comply with the changed situation and continue their business. Further Marx and Wüsthof discuss different alternatives

[117] Comp. DeGraw, James et al.: Worldwide: The U.S.-EU Safe Harbor Framework Is Invalid: Now What?, (2015). Internet.
[118] Comp. DeGraw, James et al.: Worldwide: The U.S.-EU Safe Harbor Framework Is Invalid: Now What?, (2015). Internet.
[119] Comp. Landesamt für Datenschutzaufsicht (BayLDA): Sondersitzung der DSK am 21. Oktober 2015 in Frankfurt, (2015). Internet.
[120] Comp. Marx, Lorenz and Wüsthof: CJEU shuts down Safe Harbor for Transatlantic Data Transfer, (2015), p.245.
[121] Comp. Marx, Lorenz and Wüsthof: CJEU shuts down Safe Harbor for Transatlantic Data Transfer, (2015), p.245.

how to counter the dilemma of a missing framework and the need business need of the ongoing of the data transfers.[122]

At the moment there seems to be no real solution to address the problem of a missing umbrella framework, which results in a situation of uncertainty for companies. However, with the doubts concerning the validity of the Safe Harbor Agreement before it was abolished, the number of companies that were solely relying on the framework have decreased and companies starting looking more and more into other solutions to ensure data privacy and protection for data subjects.

The next chapter will give more information regarding a possible solution and safeguards for lawful transfers of personal data with a missing framework agreement.

[122] Comp. Marx, Lorenz and Wüsthof: CJEU shuts down Safe Harbor for Transatlantic Data Transfer, (2015), p.245f.

5.2. Alternatives to the Safe Harbor Agreement

Through the European Court's decision to declare the Safe Harbor Agreement as invalid, the need for alternative measures was increased; this started many discussions about how to proceed with intercontinental data transfers. Even before the court's decision, companies were already able to recognize that the Safe Harbor Agreement was a dinosaur.

According to European law and in particular the German law, handled in §4 c Bundesdatenschutzgesetz Article 25 (Datenschutzregulation), data transfers to a third party country without an "appropriate" level of data privacy and protection compared to the EU can be executed under certain conditions.[123] Some of these methods, such as Binding Corporate Rules or Modal Contract Clauses, had been in use even when the Safe Harbor Agreement was still in place. Other methods are still discussed between member states of the EU and the U.S. government and other countries.

Monique Goyens, the director of the European Consumer Organization, stated that U.S. firms would just need to comply with the EU data privacy principles and guarantee an "adequate level of protection in line with EU rules"[124]. The problem with this is that, on one hand the big firms will have an extensive amount of paperwork to conduct to comply to the EU rules, and on the other hand the U.S. data privacy practices, especially those of secret services, will prevent companies in U.S. to be able to be compliant.[125]

Following the different alternatives for transatlantic data transfer, still possible after the abolition of the Safe Harbor Agreement, will be outlined. The opinions differ a lot in terms of adequacy of the different solutions and right now there is no right or wrong as the whole abolition topic brought a remaining uncertainty to intercontinental data transfers.

[123] Comp. Borges, Georg: Datentransfer in die USA nach Safe Harbor, (2015), p.3617 – Paragraph II.
[124] Gibbs, Samuel: What is 'safe harbour' and why did the EUCJ just declare it invalid?, (2015), Internet.
[125] Comp. Gibbs, Samuel: What is 'safe harbour' and why did the EUCJ just declare it invalid?, (2015), Internet.

5.2.1. Agreement of Data Subject

The first and ultimate solution to transfer data issues to a third party country that does not have "adequate" data privacy safeguards in place, would be an agreement and acknowledgement of the data subject himself: the so-called "unambiguous consent" of the data subject.[126] The individual is the person that the data is about, and at this individual's will this data can be disposed of.[127] If such an agreement were to be in place, the transmitting company has a comprehensive permission to transfer the data subject's data according to. §4 c I No. 1 Bundesdatenschutzgesetz (BDSG), Art. 26 a (Datenschutz Richtline). This enables companies to transfer data no matter if the Safe Harbor Framework is in place or not. However, this possibility also implies that the data subject gets informed on the impact of the data transfer and the lack of data privacy safeguards in the receiving country, which could harm the data subject's willingness to agree to the data transfer. Also, before each data transfer can be carried out, the submitting companies needs to obtain, the data subject's formal permission. This would be an intense effort for both parties and is therefore deemed as impractical as an alternative by Ronald Kogens (EY Zurich, Lawyer).

[126] Comp. DeGraw, James et al.: Worldwide: The U.S.-EU Safe Harbor Framework Is Invalid: Now What?, (2015). Internet.
[127] Comp. Borges, Georg: Datentransfer in die USA nach Safe Harbor, (2015), p.3617.

5.2.2. EU-U.S. Privacy Shield Agreement

The EU-U.S. Privacy Shield is one of three measures the EU Commission initiated to restore the trust in transatlantic data transferring. It was announced within the EU legislative package next to the EU data privacy reform (GDPR) and the EU-U.S. framework agreement on data transfer regarding prosecution which will be detailed below.[128] It should replace the invalid Safe Harbor Agreement.

The EU-U.S. Privacy Shield is a direct outcome of the court case of Mr. Schrems and the resulting sentence as well as the requirements given by the EU court.[129] The European Union introduced a full document set containing the Privacy Shield documents itself and several amendment sections; these amendments are a set of additional papers to the EU-U.S. Data Privacy Shield main file, that guarantee a safe transfer of EU citizens' private data to the U.S. and that gives explanations on underlying laws and the data privacy principles that companies have to oblige to. The amendments section contains a warrant of the U.S. government to enforce the principles in a more stringent way than had been the case during the Safe Harbor Agreement.[130] Furthermore, the documents state how data transferred under the EU-U.S. Privacy Shield will have the same data privacy standards as the European Union. Section three of the amendments contains information on an ombudsman of the U.S. State Department, where data subjects can address concerns and complaints in regards of data transfers under the Privacy Shield Agreement.[131] Moreover, it highlights the access right of U.S. intelligence services and law enforcement authorities to access the private data of EU citizens. There is also a warrant of the U.S. government included to limit this access to the private data of EU citizens and bind the access to stricter conditions.[132] Also monitoring- and control mechanisms are highlighted which should ensure the enforcement of compliance of all parties according to the agreement.[133]

---

[128] Comp. Verlag Otto Schmidt: Das Legislativpaket der EU-Kommission für's "EU - U.S. Privacy Shield", (2016). Internet.
[129] Comp. Verlag Otto Schmidt: Das Legislativpaket der EU-Kommission für's "EU - U.S. Privacy Shield", (2016). Internet.
[130] Comp. Verlag Otto Schmidt: Das Legislativpaket der EU-Kommission für's "EU - U.S. Privacy Shield", (2016). Internet.
[131] Comp. Filip, Alexander: Stellungnahme der Art. 29-Datenschutzgruppe zum EU-US-Privacy Shield veröffentlicht, (2016), p.05108.
[132] Comp. Verlag Otto Schmidt: Das Legislativpaket der EU-Kommission für's "EU - U.S. Privacy Shield", (2016). Internet.
[133] Comp. Filip, Alexander: Stellungnahme der Art. 29-Datenschutzgruppe zum EU-US-Privacy Shield veröffentlicht, (2016), p.05108.

