RIGA GRADUATE SCHOOL OF LAW

Challenges of Free Data Flow Between the EU and US: Can EU-US Privacy Shield Ensure Co-operation?

BACHELOR THESIS

AUTHOR: ***Artjoms Jurkevics***
LL.B. 2020/2021-year student
Student nr. B014013

SUPERVISOR: Ēriks Selga

DECLARATION OF HONOUR:
I declare that this thesis is my own work, and that all references to, or quotations from, the work of others are fully and correctly cited.

(Signed) .....

RIGA, 2020

TABLE OF CONTENTS

SUMMARY

The following thesis aims to provide an insight into the way US and EU data protection regulations compare to each other and how those can harmonized in the future with an idea to make it easier to understand how cross-country business might operate in this environment and whether there could be any harmonization opportunities to provide less burden on businesses in trying to comply with different laws across Atlantics. The research question of the thesis therefore is "Is current framework for data transfers between EU-US relevant and stable for future challenges in data protection field?" and "If not, then how two legal systems can be better harmonized based on the analysis of both of them?"

The first chapter of the thesis is focusing on analysis of the main points of the GDPR (General Data Protection Regulation) that might be comparable to the ones in the US and would lay down legal background as well as main principles of the document for the further comparative analysis. It will list and explain the main principles of the document such as lawfulness, fairness, transparency, accountability, storage limitation, purpose limitation, data minimization, etc. and would provide some in depth explanation for the most important changes compared to the previous data protection Directive (Directive 95/46/EC).

The second chapter of the thesis involves description and analysis of US data protection laws and how all of their regulations tie together to create an overall system of data protection within the country. It explains how the US system is different from the European one as US does not have a single regulation or authority that manages data protection questions, which in turn represents a problem for viable harmonization of those two legal systems in this field. The chapter gives the brief overview of the main legal documents that might be applicable in different cases for data protection as well as explaining the way how the main data protection enforcement body Federal Trade Commission in the US (FTC) works.

This paper will compare two legal systems as well as explores the ways how they were harmonized historically and now. It explores the historical Safe Harbor agreement which was the first attempt to make US data protection environment adequate for purposes of the EU. Afterwards it analyzes EU-US Privacy shield and challenges towards maintenance of that framework with introduction of the GDPR and its differences with US data protection laws.

INTRODUCTION

With development of social media and information sharing platforms as well as development of e-shops and auctions with giants such as Amazon and eBay selling and shipping goods all over the world, the question about the ways how the data on customer is used by the companies and governments became increasingly more relevant in recent years.

The origins of data protection might be traced to the far of 1980 when the countries that are members of OECD (Organization of Economic Cooperation and Development) established a document called Guidelines on the Protection and Transborder Flow of Personal Data which established an overall global guideline for data protection. However, while other countries such as US did not develop their legislation much further than encompassing those principles in their laws, EU (European Union) went far starting with Directive 95/46/EC on the protection of individuals with regard to the processing of personal data (PII (US)) and on the free movement of such data, which laid out basic principles of data protection that were used until GDPR (General Data Protection Regulation) coming into force.

Previously in EU every country was able to develop its own legislation in regard to privacy issues, based on the guidelines provided in the directive. Which in the end meant that some countries allowed companies to extract more information from consumers and use it more freely than in other countries, which damaged the cross-country business as well as created a more problematic environment for businesses themselves to operate in as some countries could fine them for something that they were able to do in their home country. GDPR therefore was established as a means to unify the laws of all the countries within the EU as well as to provide enlarged extraterritorial scope for the data protection laws. Additionally, it provided a heavily increased fines for the companies violating GDPR with up to four percent of annual turnover or 20 million EUR (taking the greater amount).

To address the rising privacy issues, EU has developed a regulation which started to apply as of May 25, 2018 superseding Directive 95/46/EC, to provide authority to local supervisory bodies to be able to monitor more closely the actions of the companies in regards to personal data and how it is used and stored. This now involves companies having to establish compliance departments (or outsource that) to map the data being processed by the company, as well as establish the processing procedure that is according to the legislation. Therefore, for many companies, both in EU itself as well as abroad (as GDPR has extraterritorial application), this Regulation means a lot of losses due to increased expenses for compliance as well as very strict fines in case of non-compliance.

New Regulation builds on top of many previously existing European privacy law concepts and creates new rights for the individuals in terms of their data, providing companies with more challenges to follow the regulation. As is discussed in the legal document itself, one of the main goals of GDPR is to benefit citizens and businesses by providing a unified set of rules which would build towards common welfare of the EU.

The thesis will mostly involve analysis of application of GDPR and US Data protection laws on private companies and public companies and institutions, rather than individuals (from controller/processor perspective) due to size restrictions of this thesis. The research question of the thesis therefore is “Why the EU-US framework for data transfers was found to be irrelevant and not compliant with requirements of the EU law?” and “How two legal systems

can be better harmonized based on the analysis of both of them, compared to previous frameworks, to achieve a stable free flow of information?". To analyze those research questions it would be needed to analyze the two legal systems of the European bloc and US to see what are the real differences that prevent their cooperation without the specific framework in place as well as to see where are irreconcilable differences that need to be addressed in separate agreement in the first place.

To analyze stability of the new framework it would be important to understand if it at this point is compliant to laws that are in place in EU and US, as well as if it would continue to be effective when new developments in private information monitoring, processing and controlling appear and if its broad enough to capture changes in technological area.

To analyze relevancy, we are evaluating both sides to see which one provides better protection to the individual in terms of privacy in the era of new technology and which framework would be able to ensure adequate protection in the future.

As the thesis has as its goal to propose a better way how to regulate the data exchange between the two legal systems, it might be seem inappropriate to analyze only historical and current existing frameworks, without delving into local legislation itself, as the differences of legislation between EU and US might give an insight on what is currently different in those two legal systems while not being covered by the framework or the thesis might conclude that a more laissez-faire approach should be adopted as those two legal systems do not have enough differences to try to regulate those through such a cumbersome international endeavor.

The way how the evaluation of the quality of data exchange would be considered is that both countries would be evaluated in their internal consistency of rule application, the extent of protection of private data and hence it would be understood which of the two frameworks is better for maintaining privacy of individuals and how the systems can be put in a more consistent way towards each other without overburdening either of the sides.

The work will be structured in a following way:

- First chapter will be dedicated to analysis of GDPR clauses, the way how they protect individual rights for data privacy and how they ensure that companies are unable to use private data in a way that would be disproportionate to the services they are providing to the individual based on such data

- Second chapter would be dedicated to the similar analysis of the US law and how it compares to its European counterpart, with ways regulated similarly or better and where those laws could use some improvement to be more in line with European ones

- Third chapter would be dedicated to listing conclusions of the analysis of the two systems and it lists the possible solutions to the problem of the free data flow between two countries trying to find a way to maximize relevancy and stability of the new framework

This research thesis will mainly use comparative methodology to see which of the countries provides the best solution to the problem of data protection for the individuals and how those legal systems can be harmonized to ensure equal protection for EU citizens both inside the EU and abroad.