In the following section the assurances granted by the EU-U.S. Privacy Shield are laid out in detail:[134]

- **Stringent controls, restrictions and sanctions** towards companies. This also concerns the stricter restrictions for the data processors regarding onward transfers of data to third party partners.[135]
- **Assurance and transparency for data access through U.S. authorities**. A main difference compared to the Safe Harbor Agreement is the warrant of the U.S. government regarding the enforcement and the limitation of the authority's access to private data. There will be clear safeguards and oversight mechanisms.[136] Especially this point was an allegation of the European Court in the Schrems sentence. For one of the first times, the U.S. authorities assured in written form, through the office of the director of the National Intelligence Service, that there will be clear restrictions for data surveillance by U.S. authorities as well as no indiscriminate or general mass surveillance.[137] Furthermore, the U.S. government implemented an independent office of ombudsmen within the office of foreign affairs. This office should be the central point of contact for EU citizens in regards of clarification of compliance to laws and complaints. All warranties will be published in the U.S. federal register.[138]
- Effective **assurance for the data subjects** will be assured. For this purpose, companies need to investigate complaints within 45 days. A procedure for alternative dispute resolution will be initiated to resolve disputes together with the EU and U.S. authorities in case of complaints by EU citizens; this will be free of charge for the concerned parties.[139] If this will not solve the issue, an arbitration court - the Privacy Shield Panel[140] - will need to pass judgment. Companies process HR data need to commit to the data privacy principles of the European Union's data privacy

[134] Comp. Verlag Otto Schmidt: Das Legislativpaket der EU-Kommission für's "EU - U.S. Privacy Shield", (2016). Internet
[135] Comp. Verlag Otto Schmidt: Das Legislativpaket der EU-Kommission für's "EU - U.S. Privacy Shield", (2016). Internet
[136] Comp. European Commission: EU-U.S. Privacy Shield, (2016), Paragraph: U.S. Government Access. Internet.
[137] Comp. European Commission: EU-U.S. Privacy Shield, (2016), Paragraph: U.S. Government Access. Internet.
[138] Comp. Verlag Otto Schmidt: Das Legislativpaket der EU-Kommission für's "EU - U.S. Privacy Shield", (2016). Internet; Comp. European Commission: EU-U.S. Privacy Shield, (2016).Internet.
[139] Comp. European Commission: EU-U.S. Privacy Shield, (2016), Paragraph: Redress. Internet.
[140] Comp. European Commission: EU-U.S. Privacy Shield, (2016), Paragraph: Redress. Internet.

recommendations, where companies which do not process HR data can commit to these principles.[141]

- **Cooperative annual review** of the Data Privacy Shield itself, the functioning and the warranties will be an integral component of the annual procedures within the agreement. The EU Commission and the U.S. Trade Commission will conduct this review in cooperative manner. Hereby, representatives of the U.S. Intelligence Service and the European Data Privacy Commissions will assist as subject matter experts in special questions. To review the transparency, the EU Commission will additionally request transparency reports of the companies on the frequency and extent of personal data inquiry by U.S. authorities. This had been forbidden before as companies were not allowed to reveal the authority's requests.[142] The EU commission will hold a data privacy summit to debate about the actual developments in regards of the U.S. data privacy laws and their impact to the European Union and the data subjects respectively. An annual report will be published to the European Council as well as the European Parliament containing a resume of the annual review.[143]

In regards of the communique of the European Commission it was noticeable that nothing changed during the certification process. Companies still have the possibility to self-certify.[144] [145] The main difference, however, will be the control mechanisms and enforcement of compliance. Also in the field of complaint response, the Privacy Shield Agreement should bring some improvement as a 45 days and prompt response obligation will be introduced. Also the possibility of cheap redress of complaints and help of the data authorities in these cases is a main change in comparison to the Safe Harbor Agreement.[146]

[141] Comp. Verlag Otto Schmidt: Das Legislativpaket der EU-Kommission für's "EU - U.S. Privacy Shield", (2016). Internet
[142] Comp. European Commission: EU-U.S. Privacy Shield, (2016), Paragraph: U.S. Government Access. Internet.
[143] Comp. Verlag Otto Schmidt, 2016. Internet. and European Commission, 2016.Internet.
[144] Comp. European Commission: EU-U.S. Privacy Shield, (2016). Internet.
[145] Comp. Filip, Alexander: Stellungnahme der Art. 29-Datenschutzgruppe zum EU-US-Privacy Shield veröffentlicht, (2016), p.05108.
[146] Comp. European Commission: EU-U.S. Privacy Shield, (2016). Internet.

A review through the Article 29 Working Party had been conducted and resulted in the statement about the EU-U.S. Data Privacy Shield on the 13th April 2016 in working paper 238.[147]

For the analysis, the Article 29 Working Party group compared the sentences in the Schrems' case with its reference to the Article 25 Paragraph 6 of the directive 95/46/EG, stating the adequacy of the data privacy level, against the principles of the Privacy Shield.[148] Hereby, the working party had a detailed focus on Article 7 and 8 of the Fundamental Rights Charter that states the basic rights to safeguard personal life and personal private data as well as the Article 47 that grants legal protection. Additionally, the basic rights that were taken into consideration by the court to conclude that the Safe Harbor Agreement was invalid, have been contrasted with the Privacy Shield proposal. Completing Article 8 of the Convention for the Protection of Human Rights and Fundamental Freedoms, having a focus on private and family life, had been taken in consideration as well.[149]

The working party stated in its conclusion that the actual version of the Privacy Shield Agreement does not assure a comparable data privacy level such as within the European Union; it would need to be amended and reworked. The main questions that were raised by the working party are if the ombudsperson has enough empowerment and independence from the authorities as this innovation is one of the main advances on the journey of safe transatlantic data transfer for the data subject.[150] Furthermore, it was questioned if the ombudsperson offers enough protection in regards of data access by intelligence services.[151] Strong concerns were raised according to the commercial aspects of the Privacy Shield.[152] Especially the missing maximum retention duration for gathered data, transferred by the Privacy Shield certified companies, is a main point of critics.[153] Furthermore, the earmarking of

[147] Comp. Filip, Alexander: Stellungnahme der Art. 29-Datenschutzgruppe zum EU-US-Privacy Shield veröffentlicht, (2016), p.05108.
[148] Comp. Filip, Alexander: Stellungnahme der Art. 29-Datenschutzgruppe zum EU-US-Privacy Shield veröffentlicht, (2016), p.05108.
[149] Comp. Filip, Alexander: Stellungnahme der Art. 29-Datenschutzgruppe zum EU-US-Privacy Shield veröffentlicht, (2016), p.05108.
[150] Comp. Kuntz, Wolfgang: BfDI: Art. 29-Datenschutzgruppe fordert beim EU-US-Privacy-Shield nachzubessern, (2016), p.05106.
[151] Comp. Filip, Alexander: Stellungnahme der Art. 29-Datenschutzgruppe zum EU-US-Privacy Shield veröffentlicht, (2016), p.05108.
[152] Comp. Filip, Alexander: Stellungnahme der Art. 29-Datenschutzgruppe zum EU-US-Privacy Shield veröffentlicht, (2016), p.05108.
[153] Comp. Kuntz, Wolfgang: BfDI: Art. 29-Datenschutzgruppe fordert beim EU-US-Privacy-Shield nachzubessern, (2016), p.05106.

data is mostly not regulated within the Privacy Shield framework as well as the phrasing of certain aspects for commercial data use could introduce further abuse of data.[154]

The European Court did not give a final statement on the unrestricted data access of U.S. intelligence services. However, the Article 29 Working Party stated that, as concluded in earlier working papers (215 and 228), through unlimited and unrestricted access an adequate and EU equal data privacy level is not given. The working party sees the mass surveillance as a general violation of the data proportionality principle. Opinions of the court can be expected in late 2016, also related to the exchange with Canada on flight passenger data.[155]

The Article 29 Working Party comes to the general conclusion that the Privacy Shield Agreement is a clear improvement to the Safe Harbor Agreement.[156] However, the previously mentioned points of criticism highlight that the EU commission needs further negotiations with the U.S. government to incorporate further clarification for open points and ensure to protect the data subject's rights.

An article in the journal "MultiMedia und Recht" reflects the comments of the "Verbraucherzentrale Bundesverband e.V. (vzbv)" - the German consumer advice center in regards of the data subject perspective. According to the vzbv, the Privacy Shield Agreement is not complying to the European Data Privacy requirements.[157] They state the minimum requirements from a consumer standpoint as follows: [158]

- The Privacy Shield needs to reflect the same level of data privacy as the European law. This applies to data gathering and processing, the earmarking of data, the data reduction and data economy in general.
- Monitoring and control mechanisms need to be in place to ensure detection of offences. Furthermore, companies need to prove their compliance to the principles before they are put on the list of certified Privacy Shield companies.

[154] Comp. Filip, Alexander: Stellungnahme der Art. 29-Datenschutzgruppe zum EU-US-Privacy Shield veröffentlicht, (2016), p.05108.
[155] Comp. Filip, Alexander: Stellungnahme der Art. 29-Datenschutzgruppe zum EU-US-Privacy Shield veröffentlicht, (2016), p.05108.
[156] Comp. Filip, Alexander: Stellungnahme der Art. 29-Datenschutzgruppe zum EU-US-Privacy Shield veröffentlicht, (2016), p.05108.
[157] Comp. Verbraucherzentrale Bundesverband e.V. (vzbv): EU muss Privacy Shield-Abkommen nachbessern, (2016), p.377574.
[158] Comp. Verbraucherzentrale Bundesverband e.V. (vzbv): EU muss Privacy Shield-Abkommen nachbessern, (2016), p.377574.

- Measures need to be in place to ensure that data subjects can make claim on their legal due in the U.S. and Europe. Therefore, they need to have the possibility to seek legal redress in front of European courts.

The final conclusion of the vzbv is that, especially because of the continuing mass surveillance of the U.S. authorities, the new framework agreement will not last in front of the European Court. Especially since certain parties already announced that they are taking legal action in case the Privacy Shield Agreement will be introduced as it is right now.[159]

[159] Comp. Verbraucherzentrale Bundesverband e.V. (vzbv): EU muss Privacy Shield-Abkommen nachbessern, (2016), p.377574.

5.2.3. Binding Corporate Rules

Firms can transfer personal data within the company for dedicated purposes such as transfers of HR data of EU citizens to their headquarters outside of the EU. The concept that these transmissions rely on are Binding Corporate Rules; these rules can be seen such as the code of conduct for the companies using the rules. These would be internal rules that the companies need to comply to and that will assure an adequate level of data protection. The Intercompany agreement applies to the company itself so it can only be used within the company. They cannot be used for third parties as they "do not provide a basis for transfers made outside the group" [160]. The Binding Corporate Rules are made for multinational companies which have subsidiaries within countries that do not assure an adequate data protection level to safely transfer their data within the firm.[161] Nearly half of the EU firms, have branches that rely on the Safe Harbor Agreement to process internal HR data and need to submit these from Europe to their U.S. subsidiaries or headquarters for business purpose.[162] This example shows that there is a strong need for an adequate alternative for intercompany data transfers after the abolition of the Safe Harbor Framework.

The Binding Corporate Rules should "adduce adequate safeguards for the protection of the privacy and fundamental rights and freedoms of individuals". This was derived from the article 26(2) of the directive 95/24/EC and will have its basis within that regulation after the introduction of the General Data Protection Regulation (GDPR).

For the Binding Corporate Rules to be effective they need to contain certain key items. The first section should cover the topics of privacy principles such as transparency, data quality and security. The second part should contain the so-called tools of effectiveness. This controls and safeguards' sections that handles the whole governance, auditing, training and complaint handling within the firm. The final section should have a proof, such as incorporation in working contracts, that the Binding Corporate Rules are mandatory and all members of the firm have to comply to them.[163]

---

[160] European Commission: Overview on Binding Corporate rules, (2016), What is the purpose of BCR?. Internet.
[161] Comp. European Commission: Overview on Binding Corporate rules, (2016), What is it?. Internet.
[162] Comp. European Commission: Communication from the Commission to the European Parliament and the Council on the functioning of the Safe Harbour from the perspective of EU Citizens and Companies Established in the EU, (2013), p.5.
[163] Comp. European Commission: Overview on Binding Corporate rules, (2016), What are BCR in practice?. Internet.

After formulation the Binding Corporate Rules, approval is needed in order for it to be effective. This approval has to be gathered individually per company group at the national data protection authorities.[164] Compared to the standard contractual clauses, mentioned in the chapter "EU model contract clauses" below, the Binding Corporate Rules do not need to be signed by each legal entity of the company group that wants to conduct data transfer.[165]

For the procedure of approval, the national data protection authorities will review the Binding Corporate Rules provided by companies and check them against the principles and criteria set out by the Article 29 Working Party.[166] As a first step, the companies want to obtain compliant Binding Corporate Rules that need to designate a lead authority to avoid multiple reviews by different authorities. To define the lead authority certain criteria, apply in regards of the country of the data protection authority. The country could be defined e.g. by the location of the Europeans headquarters or by the group member with delegated data protection responsibilities. Also, the location should be best placed in regards of handling of the application and the enforcement of the rules stated in the Binding Corporate Rules or the legal entity with the most transfers outside the EU.[167] However, the company needs to request a formal approval at the chosen data protection authority which should function as the lead authority. Hereby, certain documents need to be handed in and comply the above mentioned key criteria.[168] This authority then will circulate the documents provided to all other concerned data protection authorities. The authorities then have 15 days to respond to the request and approve or decline it.[169] Finally, when the Binding Corporate Rules are approved, the company needs to ask for data transfer authorization on the basis of the approved Binding Corporate Rules at each national data protection authority.[170]

The main advantage of the Binding Corporate Rules is the legal obligatory compliance to the European Directive 95/46/EC for all flows within the company's group which therefore mitigates the risk of data transfers to third countries. Once the Binding Corporate Rules are approved they assure a sufficient level of protection to companies.[171]

---

[164] Comp. European Commission: Overview on Binding Corporate rules, (2016), What is the purpose of BCR?. Internet.
[165] Comp. European Commission: Overview on Binding Corporate rules, (2016), What is the purpose of BCR?. Internet.
[166] Comp. European Commission: Procedure, (2016). Internet.
[167] Comp. European Commission: Designation authority, (2016). Internet.
[168] Comp. European Commission: Designation authority, (2016). Internet
[169] Comp. European Commission: Designation authority, (2016). Internet.
[170] Comp. European Commission: Procedure, (2016). Internet.
[171] Comp. European Commission: Overview on Binding Corporate rules, (2016). Internet.