Additionally, doctrinal method will be used throughout this thesis to analyze the relevant legal acts and to interpret them to understand what are the actual actionable bases for individual to have against the company if his/her data are processes in an unlawful manner, as well as what redress mechanisms are available.

As mentioned by many scholarly articles, comparing two legal systems such as US and EU in terms of data protection is a very complicated endeavor, which is why both sets of laws should be comprehendingly analyzed and differences understood. The author of this paper cannot provide a very deep specific insight into one or couple of themes related to those differences, as it would miss the whole point of the work and would not help in creating a unified understanding of the problems that creation of unified framework poses. Therefore, both law systems would be analyzed, and most glaring differences recorded for the analysis and further proposal of solutions.

CHAPTER 1: Description of the Legal Documents

As to explain in more details the way how GDPR can affect businesses and whether it can cause additional loses for entrepreneurs, the paper would present comparative analysis of GDPR compared to the previous Directive as well as to EU-US Privacy shield, as many companies that are now affected by GDPR are outside of the EU and a lot of those companies are registered in US. One of the main reasons for GDPR to be introduced instead of the previously mentioned Directive (Directive 95/46/EC) is that due to differences in how the countries are implementing the Directive, companies had problems to be able to comply uniformly with all the laws throughout the Union due to sometimes different requirements and other differences in adoption of this legal document. Therefore, the goal of this chapter is to give an overview of how GDPR approaches data protection within European Union, for further comparison with US.

There is little difference between definitions of the personal data under GDPR compared to Data Protection legislation in the US. GDPR defines personal data as "Personal data are any information which are related to an identified or identifiable natural person[1]", while US does not have a uniform definition (varies from state to state), most of them do not have significant differences. However, GDPR considers personal data to include ID numbers, online identifiers (such as IP address and such) or location data. It also includes biometric and genetic data as specific types of data for protection. Organizations that use this data (especially common with location data) to provide their services, will need to ensure proper use of the data and informed consent on the part of the users, in case consent is used as a lawful basis for processing of data (which it does usually in case of commercial companies and current trans-Atlantic framework is done for commercial purposes). The consent of the person is the whole theme by itself with requirements for consent being that it is given freely and only for specific purpose of the processing[2].

[1] *Infra* note 2
[2] *Infra* note 3

As was discussed earlier, GDPR has an enlarged territorial scope of application, in case for the companies established within the EU it applies for all the information they are gathering and storing would be subject to GDPR irrespective of whether the data itself is the of the EU citizens or the ones from abroad[3].

For the companies that are outside of the EU the GDPR will apply if the data subjects are monitored or used to offer goods or services for any data subject within the EU.

Firstly, to properly analyze GDPR we would need to establish a set of necessary definitions as to what is considered data subject, data controller and data processor apart from the already mentioned definitions of "data breach" and "personal data" that are already in the text.

Data controller is considered to be a main decision-maker in respect to the data, they exercise the control over what to do with data and to process this data. Controller should also have a good goal which needs to be attained (material or otherwise) and therefore obtain this data on purpose of achieving this goal. Controllers assume the highest responsibility in compliance terms towards GDPR as they must comply with all the data protection principles and other related obligations as well as to ensure that all of the data processors also comply with the regulation. In Google Spain case the ECJ established that search engine operator such as Google can be considered a controller, as despite the fact that it does not always gather the personal data that was not already published by someone else, but it provides means and determines what data will be indexed by the search engine[4].

The difference between the data controller and data processor is the degree of their control over the data acquired about the individual. If you exercise overall control over the means and the amount of data to be processed, then you are a controller, if not and you only act as per client's instruction then you can be considered processor.

Data processor has more lenient regime for data protection as he does not need to pay data protection fee which are applicable in some of the Member States, however data processors have some specific requirements under GDPR which he is obliged to fulfill.

In regard to gathering, processing and storing the data for future use, GDPR lays out seven key principles:

- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimization
- Accuracy
- Storage limitation
- Integrity and confidentiality (security)
- Accountability

It is important to note that while GDPR applies to companies and Member States (except when the data is used in accordance to activities which fall within the scope of Chapter 2 of Title V of the TEU) it does not apply to Union institutions themselves as their data processing and storage is regulated by Regulation (EU) 2018/1725 which in turn provides more lenient legislation for the purposes of the Union, to ensure that the Union is able to use personal data

[3] *Supra*
[4] *Infra* note 22

to provide its citizens with appropriate help and services, as well as to identify them throughout the Union itself. It is important to note as compared to any other public institution of the Union, all of the aforementioned analysis of the GDPR as legal document would not apply to it.

The analysis of each of the principles is important to understand how similar principles surface themselves in US legislation and to understand whether US legislation provides similar or higher degree of protection in each of the mentioned principles and if not, what parts are lacking.

Data Minimization

Compared to the previous Directive, GDPR does little to change the data minimization principle in data gathering. In general the personal data that is gathered should be sufficient to properly fulfill your stated purpose, has a rational link to that purpose and you do not hold more than you need for that purpose as per the Article 5 (1) (c): "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed"[5]. The most prominent difference between GDPR and Directive 95/46/EC is that under new accountability requirements the company should show and be able to prove that the data gathered actually fulfills the aforementioned criteria[6].

Additionally, according to GDPR individuals also have right to complete the data they find insufficient or incorrect about them providing just enough for the purposes of data processing of the company in question. This is the right of rectification presented to individuals under the new regulation.

There are no specific guidelines in determining what can be considered to satisfy criteria of data minimization under GDPR, moreover, there is no relevant case law available as of today for this principle under new regulation. However, since this principle can be considered comparable to the one enshrined in Directive 95/46/EC under Article 6 (c): "Member States shall provide that personal data must be: adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed"[7] therefore, the cases related to same principle under this directive would be used to explain how they could be used under GDPR as well.

In the case Rechnungshof (C-465/00), the case itself involved the law that required Austrian public bodies that are controlled over by The Court of Auditors to submit information about salaries and pensions that their employees receive if it is above a certain limit. This information would be further transmitted to other governmental bodies and then consequently

[5] *Supra* see 2
[6] Information Commissioner Office, Guide to the General Data Protection Regulation (GDPR) August 2018
[7] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal L 281 , 23/11/1995 P. 0031 – 0050, October 1995, https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A31995L0046

published. The idea of this law was to increase the public pressure upon the public bodies, therefore ensuring that salaries for their employees would stay in reasonable limits[8].

The case itself dealt not only with the issue of necessity but also with issue of applicability of the Directive and its scope, however, for the purpose of this research this issue might not be as relevant as it new regulation has enlarged scope, therefore rendering this part of the decision obsolete. However, firstly this case indicates that under the scope of the directive, hence under the scope of GDPR as well, information about salaries of the people fall under protection of personal data. Secondly, this case stipulates that while the reason to promote economic well-being and creating a system of checks and balances within the system is an acceptable goal under the Directive to be gathering and publishing data about, ECJ (European Court of Justice) argues that in this case the national courts should examine whether the data gathered and published is proportional to the aim that the government was aiming to achieve and whether it is both "necessary and appropriate" to use this type of data to achieve this social goal[9].

Another case that analyses proportionality of the data collected is C-291/12. In this case a citizen of Germany refused to give his fingerprint for the purposes of receiving a passport. And when in turn the agency that gives out passports refused to provide him with one, he disputed the validity of the regulation (Regulation No 2252/2004) that requires European citizens to have fingerprints on their passports. The court argued that action itself does not represent any physical and mental discomfort and this data by itself cannot be classified as sensitive. Moreover, court argues, that there is no better alternative to achieve sufficient means to identify person who is carrying the passport without the fingerprints scan. Moreover, it argues that while there is a possibility for this data to be used for other purposes, due to it being stored centrally, it does not preclude validity of the regulation in respect to data protection as it tries to achieve sufficiently relevant social goal.[10]

Accuracy

Accuracy principle entails that the personal data that is gathered by the company (or other data controllers) should not be incorrect or misleading in any way that is possible for the company in question to check. It does also require the company to keep the information updated to the best of its ability, as to ensure it stays correct. And in case the data is incorrect or misleading the company should take reasonable steps to correct the data or erase it fully[11].

---

[8] JUDGMENT OF THE COURT, REFERENCES to the Court under Article 234 EC by the Verfassungsgerichtshof (C-465/00) and the Oberster Gerichtshof (C-138/01 and C-139/01) (Austria) for preliminary rulings in the proceedings pending before those courts between Rechnungshof (C-465/00), 20 May 2003, http://curia.europa.eu/juris/document/document.jsf?text=&docid=48330&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=6469063

[9] *Ibid*

[10] JUDGMENT OF THE COURT In Case C-291/12, REQUEST for a preliminary ruling under Article 267 TFEU from the Verwaltungsgericht Gelsenkirchen (Germany), made by decision of 15 May 2012, received at the Court on 12 June 2012, in the proceedings, 17 October 2013, ECJ(Fourth Chamber), http://curia.europa.eu/juris/document/document.jsf?text=&docid=143189&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=10252650

[11] *Supra* note 6

Compared to the previous directive, GDPR has introduced a requirement for the companies to act more proactively in respect to data deletion or correction in instance when it's wrong or is already not relevant.

Lawfulness, fairness and transparency

This principle entails that for data gathering the controller should first identify valid grounds (lawful basis) under which the data would be gathered, according to the regulation. It also requires that the actor ensure that the way how the data is acquired stored and used does not breach any other relevant international or local law[12].

Additionally, it also requires the company to use the data in a way that is fair towards individuals that are concerned with it. This means that the company cannot use the data in any way that might be misleading or detrimental to the individual, unless there is a lawful reason to do so (as to providing information to authorities in charge of criminal investigation of the individual)[13].

The actor that uses the data should also be sufficiently clear and honest about the way how the data is going to be used, since the company has the right to use any personal data only in a way that was authorized by the person who is the data subject. It is however only relevant to the cases where the lawful basis for processing of data is consent.

To ensure that the data of the data subject is processed lawfully the company needs to make sure that the data that is provided was gathered based on some lawful basis. There are 6 legitimate lawful bases on which the data can be gathered about the individual:

1. Consent: as the individual is providing the actor with clear consent to process their personal data to achieve specific purpose. This is usually the legal basis under which most of the marketing activities fall under.

2. Contract: The processing of the information provided by the individual is necessary to fulfill the contractual obligation between two actors, one of which is the data subject in question. This can also work before signing the contract if the individual has requested the actor to take specific steps before entering into contract.

3. Legal Obligation: The processing of the information is necessary for the individual to comply with the law of the country (or Union) excluding contractual obligations.

4. Vital interests: Where the processing of the information is required to protect someone's life.

5. Public task: the processing of the information is necessary for the controller to perform a task that is in one way or another related to fulfillment of public interest or to perform your work duties in official environment, where this task has a clear legal basis in the law of the country.

[12] *Supra* note 6
[13] *Ibid*

6. Legitimate interests: Where the processing of the information is necessary for legitimate interests of the individual or the third party, unless there is an overriding reason that would require to protect individual's personal data[14].

Therefore, for the company/institution to comply with lawfulness principle it has to gather the data in accordance of one of the aforementioned principles.

The consent as reason for gathering data is considered to be much stricter under GDPR. Therefore, unless u specifically have no other applicable legal basis for gathering of data it is easier for the company to use other reasoning as legal basis. Consent require the company to provide an opportunity for the individual to exert control over his data, in the way of which data will be collected, to which purposes it will be used and for how longs it will be stored, as well as opportunity to review this data and modify it for the sake of its accuracy.

For the consent to be considered legitimate, there are several conditions that the company has to fulfill:

- Firstly, consent should be "freely given" as there should not be any pressure applied towards the data subject in respect to giving his/her private data. There should be balance of power between two parties in negotiation and furthermore, the provision of the service must not depend on the data subject providing consent unless it is specifically necessary for provisions of the service
- Secondly, consent should be "specific" as discussed throughout this paper, it should be specific towards the operation that the company needs to fulfill with this data. It is also required that the consent would be received in such form that it would be "clearly distinguishable" on the aim of it and what are allowed ways how the data can be used and it should be provided in "intelligible and easily accessible form"
- Thirdly, consent given by the individual should be "informed", which means that the data subject must be aware of the identity of the controller and of the purpose of the processing.
- And lastly, the consent should be given in "unambiguous" way, as to be declared with statement or affirmative action. It is specifically said that the consent would not be considered unambiguous if it given with "silence, pre-ticked boxes or inactivity"[15].

To use contractual obligations as the legal basis for the processing it is absolutely required that it would be the only way for the company to fulfill its contractual obligations towards the individual. Therefore, this lawful basis can only be used in event where there are no less intrusive ways how to perform contractual duty. It is also important to note that in this sense it should be necessary for the company to perform the contract especially with this person as if gathering of the personal data is part of company's business model then this by itself does not constitute the necessity for the sake of GDPR[16].

The use of legal obligation principle is quite similar to using contract one, as it also requires the party to consider all the less-intrusive ways on how to fulfill its legal obligations without using individual's personal data or using as little as possible for the fulfillment of the given goal. It is not by itself necessary that the law explicitly allows to gather data in such

[14] *Supra* note 6
[15] CHALLENGES FOR THE BUSINESS WHEN COMPLYING WITH THE GENERAL DATA PROTECTION REGULATION, Vyara Gocheva, June 2017, http://arno.uvt.nl/show.cgi?fid=143639
[16] *Ibid*

situation, it just should be "foreseeable" for the individual that for fulfillment of this obligation the company/individual would have to gather and use the data that was stored about the person[17].