Furthermore, harmonized practices in regards of the protection of personal data within the company group are assured, where e.g. single contracts with the subsidiaries could differ and easily confuse and not be maintainable – with Binding Corporate Rules the need for single contracts is obsolete. Also, within the firms, the Binding Corporate Rules have the advantage of giving employees a guideline on personal data treatment and management.[172]

The European Union publishes the companies that have approved Binding Corporate Rules on their website. This helps an individual data subject see which companies have such agreements, reliable safeguards and controls in place, but also whom to contact in regards of claims in case of data mistreatment.

More information on the implementation can be found in the following literature:

"Binding Corporate Rules (BCR) – Als Mittel zur Datenschutz Compliance – Leitfaden für die Praxis", Rechtsanwaltskanzlei Dr. Thomas Helbing, Juni 2015

"Binding Corporate Rules", Allen & Overy international legal practice, February 2013

[172] European Commission: Overview on Binding Corporate rules, (2016), What are the advantages of BCR?. Internet.

5.2.4. EU Model Contract Clauses

The actual and more practical way for companies to prevent unlawful data transfers to the U.S. are the model contract clauses that are incorporated in the company's contracts with vendor or partner.

The inter-organizational agreements, or so-called data transfer agreements, use these model contract clauses provided by the European Commission[173] that enable the companies to transfer personal data between each other under legal compliance. The model contract clauses give a baseline for amendments to contracts, when third parties that are residing in countries with a different data protection standard than the EU, are involved. The model contract clauses have a standard wording about how the data processor in countries with lower data privacy standards, e.g. the U.S., have to ensure "adequate" data privacy and protection level.

The main advantage for companies using model contract clauses is that they do not need to conduct their own assessment of the adequacy of the protection level. This advantage only applies, if they use the exact wording as the contract clauses in their contracts.[174] The model contract clauses allow for data transfers between the two parties without a need for further approval by EU authorities. The main difference, however, is that the above mentioned Binding Corporate Rules need individual approval by the Data Privacy Commission, while the model contract clauses would be applicable even without such approval.[175] These pre-approved model clauses give an overall adequate and secure framework with safeguards to rely on from a legal and regulatory perspective. The agreement is made on a company level and covers all data transfers performed by the two parties. However, the assurance and control of the data protection itself need to be controlled by the controller and processors based on the type of model contract clause used, which will be highlighted on the next page.

[173] Comp. Gibbs, Samuel: What is 'safe harbour' and why did the EUCJ just declare it invalid?, (2015), Internet.
[174] Information Commissioner´s Office: Model Contract Clauses, (2012). Internet.
[175] Comp. Borges, Georg: Datentransfer in die USA nach Safe Harbor, (2015), p.3617 – Paragraph II.

There are four different types of model contract clauses depending on the data transfer relationship between the different parties. These can be used for different data processor and controller scenarios and their different data flows.[176] The European commission therefore approved four sets of data transfer agreements: [177]

- *Set 1 controller to controller* (2001 controller to controller)
  Based on the Commission decision 2001 / 497 / EC (15. June 2001)
  This set of clauses authorizes to transfer data from data controllers within the EEA to those outside the EEA.
- *Set 1 controller to processor*
  Based on the Commission decision 2002 / 16 / EC (27. December 2001)
  This set authorizes transfers from data controller in the EEA to data processors outside the EEA. This agreement had been used and is effective for all contracts before the 15th May 2010 but not available for new users.
- *Set 2 controller to controller* (2004 controller to controller)
  Based on the Commission decision 2004 / 915 / EC (27. December 2004)
  This is an alternative set of model clauses for transfers from data controllers within the EEA to those outside the EEA.
- *Set 2 controller to processor* (2010 controller to processor)
  Based on the Commission decision 2010 / 87 / EU (5. February 2010)
  This set is the replacement for the Set 1 controller to processor and authorizes transfers from data controller in the EEA to data processors outside the EEA.

The controller to controller clauses (Type 1 and 2) fit the purpose of transferring data from one company to another, where the receiving company in this scenario uses the data for its own purpose. The choice of which clauses are used resides at the companies. The difference between the clauses is mainly driven by the liability and ownership of the data that is being transferred. Both clauses obligate both parties to ensure that safeguards and controls are in place for the data transfer. This should protect the data subject's freedom, rights and level of protection regarding his data.[178]

[176] Comp. European Commission: Model Contracts for the transfer of personal data to third countries, (2015). Internet.
[177] Comp. European Commission: Model Contracts for the transfer of personal data to third countries, (2015). Internet.; Information Commissioner´s Office: Model Contract Clauses, (2012). Internet.
[178] Comp. Information Commissioner´s Office: Model Contract Clauses, (2012), p.4. Internet.

While with Set 1 controller to controller clauses make all parties responsible and liable for the data of the subject individually, they also make them share the risk for any damage the subject may endure because of a data breach. Regarding the right of enforcement by the data subject, the set 1 clauses allow that either one of the parties involved will be approached in case of a breach. In case one party is not accessible by the data subject, the data subject is within its right to approach the data exporter instead of the importer to enforce his rights there instead. This is a possibility as the data exporter also failed to ensure the security of the data.

In the set 2 clauses, the data subject can only make the firm that caused the data breach liable for the damage.[179] This means that the data importer and exporter need to carefully think of which set they want to use, especially because they have a greater risk premium in either one or the other clause type.

The set 2 controller to processor clauses focusses on transferring data to a third party. This party processes the data for the data controller, rather than using it for its own purpose. These clauses follow the principle of root cause, meaning that the party causing a data breach will be held liable for the breach.[180] The contract clauses even include the case of sub-processing, where a subcontractor would engage in data processing after an onward transfer of the data from the processing party. If this is the case, the data controller needs to explicitly agree to the sub-processing.[181] Furthermore, the controller will in this last instance be responsible as he initially transferred the data for processing.[182]

All model contract clauses need to be applied in its original form and will lose liability in case of alteration. However, they can be incorporated into other contracts and amended with additional provisions of obligations, e.g. sections and agreements to dispute resolutions or extraordinary termination clauses.[183] In case of alteration of the clauses the transfer will still be possible, but in case of investigation, companies need to proof that they have the same data protection and privacy level for the data subject's data as the original model contract clauses ensured. This can cause extensive cost and efforts on the data controller's side.