The use of vital interest as a lawful basis for gathering and processing data requires a specific instance of having to protect individual's life. In the similar way as with previous two bases, it requires that there will be no other way to ensure person's safety other than gathering and using his/her personal data. The situations for using such legal basis usually arise in even of requiring urgent medical care, where the medical institution needs data to save individual's life but individual is incapable at that moment to provide consent[18].

Public task legal basis is the most relevant of course for the public institutions and authorities that process data based on their lawful requirements. Again, to be able to gather and use individual's personal data, a person exercising public authority or acting in public interest should be able to demonstrate that the data is absolutely necessary to perform the duty laid down in the law. The institution itself does not have to have specific legal authority to be able to process such data if it can prove that it does it for specific public need that is necessitated by law.

Legitimate interest is perhaps the most confusing of the lawful bases under which the data can be gathered and processed. It is one of the most flexible principles, however, it is better to use any other one if there is a possibility to do so. In general, to process data for legitimate interest it is required to provide this legitimate interest based on some other lawful right, you need to prove that the gathering, storing or use of this data is necessary to fulfill this legitimate interest. Furthermore, achieving this legitimate interest needs to be balanced against other rights and freedoms. Therefore, it is most likely to be used where either the interest of the party has a great weight or where the impact on individual's data protection rights is minimal. As was discussed in case C-212/13 by CJEU, the use of legitimate interest where the person is afraid for his own life and installs surveillance to be able to track assailants can be considered a use of the derogation such as legitimate interest[19].

Additionally, in case C-73/07 it was established as the countries are obliged to provide derogation from data protection laws for purely journalistic purposes that can be considered as being a legitimate interest mentioned above. It was established that actions performed to disclose "public information, opinion and ideas" irrespective of the medium of information, then it can be considered to be used solely for journalistic purposes for the sake of GDPR and hence GDPR would be not applicable in this case[20].

To satisfy fairness principle the company must ensure that the data that is gathered from the data subject is used within the limits of reasonable expectation of the person about the ways

---

[17] *Ibid*

[18] *Ibid*

[19] JUDGMENT OF THE COURT In Case C-212/13, REQUEST for a preliminary ruling under Article 267 TFEU from the Nejvyšší správní soud (Czech Republic), made by decision of 20 March 2013, received at the Court on 19 April 2013, in the proceedings František Ryneš V Úřad pro ochranu osobních údajů, http://curia.europa.eu/juris/document/document.jsf;jsessionid=0D9FE943F58828D6327EBB72760C2F4F?text=&docid=160561&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=506951

[20] JUDGMENT OF THE COURT, In Case C-73/07, REFERENCE for a preliminary ruling under Article 234 EC from the Korkein hallinto-oikeus (Finland), made by decision of 8 February 2007, received at the Court on 12 February 2007, in the proceedings Tietosuojavaltuutettu v Satakunnan Markkinapörssi Oy,Satamedia Oy, 16 December 2008, http://curia.europa.eu/juris/document/document.jsf;jsessionid=7F7F47B1C4DD9A332A383F92ADD9DFFE?text=&docid=76075&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=696472

how it can be used. It therefore expects that the use of data would not result in unnecessarily harmful or adverse effects towards the individual[21].

The answer to the question whether the data usage is fair or not can be strongly affected by the way in which the data was gathered from the individual. Which means that if the individual was misled or deceived when consenting to use of his personal data, it is unlikely that this use of data would be considered fair[22].

To ensure that the company complies with the transparency principle it should also ascertain that the way how they are performing their data gathering is honest and clear to any individual involved. Therefore, as it can be understood it is closely linked to the fairness principle discussed above[23].

This principle is important in any dealings with data, but especially it is relevant in case where the individual has the choice of whether to provide you with his personal data or not. Therefore, if the individual would know about the ways how his data would be used, it is more likely that he would be able to make an informed decision about whether he wants to provide his data or not[24].

As was discussed by the ECJ in Google case, the non-compliance with the lawfulness principle might arise for the company even in the event where the company does not disclose or provide the information to the controller or the third party which has the "legitimate interest" in the data stored[25].

Storage limitation

The basic premise of storage limitation requirement is that the company should not hold onto the data for longer than it is needed to fulfill any of its legitimate goals. It is however not applicable in respect to anonymized data, as the regulation allows the companies to keep such data and treat it as an erased data for the purposes of the law[26].

The Regulation also provides that the company or institution can maintain the data for the purposes of public interest, such as future scientific research, historical research or statistical purposes[27][28].

---

[21] *Ibid*
[22] *Ibid*
[23] *Ibid*
[24] *Ibid*
[25] JUDGMENT OF THE COURT In Case C-131/12, REQUEST for a preliminary ruling under Article 267 TFEU from the Audiencia Nacional (Spain), made by decision of 27 February 2012, received at the Court on 9 March 2012, in the proceedingsGoogle Spain SL, Google Inc. V Agencia Española de Protección de Datos (AEPD),Mario Costeja González, 13 May 2014, http://curia.europa.eu/juris/document/document.jsf?text=&docid=152065&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=924847
[26] *Supra* note 6
[27] *Supra* note 6
[28] Pasi Reini, GDPR implementation, 2019, https://www.theseus.fi/bitstream/handle/10024/166514/Reini_k7696_thesis_versio4.1.pdf?sequence=2&isAllowed=y

The Storage limitation principle is closely related to data minimization principle as well, as the timely erasure of the data might allow the company to be better compliant with the regulation. The main reasoning under which the company should not retain the information about the person for longer that is needed is that the data tends to become unnecessary at times as well as become inaccurate due to it being out of date, which would also violate another principle enshrined in the regulation[29].

In general US does also provide some laws in regards to storage limitation, as legislators have shown that there is no possibility for anyone to store data about individuals indefinitely, however, for government institutions this period can be up to 180 days after the use of the data, unless it is needed still, which is different under GDPR where even government institutions are required to erase data immediately if its not anymore required for performance of any public related duty and is not covered by any of the clauses in lawfulness principle[30].

Integrity and confidentiality

One of the key principles in GDPR is the data is processed securely through means of "appropriate technical and organizational measures". To satisfy these criteria the company needs to put in place risk analysis procedures as well as other measures (technical in both virtual and physical space) that would allow it to ensure safety of the data from external tampering.

The company must ensure that it uses sufficiently new technologies according to their financial position and type of data that they are holding. The investment into data security within the company should be appropriate to the risks that the company is facing as well as circumstances under which data is gathered and stored.

Accountability

This principle requires the company to analyze its activities and to take accountability in respect to its fulfilment of the GDPR. It requires the company to put in place proper technical and organizational measures to ensure accountability on the side of employees and management of the company[31].