The model contract clauses have one main disadvantage which is the number of contracts with different parties that are needed when putting them in place. With each transmitting or

[179] Comp. Information Commissioner´s Office: Model Contract Clauses, (2012), p.4f. Internet.
[180] Comp. Information Commissioner´s Office: Model Contract Clauses, (2012), p.5. Internet.
[181] Comp. Information Commissioner´s Office: Model Contract Clauses, (2012), p.5f. Internet.
[182] Comp. Henderson, Steve: Safe Harbor: How to use Model Contract Clauses for EU - US data export and processing, (2015). Internet.
[183] Comp. Information Commissioner´s Office: Model Contract Clauses, (2012), p.6. Internet.

receiving firm the counterparty would need to have one contract, including model contract clauses, in place. Other companies, according to the European Commission's statement are not able to count on these system of contracts as the effort would be extensive. "For example MasterCard deals with thousands of banks and the company is a clear example of a case where Safe Harbor cannot be replaced by other legal instruments for personal data transfers such as binding corporate Rules or contractual arrangements."[184] In these types of cases, the firm needs to rely on an overall framework.

For less data and counterparty intense companies, the model contract clauses provide a proper framework which can be applied without excessive efforts as the clauses can be used exactly as they are and be incorporated into contracts with other parties. However, the effort to put in place even the contracts with all counterparties slightly vary by the origination of the business and the amount of business partners. Transfers using contractual clauses cannot always effectively replace a framework agreement on governmental level and therefore cannot be seen as the ultimate solution for all data transfer cases.

[184] European Commission: Communication from the Commission to the European Parliament and the Council on the functioning of the Safe Harbour from the perspective of EU Citizens and Companies Established in the EU, (2013), p.4.

5.2.5. Exceptional statement of facts and single contracts

A more uncommon way of bypassing the data privacy law would be the possibility to have an exceptional statement of facts, which could mean that the transfer is eligible for an exception. The exceptional statement of facts is defined in the Directive 95/46/EC Article 26 I and the German federal data privacy law (BDSG) § 4 c I. The exceptional permission requires a case by case decision of the data privacy authorities.[185] Generally spoken, this possibility is not very often used and therefore uncommon as the agreement is on a transfer by transfer basis. This would mean that for each new system and data transfer an own agreement has to be drawn-up with the data subject and the exception needs to be proven for each of individual.

Comparable to the exceptional statement of facts are individual contracts with counterparties. In these cases, the extent of individual contracts would easily extend the capacity that business lines would be able to cover in designing, maintaining and disposing each contract. In addition, these contracts would need individual approval from the EU's data privacy authorities, thereby adding another level of complexity to these single contracts.

[185] Comp. Grau, Timon and Granetzny: EU-US-Privacy Shield - Wie sieht die Zukunft des transatlantischen Datenverkehrs aus?, (2016), p.408.

5.2.6. Technical solutions

When it comes to technical solutions, it needs to be analyzed what kind of technical solutions are in place in order to ensure a legal data transfer of personal data to the U.S. The alternatives covered in the chapters about other alternatives above approach the topic the data transfer from a legal and corporate governance standpoint, while the technical solution idea focuses more on the approach to alternate the substance of the data themselves. This either causes an inaccessibility by the authorities, or the data itself would change their classification to non-person related information because of the alteration. The different procedures that are covered address dissimilar approaches to ensure the data transfer and storage.

Within the GDPR the following technical solutions are proposed as good practice safeguards to ensure the protection of the data subjects information.[186]

[186] Comp. European Parliament: Regulation (EU) 2016/679 of the European Parliament and of the Council - Document 32016R0679, (2016), Article 6 Pargraph 4 e), Article 32 Paragraph 1 a).

5.2.6.1. Tokenization & Pseudonymisation

One way to address the data transfer possibility is to ensure the safeguard by altering the nature of the data itself. Meaning, if the data transfer within the scope of the data privacy law concerns only personal data that is assignable to individual data subjects within the EU, the alteration of the nature of the data is a possibility. By doing so, the data fragments that allocated specific data to any individual is removed from the context. This method can be achieved with the so called *Tokenization*; this splits the data and enables its fragments to be transferred. Only with the corresponding mapping tables can the data be put back together again accordingly. The mapping table resides in a safe place and could for example be used on the receiver side for a decrypting program to only decrypt and put back together the data on the fly. This would happen in the cache of the receiving infrastructure in the memory of the servers, where data would be deleted after the operation is finished. This would prevent the data to permanently reside there unencrypted and unsecured.

5.2.6.2. Encryption

Another way of ensuring that the data transfer is legal, is by using secure file and data encryption techniques. By doing so, the data is encrypted before the transfer using the public-private key encryption method – where private keys reside at the sender a receiver side and public keys are public available. This method signs the data with the private key and encrypts them with the public key of the receiver. The receiver can then verify with his public key if the data is really coming from the expected sender. On the other hand, the receiver and only him can decrypt the data with his private key as it was decrypted with his public key and only he holds his private key needed to decrypt the data. This method prevents, as long as the private keys are kept safe and secret, access by authorities or other third parties. The private keys reside in the European Union at the transmitting company, as this constitutes the general access to all data.

5.2.6.3. Data Center resides in the EU

Another possibility that companies started to use is to avoid the transfer of data to the U.S. Especially companies who offer services that do not necessarily require data transfers, such as cloud providers, started to set up data centers in the European Union. By doing so, the EU citizen's private data would be stored and processed inside the European Union. This would therefore prevent any access of U.S. authorities. Even though this does not directly address data transfers itself, it would be a possibility to avoid the transfer completely.

6. Conclusion

"Relying on the government to protect your privacy is like asking a peeping tom to install your window blinds." [187]

John Perry Barlow
(Declared on the World Economic Forum in Davos the Independence of Cyberspace)

Ranging from the abolition of the Safe Harbor Agreement to naming possible alternatives; this thesis covered different aspects, such as impacts and alternative solutions as well as an outlook on the ongoing initiatives of the European Union. Looking at citation of John Perry Barlow, it becomes clear that the controversial part about this entire topic is without a doubt the governmental data privacy and protection practices.

This thesis highlighted the clear negative impact that a missing privacy protection framework had on the industry and on reputation, such as in the U.S. Due to this negative impact, companies as well as the U.S. government lost their trustworthiness in regards of their data privacy, and protection treatments and principles. The abolition clearly forces the industry in U.S., which was able to self-certify themselves as proof of good data practice prior to the abolition, to put pressure on the government in order to force them to come to an agreement with the European Union about data privacy regulations and to come up with alternative solutions.

The unfinished Privacy Shield Agreement will be finalized in the near future and will then become effective for data transfers between the EU and the U.S. As this is a stricter replacement for the Safe Harbor Agreement, this solution is the most effective alternative and will again be a covering framework applicable for all data transfers to the U.S.