Accountability can be considered to be the biggest introduction in GDPR as previous Directive did not include explicit mentions of company accountability for following the aforementioned principles of the GDPR. The company is now required to be much more proactive in respect to fulfilling its responsibilities under this document. This accountability also involves proactive actions such as implementation of impact assessments for the data protections procedures[32].

---

[29] *Ibid*
[30] *Infra* 103

[31] *Supra* see 2
[32] *Ibid*

In general, there are 2 elements for this principle, first one that the company is responsible for its actions and secondly that the company should be able to present that they are compliant with the regulation, as opposed to authorities trying to find mistakes within the system of the company[33].

While the requirements might seem superfluous and too general to be applied, it actually would require a series of a concrete steps to ensure that the company is compliant with the regulation. In essence the company must be able to demonstrate that they are treating private data in a responsible way. To achieve that larger companies usually work out a set of obligatory procedures and educational programs for employees to ensure that all the representatives of the company are aware of the best practices in terms of data protection[34].

Additionally, the company should establish the framework which would at least include a strong program controls that ensure compliance with the GDPR. It should also ensure appropriate reporting procedures and culture as well as regular assessment of other measures that need to be implemented to ensure better control over data stream. It also requires that the fulfillment of the aforementioned principles would be documented, as the company needs to provide the procedures for the ways how it retains, acquires and stores the data that comes into its possession. Most importantly, of course, is that in instance where the company uses person's consent as legal basis to acquire and store his data, they should also provide that this information is readily accessible in case authorities would like to check it.

CHAPTER 2: US Legislation

Compared to European Union, US does not have one uniform document that encompasses all the regulations and procedures needed to be taken in order to comply with Data Protection within the country, instead a series of legal acts are taken.

The first and perhaps the most important document that provides rights for protection of individual's privacy is the Constitution itself, as it provides: "the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures"[35]

Therefore, effectively it provides a legal basis for people who consider their data to be seized and/or used in a way that they might see as unreasonable. In addition to that a plethora of various federal laws are dealing with more concrete examples of individual's right to protection of personal data. These laws concern (but are not limited to) any kind of financial information, health related information, child related information or education records that are protected by specific federal laws. Additionally, due to this there are many bodies within the country that are dealing with improper use of data, which makes the general way to report the data breach violation more complex. There are several bodies that might be dealing with certain kind of violation related to personal data, such as: Federal Trade Commission (FTC), the U.S.

[33] *Supra* see 6
[34] *Ibid*
[35] United States Constitution Fourth Amendment, US Congress September 25, 1789. Ratified December 15, 1791.

Department of Health and Human Services (HSS), the Consumer Financial Protection Bureau (CFPB) and the Federal Communications Commission (FCC)[36].

While all of the aforementioned bodies are involved in data protection in one way or another, only FTC can be considered a body whose primary objective is protection of customers from unfair use of their information for commercial purposes. This body has jurisdiction based on Federal Trade Commission Act, which provides the broadest jurisdiction within US in case of data privacy questions. It has jurisdiction over most of the individuals and entities, however with some notable exceptions being financial institutions (such as banks, federal credit unions etc.) and non-profit organizations[37].

Under FTC Act, the FTC itself has the jurisdiction to enforce the following laws to protect the data of the individuals:

- The Children's Online Privacy Protection Act (COPPA)
- The Fair Credit Reporting Act (FCRA)
- The Telemarketing Sales Rule[38]

There are several other documents that in one way or another regulate protection of data for individuals and that are enforced by other federal agencies throughout the US: The Communications Act of 1934, Electronic Communications Privacy Act of 1986, Federal Privacy Act of 1974, Family Educational and Privacy Rights Act (FERPA), The Gramm-Leach-Bliley (GLB) Act, The Health Insurance Portability and Accountability Act of 1996.

The application of data protection laws is not as uniform as it is going to be now within the EU with introduction of the GDPR, due to many agencies performing their own enforcement and States still having jurisdiction to provide further application of data protection laws. As for Example State of California has more than a dozen of additional legal documents governing the rights of its citizens related to digital privacy rights for children, online privacy notices, and disposal of customer record and telecommunications privacy. While California does have one single act CCPA (California Consumer Privacy Act) that has its sole purpose to attain enhance privacy rights, it does apply only for commercial relationships, as can be deduced from its name[39].

Privacy by design entails that the company does ensure data protection and privacy not just as a legal requirement to fulfill at some stage of the project or organizational development, but by default. Privacy must come integral to every project, organization structure, workplace culture etc. to provide an environment where data will be secure[40].

To fulfill the requirement of privacy by design the company has to ensure that its actions towards data privacy are proactive, rather than remedial. Which means that the company should strive to foresee the problems it might encounter in terms of data protection. It should also ensure that its community and stakeholders are also treating data, that is transferred to them or that they might come into possession of, with the same care as the company itself.

---

[36] Data protection regulations and international data flows: Implications for trade and development, United Nations, 2016, https://unctad.org/en/PublicationsLibrary/dtlstict2016d1_en.pdf
[37] Data Protection Law: An Overview, Congressional Research Service, March 25, 2019, https://fas.org/sgp/crs/misc/R45631.pdf
[38] *Ibid*
[39] *Ibid*
[40] Privacy by Design The 7 Foundational Principles Implementation and Mapping of Fair Information Practices6 Ann Cavoukian, Ph.D, 2011, https://iab.org/wp-content/IAB-uploads/2011/03/fred_carter.pdf

It also requires that the company incorporates data privacy in its design. It also requires that the company provide a detailed self-assessment reports on the possible privacy risks within their structure and try to implement continuous improvement process to ensure that the potential gaps in its data security are spotted and filled.

US data protection laws also require that the data that is gathered by the company is sufficiently accurate, in essence mirroring the one in the EU. Requirement for accuracy of the data also provides the safeguards for storage limitation, as data that is obsolete cannot be considered accurate anymore, therefore for the sake of data not being used incorrectly towards the individual it should be erased by the company in question[41].

To analyze principles and safeguards provided by them in depth, we would need to give a short overview of each of the documents that regulates data protection in US and compare it to the way how GDPR handles issues in those documents.

Federal Trade Commission Act

As was discussed earlier, the main legal document that regulates most of the data protection spheres as well as provides the main body that deals with it with jurisdiction to do so is FTCA. The main reason for creation of FTCA was to prohibit "unfair or deceptive practices in or affection commerce"[42]. The Federal Trade Commission oversees vast swathes of information coming towards it from every state as well as oversee international cooperation in respect to data protection[43].

In respect to preventing deceptive practices the FTCA is enforced in a way that the company is found liable for deceptive practices in any event of the company not withholding their promises in terms of their privacy policy of protection of data from external threats (such as hacker attacks). It also provides that the company must not miscommunicate or twist the facts to induce disclosure of personal information[44].