The actual status of the review, through the Article 29 Working Party, shows that certain concerns regarding the Privacy Shield Agreement, which should be seen as a replacement for the Safe Harbor Agreement, are still not solved, especially the opinions of the Article 29 Working Party with regards to alternative data transfer methods, other than the Privacy Shield safeguard, are outstanding. This results in an ongoing legal uncertainty for companies that want to transfer personal data to the U.S.[188]

[187] http://www.brainyquote.com/quotes/quotes/j/johnperryb129891.html
[188] Comp. Filip, Alexander: Stellungnahme der Art. 29-Datenschutzgruppe zum EU-US-Privacy Shield veröffentlicht, (2016), p.05108.

However, with the effectiveness of regulation (EU) 2016/679 and its enforcement by 2018, the European Commission and local data protection authorities need to come up with a framework solution to offer a practical and effective method for cross border data transfer. Especially the economic burdens for companies doing business with EU countries will force authorities from a financial standpoint to act timely. Nevertheless, experts have a critical opinion on the Privacy Shield Agreement as even though it is effective on paper, but U.S. authorities will most likely not stick to the rules even if they break foreign law. It can therefore be concluded that it will be unlikely that the Privacy Shield Agreement will protect the data subject's data and it will consequently not take long, according to experts, until the Privacy Shield Agreement, just like the Safe Harbor Agreement, lands in front of a court.

The Binding Corporate Rules such as company agreements within firms have been discussed in order to analyze their effectiveness as alternatives for intercompany data transfers. The EU will release new Binding Corporate Rules for data processors and these rules will be comparable to internal certification and will thereby make single contracts for data processing with each individual counterparty obsolete. A good example of this would be Microsoft with its Office 365 cloud service, which enables clients to store their data in the cloud. With the new data processor rules, Microsoft would be enabled to internally process and transfer the data within the corporation while complying to EU privacy laws and without a need for single contracts between all branches or subcontractors. However, the Binding Corporate Rules remain an alternative for transfers within a firm, which result in separate contracts for data transfers to external parties.

Therefore, model contract clauses function as an agreement to transfer personal data to third parties. As the model contract clauses in place today have already existed for some years, it can be expected that the EU will renew these and provide companies with new modal contract clauses having an alignment to recent regulations and standards. It seems to be a valid alternative to the Safe Harbor Agreement as the contract clauses do not need to be individually customized and can be put in place exactly as they are provided by the EU. This minimizes the effort and can help companies quickly resume to lawful data transfers.

The exceptional statement of facts, which functions as a solution for very few cases, has also been evaluated, but as a more theoretical alternative that is not used often within industry boundaries as a common standard to lawful data transfer.

After several regulations were analyzed, multiple practical solutions for the missing data protection framework were reviewed. These solutions handle the data transfer issue from a more technical standpoint and highlight the data privacy and protection by design topic. The technical systems are designed to ensure privacy already on a system level according to how they are programmed, setup and configured rather than looking at the corporate governance component how to use the software and by what personal it should be used. As a key requirement stated in the GDPR, encryption and privacy by design will be required characteristics of future system setups. It will become common practice that all data transfer and storage will be encrypted, tokenized and will undergo a pseudonymization by standard. Through cyber-attacks and high penalties, the awareness of the topic of technical privacy will be risen.

From a company standpoint the whole topic will enforce companies to rethink their data protection and data privacy strategy completely. An age of good personal data treatment practice for data subjects will commence. Therefore, companies need to put in place effective governance measures and safeguards to assure the control of data flows. It seems key to know your data flow as a company in order to effectively manage data transfers and to take measures and put safeguards in place whenever necessary. The authorities will come up with more and more obligations to gain control over cross border data flow which will eventually result in stricter data privacy laws and regulations.

When comparing the concluding citation to the introduction citation, the concluding citation is very different in its meaning and very well highlights how I personally developed my opinion in regards of this topic. The effort that the European Union puts into the topic of data protection to ensure an adequate level of protection for EU citizens' data is enormous. However, the concepts that the EU came up for now as an alternative to the Safe Harbor Agreement has one major weakness: no one can assure that U.S. authorities will really comply to the agreements that will be made, such as the Privacy Shield Agreement. Binding Corporate Rules will lose their effectiveness if U.S. secret services are easily able to access the data by using their governmental power. As was stated by John Perry Barlow: as long as governments are in control of your privacy they will use that opportunity, and this does not exclude EU governments, to gain backdoor access to your personal data.

I. Sources

ARTICLE 29 DATA PROTECTION WORKING PARTY. (2002, 07 02). *Working Document on Functioning of the Safe Harbor Agreement.* Retrieved 08 12, 2016, from European Commission Justice: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2002/wp62_en.pdf

Article 29 Data Protection Working Party. (2016, 02 02). *Justice - Building a European Area of Justice.* Retrieved 08 20, 2016, from Work programme 2016 – 2018: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2016/wp235_en.pdf

Ashford, W. (2016, 01 19). EU data protection rules will leave no organisation untouched, say legal experts. *Computerweekly*, pp. 4-7.

Borges, G. (2016). *Cloud Computing* (1. Auflage ed.). In Leinen: C.H.BECK.

Borges , G. (2015, - -). Datentransfer in die USA nach Safe Harbor. *Neue Juristische Wochenschrift (NJW)*(50), pp. 3617-3621.

BOT, A. (23, 09 2015). *Opinion of Advocate General Bot delivered on 23 September 2015.* Retrieved 08 15, 2016, from InfoCuria - Rechtsprechung des Gerichtshofs: http://curia.europa.eu/juris/document/document.jsf?docid=168421&doclang=EN

Düsseldofer Kreis. (2010). Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffnetlichen Bereich am 28./29. April 2010 in Hannover (überarbeitete Fassung vom 23.08.2010). In D. Kreis (Ed.). (p. 2). Hannover: Düsseldofer Kreis.

de Hert, P., & Papakonstantinou, V. (2016, 04 -). The new General Data Protection Regulation: Still a sound system for the protection of individuals? *Computer Law & Security Review*, pp. 179-194.

DeGraw, J. S., Barnes, M., Massey, R., McIntosh, D., Parghi, I., & Sussman, H. E. (2015, 10 12). *Worldwide: The U.S.-EU Safe Harbor Framework Is Invalid: Now What?* Retrieved 08 13, 2016, from Mondaq: http://www.mondaq.com/unitedstates/x/433814/Data+Protection+Privacy/The+USEU+Safe+Harbor+Framework+Is+Invalid+Now+What

Dhont, J., Asinari, M. V., & Poullet, Y. (2004, 04 19). *Justice - Building a European Area of Justice.* Retrieved 08 11, 2016, from Safe Harbour Decision Implementation Study: http://ec.europa.eu/justice/data-protection/document/studies/files/safe-harbour-2004_en.pdf

Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit. (2016, 02 29). *Safe Harbor*. Retrieved 08 15, 2016, from Safe Harbor – Datenschutz-Wiki: https://www.bfdi.bund.de/bfdi_wiki/index.php/Safe_Harbor

Die Bundesbeauftragte für den Datenschutz und die Infromationsfreiheit. (2015, 10 06). *Safe Harbor*. Retrieved 08 14, 2016, from Safe Harbor: https://www.bfdi.bund.de/DE/Europa_International/International/Artikel/SafeHarbor.html

Dropbox Inc. (2016). *Info - Dropbox.* Retrieved 10 22, 2016, from Dropbox: https://www.dropbox.com/about

European Commission. (2000, 08 25). *Official Journal of the European Communities.* Retrieved 08 16, 2016, from COMMISSION DECISION of 26 July 2000: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32000D0520&from=de

European Commission. (2013, 11). *Communication from the Commission to the European Parliament and the Council on the functioning of the Safe Harbour from the perspective of EU Citizens and Companies Established in the EU.* European Commission. Brussels: European Commission.