Federal Trade Commission Act indicates the requirement for data security of the data, providing that the ongoing monitoring to ensure data Integrity and Confidentiality is to be applied, however the specific "technical" requirements that are obligatory to follow in EU does not apply in US and are instead just recommended by Federal Trade Commission[45].

---

[41] *Supra* note 26

[42] Marcia Hofmann, Federal Trade Commission Enforcement of Privacy, (2011), https://www.ftc.gov/policy/policy-statements

[43] Data Protection Law in the USA, Robert Hasty, Dr. Trevor W. Nagel and Mariam Subjally White and Case, August 2013, https://www.neighborhoodindicators.org/sites/default/files/course-materials/A4ID_DataProtectionLaw%20.pdf

[44] *Supra* note 28

[45] Julie Brill, Two-Way Street: U.S.-EU Parallels Under the General Data Protection Regulation, Ghostery/Hogan Lovells Data Privacy Day, 2016 https://www.ftc.gov/system/files/documents/public_statements/910663/160121hoganghostery_dpd.pdf

Health Insurance Portability and Accountability Act

The Health Insurance Portability and Accountability Act (or HIPPA in short) provides prediction to individuals in respect to entities that collect, maintain, use or disclose health information of their clients and/or other individuals whose data they possess. This document provides less protection to individuals in respect to their data. It's scope by itself includes only Healthcare Institutions, either governmental or private. As while it requires the entity obtain consent of the individual for data collection as well as for other further uses of this data, it does not provide storage limitation and accountability principles in the similar fashion as Federal Trade Commission Act[46].

Under the Health Information Technology for Economic and Clinical Health Act the application of this document was extended to cover not only healthcare institutions themselves but also the "Business Associates" of such institutions. By itself this might lead this document to overlap in data security measures with other documents. Even if "Business Associates" are not covered by any other document with US, they would still be liable to provide same measures for data integrity and lawfulness of its acquisition and storage as any Healthcare Institution would need to provide[47].

In general, this act provides a greater protection to the individuals at least in respect to their healthcare information, as it prohibits the company to do anything outside of the firstly stated cause or disclose the information of the patient to any third institution without a clear consent from an individual involved. It also in a similar way provides that the company is obliged to provide the person with the copy of his information in the event where the individual requests that. It is also important to note that this act allows the U.S. Department of Health & Human Services to maintain a report of all the data breaches reported to them, providing additional incentive for companies to ensure security of the data in fear of losing public face[48].

It is important to note that while this document does provide the similar level of data protection as GDPR, it does not provide a large enough scope as even not all the health data of the individuals is covered, but only doctors' offices, hospitals, and insurance companies, which are already for a long time not only kinds of businesses that have access to health information of the individuals[49].

Gramm-Leach-Bliley Act

As was discussed above the Federal Trade Commission Act does not provide the companies with jurisdiction over the financial institutions. For this there is Gramm-Leach-Bliley Act in US which protects the consumer against use of his non-public data. Firstly, in a similar way as HIPPA it prohibits the companies to share the data with any third parties unless the person was specifically notified and offered an opportunity to opt-out of the service

[46] *Supra* note 36
[47] *Ibid*
[48] *Supra* note 28
[49] Christine S. Wilson, A Defining Moment for Privacy: The Time is Ripe for Federal Privacy Legislation, US Federal Trade Commission, 2020, https://www.ftc.gov/system/files/documents/public_statements/1566337/commissioner_wilson_privacy_forum_speech_02-06-2020.pdf

provision. It also prohibits use of some specific types of data to be used in direct marketing campaigns, such as account numbers or credit card numbers[50]. In this way it is similar to the way how European laws protect its citizens in a way that the company should provide opt-out options and make sure not to disclose information to third parties without the consent of the individual[51].

However, this document does not address the problems of data minimization nor other principles enshrined in GDPR and it does not provide an opportunity for individuals to redress the third party in case it accesses their data (for example legal authorities) if the individual is not a US citizen[52].

This document does not have one enforcement body, but rather two of them, as discussed above FTC is responsible for enforcement of all the non-depository data protection violations while banking regulators are the one responsible for depository ones[53].

Fair Credit Reporting Act

Fair Credit Reporting Act (FCRA) governs the information about individuals relating to their creditworthiness. Contrary to the previous two legal acts FCRA does not provide requirement for the companies to inform customers of disclosure of their information to the third parties as well as the option to provide opt-out options. It is mostly concerned instead with the accuracy of the information transmitted between the parties and with restricting the purposes under which this data might be gathered and used[54].

To ensure accuracy of the reports the company must gather information only from trusted sources as well as follow storage limitation rules, providing that the person had civil judgments in respect to one of his account, they must delete and disregard such information after certain amount of times passes[55].

Video Privacy Protection Act

Video Privacy Protection Act (VPPA) was enacted to ensure data protection for video tapes, and other audio and visual materials in terms of their rental, purchase or delivery. In contrast to other legal acts discussed above, VPPA does not provide companies with the obligation of creating a secure environment for storing the data on their customers as it does not provide any reasonable safeguards for individual's information. At the first glance, it is

---

[50] *Ibid*
[51] *Ibid*
[52] Leena Salolatva, Privacy Shield Redress Mechanisms Assessment in the Light of the Schrems Case, University Of Helsinki, https://helda.helsinki.fi/bitstream/handle/10138/191333/Privacy%20Shield%20Redress%20Mechanisms%20Assessment%20in%20the%20Light%20of%20the%20Schrems%20Case.pdf?sequence=2&isAllowed=y&fbclid=IwAR05D-rGw3IlW5-C37hhgkZahnZ8aZLAvsZQ_NOL5ZeIvdOGYix-TM_oXcY

[53] *Ibid*
[54] *Ibid*
[55] *Ibid*

unclear whether in this case FTCA would apply as well, since rental or purchase of the audio-visual material can be considered a commercial activity[56].

It does, however, provide that any company that provides such services must always provide an individual with an opt-out option before transferring their data to the third party, unless this information is not personally identifiable. However, this provision has an exception in case such data transfer is "within ordinary course of business".

Family Education Rights and Privacy Act

Family Education Rights and Privacy Act is applicable towards educational institutions in respect to their data related to school and university records. In general, this act requires that the individual or in case of a school pupil, his parents, have control over disclosure of private information of the student towards the third parties as well as opportunity to review the records gathered with possibility to propose changes to improve accuracy of those reports.

Consumer Financial Protection Act

Consumer Financial Protection Act (CFPA) has in its scope any company or individual that provides any kind of financial service to the consumer (which means it overlaps with both FTCA and FCRA). The structure of the document can be considered similar to FCTA, as its main task is also to prohibit the companies to engage in "unfair, deceptive or abusive" practices towards the consumer's data.