European Commission. (2015, 10 06). *Article 29 Working Party*. Retrieved 08 13, 2016, from http://ec.europa.eu/justice/data-protection/article-29/index_en.htm

European Commission. (2015, 12 02). *Model Contracts for the transfer of personal data to third countries*. Retrieved 08 15, 2016, from European Commission: http://ec.europa.eu/justice/data-protection/international-transfers/transfer/index_en.htm

European Commission. (2015, 09 08). *Questions and Answers on the EU-US data protection "Umbrella agreement".* Retrieved 08 14, 2016, from European Comission - Press release database: http://europa.eu/rapid/press-release_MEMO-15-5612_en.htm

European Commission. (2015, 09 08). *Statement by EU Commissioner Věra Jourová on the finalisation of the EU-US negotiations on the data protection "Umbrella Agreement".* Retrieved 08 15, 2016, from European Commission Press release database: http://europa.eu/rapid/press-release_STATEMENT-15-5610_en.htm

European Commission. (2016, 07 12). *Article 29 Working Party - Binding Corporate rules* . Retrieved 08 20, 2016, from http://ec.europa.eu/justice/data-protection/article-29/bcr/index_en.htm

European Commission. (2016, 07 12). *Overview on Binding Corporate rules*. Retrieved 08 20, 2016, from http://ec.europa.eu/justice/data-protection/international-transfers/binding-corporate-rules/index_en.htm

European Commission. (2016, 01 15). *About the European Commission*. Retrieved 08 17, 2016, from About the European Commission: http://ec.europa.eu/about/index_en.htm

European Commission. (2016, 07 12). *European Commission - Binding Corporate Rules - Procedure*. Retrieved 08 20, 2016, from http://ec.europa.eu/justice/data-protection/international-transfers/binding-corporate-rules/procedure/index_en.htm

European Commission. (2016, 07 12). *European Commission - Designation authority*. Retrieved 08 20, 2016, from http://ec.europa.eu/justice/data-protection/international-transfers/binding-corporate-rules/designation_authority/index_en.htm

European Commission. (2016, 02 -). *Justice - Protection of personal data.* Retrieved 08 15, 2016, from EU-U.S. Privacy Shield: http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_eu-us_privacy_shield_en.pdf

European Commission. (2016, 09 29). *Reform of EU data protection rules*. Retrieved 10 09, 2016, from Justice Building a European Area of Justice: http://ec.europa.eu/justice/data-protection/reform/index_en.htm

European Commission Justice. (2012, 10 09). *Opinions and recommendations - How will the "safe harbor" arrangement for personal data transfers to the US work?* Retrieved 08 10, 2016, from http://ec.europa.eu/justice/policies/privacy/thridcountries/adequacy-faq1_en.htm

European Council. (2015, 01 28). *The Council of the European Union*. Retrieved 08 13, 2016, from http://www.consilium.europa.eu/en/council-eu/

European Court. (2015, 10 06). *Rechtsprechung des Gerichtshofs - ECLI:EU:C:2015:650.* Retrieved 08 12, 2016, from InfoCuria: http://curia.europa.eu/juris/document/document.jsf?text=&docid=169195&pageIndex=0&doclang=DE&mode=lst&dir=&occ=first&part=1&cid=135951

European Court. (2015, 10 22). Ungültigkeit der Safe-Harbor-Entscheidung der EU betreffend die USA. *Neue Juristische Wochenschrift*, p. 3151.

European Data Protection Supervisor. (2016, 02 12). *EDPS welcomes EU-US "Umbrella Agreement" and stresses need for effective safeguards.* Retrieved 08 14, 2016, from EDPS PRESS RELEASE DATABASE: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/PressNews/Press/2016/EDPS-2016-06-Umbrella_Agreement_EN.pdf

European Parliament. (1995, 11 23). *Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr.* Retrieved 08 10, 2016, from EUR-Lex - 31995L0046 - DE: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:DE:HTML

European Parliament. (2016, 04 27). *Regulation (EU) 2016/679 of the European Parliament and of the Council - Document 32016R0679* . Retrieved 10 09, 2016, from EUR-Lex Access to European Union law: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679

European Union. (2016, 02 18). *European Parliament*. Retrieved 08 13, 2016, from http://europa.eu/about-eu/institutions-bodies/european-parliament/index_en.htm

EYGM Limited. (2016, - -). When is privacy not something to keep quiet about? New EU General Data Protection Regulation. (E. Limited, Ed.) UK.

Filip, A. (2016, 04 27). Stellungnahme der Art. 29-Datenschutzgruppe zum EU-US-Privacy Shield veröffentlicht. *ZD-Aktuell*, p. 05108.

Gibbs, S. (2015, 10 06). *What is 'safe harbour' and why did the EUCJ just declare it invalid?* Retrieved 08 12, 2016, from The Guardian: https://www.theguardian.com/technology/2015/oct/06/safe-harbour-european-court-declare-invalid-data-protection

Grau, T., & Granetzny, T. (2016, 04 11). EU-US-Privacy Shield - Wie sieht die Zukunft des transatlantischen Datenverkehrs aus? *Neue Zeitschrift für Arbeitsrecht*, pp. 405-410.

Härting, N. (2015, 10 15). EuGH v. 6.10.2015 - Rs. C-362/14, EuGH: „Safe Harbor“-Entscheidung ungültig. *Computer und Recht*, pp. 633-641.

Henderson, S. (2015, 10 15). *Safe Harbor: How to use Model Contract Clauses for EU - US data export and processing*. Retrieved 08 23, 2016, from DMA: http://dma.org.uk/article/safe-harbor-how-to-use-model-contract-clauses-for-eu-us-data-export-and-processing

Hert, P. (2016, 04 01). The new General Data Protection Reulation: Still a sound system for the protection of individuals? *Computer Law & Secuirty Review*, pp. 179-194.

Information Commissioner´s Office. (2012, 02 28). *Information Commissioner´s Office.* Retrieved 08 23, 2016, from Model Contract Clauses: https://ico.org.uk/media/1571/model_contract_clauses_international_transfers_of_personal_data.pdf

Kuntz, W. (2016, 04 27). BfDI: Art. 29-Datenschutzgruppe fordert beim EU-US-Privacy-Shield nachzubessern. *ZD-Aktuell*, p. 05106.