However, there are several important differences of CFPA compared to FTCA. Firstly, as is clear from the wording, CFPA adds abusive practices to the list of "unfair and deceptive" ones in FTCA. Those practices are considered to be the ones that "materially interfere with the ability of the customer to understand a term or condition of a consumer financial product or service" or "take unreasonable advantage of consumer's (a) lack of understanding, (b) inability to protect her own interest in selecting or using a consumer financial product or service, or (c) reasonable reliance on a covered person to act in her interest[57]"

Computer Fraud and Abuse Act

The main idea of Computer Fraud and Abuse Act (CFAA) was not to provide data protection right but to prohibit hacking attempts or other unauthorized intrusions. It relates to information acquired from any "protected computer" and does not rely on it being personal data or any other type of data, but due to it protecting all kinds of information stored, it can be considered to be overlapping with other legal acts described above[58].

---

[56] *Supra*
[57] *Supra*

[58] *Supra*

Another reason why this Act can be important in terms of data protection for individuals is that it is not only enforceable by public institutions, but also gives the right to individual to seek remedy for the actions of anyone who has received unauthorized access to their data. It in turns would also enact criminal responsibility for the person. It is, however, harder to prove as it also requires that the damage done to the party by this theft of information would be significant and would be possible to translate into financial losses (rather than only moral damage)[59].

59 *Supra*

CHAPTER 3: Analysis OF Data Protection Laws

Harmonization: History and Contemporary Perspective

To compare US legislation to the European GDPR for data protection it would be useful to understand the things that already existing framework of data protection for companies between EU and US works, and how maybe it can be improved in one way or another or the way in which laws of the two countries could be harmonized. To do that we need to analyze contemporary ES-US Privacy Shield, the laws of the countries themselves and to see what the history of their cooperation is.

History of EU-US data transfer

The main basis for cooperation in data transfer sense between European countries and US before introduction of Directive 95/46/EC was relying on the OECD (Organization for Economic Co-operation and Development) guidelines as well as Convention 108 (Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data). While the guidelines from OECD quickly overtook global arena in terms of data protection legislation (as countries were implementing laws similar to the guidelines), EU decided to go further than the guidelines entail in a way of internal, EU level, legislation in form of the directive should have ensured a more harmonious and uniform legal environment throughout the Union compared to countries implementing data protection legislation on their own. The aforementioned convention was a document designed specifically to "*secure in the territory of each Party for every individual, whatever his nationality or residence, respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him*[60]".

As you can see from the analysis above, the data protection framework in US is much more lenient than it is in European Union, therefore just following one set of guidelines, which impose no legal obligations upon the countries. However, the "Safe Harbor" framework that was implemented between EU and US on July 26, 2000 was meant to address exactly this problem. The Directive 95/46/EC already entailed a way for third-countries to operate within the Union if they comply to "adequate level of protection" criteria set by the Union, the list of the countries that did not require any additional authorization was quite extensive including Andorra, Argentina, Canada, Faeroe Islands, New Zealand and Switzerland, etc.[61].

[60] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Strasbourg, ETS 108, 1981.
[61] Harpo Vogelsang, An analysis of the EU data protection policy and the significance of the Maximillian Schrems case, University of Twente, July 2019

Despite that, due to US not having a uniform data protection law and in many cases its regulations being much more lenient towards corporations, EU did not deem US data protection laws to be "adequate" without additional agreements[62].

As was stated in the decision of the Commission, the reason for US laws being deemed not adequate are *"The United States uses a sectoral approach that relies on a mix of legislation, regulation, and self-regulation. Given those differences, many U.S. organizations have expressed uncertainty about the impact of the EU-required "adequacy standard" on personal data transfers from the European Union to the United States[63]"*

Therefore "Safe Harbor" agreement was mainly made to ensure that US companies follow similar rules compared to the European ones within EU. The agreement entailed seven principles that the companies must follow (Notice, Choice, Onward Transfers (transfers to third parties), Access, Security, Data Integrity, and Enforcement) such as[64]:

- Notice Principle under which any company within US should make sure that data subjects are informed about their data being collected as well as informed about the reasons for this data collection, the way how data will be used, as well as whether this data is going to be given to third parties for processing. Additionally, the company should provide an opportunity to the data subject to provide complaint or withhold consent to processing of his/her personal data.

- Data integrity principle, in a similar way as it is now enshrined in GDPR and as it was presented in Directive 95/46/EC, data integrity principle required companies to ensure that the collected data remain relevant for the purposes of processing this data as well as the relevant measure are implemented to ensure there are no errors in data and if there are, there is a possibility for data subject to dispute and correct the data.

- Choice principle relates to the first one in a way, that whenever the purposes for which the data will be used or the parties that would be processing the data of the data subject are changing, there should be a possibility for the said data subject to withdraw his/her consent for further data processing.

- Onward Transfers Principle entails that any transfer to the third parties would go through necessity test, as to ascertain that this transfer is actually required to achieve the goals intended for the data.

- Security principle provides that all the data must be stored safely and protected against possible misuse, unauthorized alteration, loss or being stolen.

- Access, is that the data subject should always have a possibility to access and request the data that was gathered by the data controller. Data subject should also always have an opportunity to correct the data in cases where it is not accurate, instead of the cases where such system would entail disproportionally big expenses on data controller.

---

[62] *Ibid*

[63] Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbor privacy principles and related frequently asked questions issued by the US Department of Commerce, European Commission, 2000, https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX%3A32000D0520

[64] *Ibid*

- Enforcement principle entailed that US should establish an effective system to ensure that the companies that operate under Safe Harbor framework are actually complying with all the principles laid out in the document and that any violations that appear are severely sanctioned from the US side.[65]

Under Safe Harbor framework, companies would certify themselves to be compliant with all the of the aforementioned principles to the Department of Commerce in US. The participation in the framework was open to any company that was regulated by FTC (which as was mentioned before is the main data protection body within US). This however excluded health-relate institutions, telecommunications and financial companies and other companies that were regulated by other bodies, due to data protection principles not being uniformly regulated within the country[66].

When the company certifies itself for the Safe Harbor Framework, it had to present a documentary description of the ways how and for which purposes personal data is used within their company. Additionally, the company had to pledge the willingness to co-operate with EU authorities in the scope of data protection, as well as train employees in respect to data protection requirements that the company is facing. The company had to submit self-certification documentation every year to make sure they stay within Safe Harbor framework.[67]

US did not regulate the application of the Safe Harbor framework and any violations were proceeding through complaints filed by EU MS authorities which were further reviewed by FTC. In case FTC found the ground for complaint filed from EU it could fine the company to up to 16 000 $ for each day of the violation and during the work of this agreement has penalized approx. 40 companies with such charges[68].

While all of those principles allowed the corporations to operate on the EU territory, this agreement also allowed a broader access to personal data of data subjects within the EU to the US government, which in turn was one of the big reasons for dismissing this framework. The decision was heavily influenced by political scenery at the time, as due to easier access to data of the EU citizens, MS (Member States) were concerned about what kind of data might be used by the US authorities, especially in the light of the leak in 2013 with information brought to light from former CIA employee Edward Snowden.