Landesamt für Datenschutzaufsicht (BayLDA). (2015, 10 21). *Landesamt für Datenschutzaufsicht (BayLDA).* Retrieved 09 24, 2016, from Landesamt für Datenschutzaufsicht (BayLDA): https://www.lda.bayern.de/media/dsk_positionspapier_safeharbor.pdf

Long, W. (2015, 07 21-27). EU General Data Protection Regulation comes into sharper focus. *Computer Weekly*, pp. 18-19.

Long, W. R., & Blythe, F. (2015, 09 21). *EU-US Data Protection “Umbrella Agreement” Finalised*. Retrieved 08 14, 2016, from Sidley Austin LLP. - Data Matters: http://datamatters.sidley.com/eu-us-data-protection-umbrella-agreement-finalised/

Marx, L., & Wüsthof, L. (2015, 12 11). CJEU shuts down Safe Harbor for Transatlantic Data Transfer – Case C-362/14 Maximilian Schrems v Data Protection Commissioner. *Journal of European Consumer and Market Law*.

McQuillen, M., Barrett, P., & Myers, T. (2015, 10 13). *Safe Harbor ruled INVALID- News - Eversheds International*. Retrieved 08 10, 2016, from Eversheds: http://www.eversheds.com/global/en/what/publications/shownews.page?News=en/switzerland/en/10_2015_Safe_harbor

Nwankwo, I. S. (2016, 03 24). The Proposed Data Protection Regulation and its Limitations in Disaster Situations. *ZD-Aktuell*, p. 05061.

Reuters. (2015, 10 06). *Aktien von Facebook und Google nach EuGH-Urteil im Minus*. Retrieved 08 13, 2016, from Börse Online: http://www.boerse-online.de/nachrichten/aktien/Aktien-von-Facebook-und-Google-nach-EuGH-Urteil-im-Minus-1000844895

Revolidis, I., & Dahi, A. (2015, - -). Further Processing of Personal Data - Is there a Future for the Purpose Limitation Principle in the Upcoming General Data Protection Regulation? *ZD-Aktuell*, p. 04618.

Sidley Austin LLP. (2016, 02 26). *President Obama Signs Judicial Redress Act*. Retrieved 08 15, 2016, from Lexology - Data Matters: http://www.lexology.com/library/detail.aspx?g=bd560266-05ac-434a-a1ce-95ada7de0b7f

Spies, A. (2013, 12 05). EU-Kommission äußert sich zu EU/US-Safe Harbor – 13 Empfehlungen. *ZD Aktuell*(21), p. 3837.

Spies, A. (2016, 02 24). USA: Judicial Redress Act verabschiedet. *ZD-Aktuell*, p. 05005.

Stupp, C. (2016, 02 17). *Commission's 'Umbrella Agreement' with US under fire from MEPs*. Retrieved 08 13, 2016, from EurActive: http://www.euractiv.com/section/digital/news/commissions-umbrella-agreement-with-us-under-fire-from-civil-liberties-meps/

Taylor Wessing LLP. (2015, 11 17). *Safe Harbor is invalid. Now what?* Retrieved 09 24, 2016, from TaylorWessing: https://united-kingdom.taylorwessing.com/en/safe-harbor-is-invalid-now-what

U.S. DEPARTMENT OF COMMERCE. (2009, 01 30). *SAFE HARBOR PRIVACY PRINCIPLES*. Retrieved 08 12, 2016, from https://build.export.gov/main/safeharbor/eu/eg_main_018475

US Government. (2009, 01 30). *SAFE HARBOR PRIVACY PRINCIPLES*. Retrieved 08 10, 2016, from https://build.export.gov/main/safeharbor/eu/eg_main_018475

US Government. (2015, 08 05). *Export.gov Helps American Companies Succeed Globally*. Retrieved 08 10, 2016, from https://build.export.gov/main/about/index.asp

Verbraucherzentrale Bundesverband e.V. (vzbv). (2016, 04 27). vzbv: EU muss Privacy Shield-Abkommen nachbessern. *MMR-Aktuell*, p. 377574.

Verlag Otto Schmidt. (2016, 02 29). *Das Legislativpaket der EU-Kommission für's "EU - U.S. Privacy Shield"*. Retrieved 08 14, 2016, from CR Online Portal zum IT-Recht: http://www.cr-online.de/43754.htm

Warren, S. D., & Brandeis, L. D. (2011, 12 19). *Unabhängiges Landeszentrum für Datenschutz - Schleswig-Holstein*. Retrieved 08 11, 2016, from Das Recht auf Privatheit The Right to Privacy: https://www.datenschutzzentrum.de/allgemein/20111219-Warren-Brandeis-Recht-auf-Privatheit.html

EIKV-Schriftenreihe zum Wissens- und Wertemanagement

Bereits erschienen

2015	Francesca Schmitt	Intellectual Property and Investment Funds	Band 1
2016	Sebastian Fontaine	The electricity market reinvention by regional renewal	Band 2
2016	Tim Karius	Intellectual Property and Intangible Assets - Alternative valuation and financing approaches for the knowledge economy in Luxembourg	Band 3
2016	Irena Hank	Emotionale Intelligenz und optimales Teaming – eine empirische Untersuchung	Band 4
2016	Pascal Berg	European Market Infrastructure Regulation (EMIR)	Band 5
2016	Dr. Sverre Klemp	Die Angemessenheit der Vergütung nach § 32 UrhG für wissenschaftliche Werke im STM-Bereich	Band 6
2016	Lars Heyne	Immaterialgüterrechte und Objektreplikation: Juristische Risiken und Lösungsmöglichkeiten bei der Vermarktung von 3D-Druckvorlagen	Band 7
2016	Torsten Hotop	Äquivalenzinteresse im Erfinderrecht	Band 8
2016	Christian Wolf	Zur Eintragungsfähigkeit von Geruchs- und Hörmarken	Band 9
2016	Nadine Jneidi	Risikofaktor Pflichtteil - Grundlagen und Grenzen der Regelungs- und Gestaltungsmöglichkeiten von Pflichtteilsansprüchen bei der Nachfolge in Personengesellschaften	Band 10
2016	Meika Schuster	Ursachen und Folgen von Ausbildungsabbrüchen	Band 11
2016	Julie Wing Yan Chow	Activity Based Costing - A case study of Raiffeisen Bank of Luxembourg	Band 12
2016	Peter Koster	Luxembourg as an aspiring platform for the aircraft engine industry	Band 13
2016	Stefanie Roth	The Middle Management – new awareness needed in the current information society?	Band 14
2016	Alexander Fey	Warum Immaterielle Wirtschaftsgüter und Intellectual Property die Quantenteilchen der Ökonomie sind	Band 15
2016	Daniel Nepgen	Machbarkeitsstudie eines Audioportals für Qualitätsjournalismus. Eine empirische Untersuchung in Luxemburg	Band 16
2016	Niklas Jung	Abolition of the Safe Harbor Agreement – Legal situation and alternatives	Band 17