Reasons for Collapse of Safe Harbor

The decision that led to the abolishment of Safe Harbor agreement was the ECJ case C-362/14, where Maximillian Schrems, an Austrian citizen submitted a complaint within Irish Data Supervisory Authority (The Data Protection Commissioner) in relation to Facebook not being able to provide sufficient protection to personal data due to the recent leaks relate to Snowden case. He, therefore, argued that US is unable to ensure sufficient protection from

[65] Fransesca Bignami, The US Legal System on Data Protection in the Field of Law Enforcement. Safe-guards, Rights and Remedies for EU Citizens (2015)
[66] *Supra*
[67] Gert Vermeulen, Eva Lievens, Data Protection and Privacy under Pressure, Maklu, 2017
[68] *Supra*

surveillance by public authorities, therefore creating a framework that does not work (Safe Harbor)[69].

The decision that was reached by the ECJ did not come out of the blue as European Commission has already stated just as the crisis was starting that Safe Harbor agreement became "one of the conduits through which access is given to US intelligence authorities to collecting personal data initially processed in the EU"[70] .

First question was whether national authority has the right to evaluate decision by the commission which stated that the US has an adequate protection environment with Safe Harbor framework in place. To this ECJ states that irrespective of the decision of the European Commission, national authorities must be able to independently assess whether transfer of personal data to the third country comply with requirements of the Directive. It is however up to ECJ to decide whether the country in general fulfills the requirements of adequacy to EU data protection Directive[71].

Furthermore the court establishes that since as mentioned before, only companies that are within the scope of FTC jurisdiction (which has jurisdiction only over commercial companies as discussed above) are under the scope of Safe Harbor agreement, it does not apply to US public authorities and institutions, which in turn have legal access to data stored within the corporations[72]. The Safe Harbor allowed US government in the similar way as to any EU country to process and access the data transferred from EU for questions of national security, however, in point of view of ECJ the monitoring performed by US government was disproportional to the goals that it tried to achieve. It therefore argues that governmental authorities having generalized access to personal data of the individuals from EU must be regarded as "compromising the essence of the fundamental right to respect for private life"[73].

Additionally, the CJEU found that this Safe Harbor framework restricts national authorities from deciding whether the agreement violates fundamental rights of individuals for respect for their private life, to which European Commission does not have any legal authority. Based on which the Court considers Safe Harbor framework to be invalid and leaves it in the hands of national supervisory authorities to establish whether personal data of the individuals can be transferred from EU to the US without compromising rights of individuals for data protection that it enshrined within the Directive[74].

---

[69] JUDGMENT OF THE COURT (Grand Chamber), 6 October 2015 (*) n Case C-362/14, REQUEST for a preliminary ruling under Article 267 TFEU from the High Court (Ireland), made by decision of 17 July 2014, received at the Court on 25 July 2014, in the proceedings Maximillian Schrems V Data Protection Commissioner, joined party:Digital Rights Ireland Ltd.

[70] COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL, on the Transfer of Personal Data from the EU to the United States of America under Directive 95/46/EC following the Judgment by the Court of Justice in Case C-362/14, European Commission, 06.11.2015

[71] *Supra*

[72]Tossapon Tassanakunlapan, Protection of personal data in cyberspace:the EU-US E-market regime, University Of Barcelona, 2017, https://www.tdx.cat/bitstream/handle/10803/463075/TOSSAPON_TASSANAKUNLAPAN_PhD_THESIS.pdf?sequence=1&isAllowed=y

[73] *Supra*

[74] *Supra*

Current EU-US data protection comparative study

First and foremost, the definition of a data breach varies from the first directive that was introduced by the EU and the current regulation. GDPR defines it as "breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data"[75] while in the US more sensitive information(such as social security number, while political views would not be considered sensitive information compared to the EU) that was acquired in an unauthorized way. The data breach definition varies between legal systems in EU and US, therefore already creating a problem for harmonization of two legal systems.

Additionally, due to the nature how the US laws are structured, the data subject definition is also rather vague, as for the most important document in US structure which is FTCA it is defined to be a "consumer" while in other it may range, depending on the scope of document itself (patients in case of Health Insurance Portability and Accountability Act or similarly depending on the scope in other cases). It is also important to note that definition of "consumer" may also vary from one state to another, which further complicates the matter[76].

It is important to note that one of the main differences between EU and US legislation is that in US there are no clear guidelines and clear rules that the company has to follow. As many of the similar principles and tools such as privacy by design are recommended to be used by the companies, it is not obligatory as in EU. The reason why it is not "obligatory" is that any failure to implement systems that observe such rules is not faulty unless it reaches the point where it can be considered "unfair or deceptive practice" by the company. It is, however highly probable that the companies should be following said guidelines as FTC has the authority to persecute unfair practices that have not yet been previously stipulated in any legal document or case[77]. In many ways it is so due to the common law system of the country which ensures more "case by case" approach towards all such violations. Additionally, the amount of cases that were actually resolved by the court are abysmal, due to most of the cases resulting in settlements.

While there is no overall system of principles as in EU law, to see how similar principles might work in the US, we can take a look at several cases representing certain principles. For example, there are similar requirements for the companies to provide lawful, clear and transparent ways of obtaining the data from the data subject.

In relation to this it is important to note that US does not have a strict set of reasons why the company can collect the data. It does not require explicit consent for data gathering as is the case in EU, however, it does require the companies to expressly stipulate that the consumer has the ability to opt-out from data gathering[78].

Other related rights, such as right to deletion or a right to correct the data may vary from state to state as not all of the issues, especially not the issues that can't be classified as unfair or

---

[75] REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), Official Journal of the European Union, 27 April 2016, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679

[76] Daniel J. Solove∗ & Woodrow Hartzog, THE FTC AND THE NEW COMMON LAW OF PRIVACY, COLUMBIA LAW REVIEW, 2014

[77] *Supra*

[78] *Supra*

deceptive, are regulated on the federal level. This is one more reason why it would be impossible for EU to cooperate with US companies without a certification methods provided in Privacy Shield and previously in Safe Harbor.

In regards to purpose limitation the FTC does not give specific guidelines on how the company should behave, however there were several cases where the fines were applied to the company for obtaining information that does not have any purpose except for it to be sold later, therefore some limitations still apply[7980].

Integrity and Confidentiality principles are not clearly stipulated as well, however, there are several cases that are stipulating what exactly is considered to be unacceptable under the US legislation which is:

- Allowing data to be attacked with tools such as Structured Query Language (SQL) injection attacks and Cross-Site Scripting (XSS) attacks[81]
- Lack of encryption (storage of data in plain text)/bad encryption[82]
- Failure to ensure relevant access restrictions (security flaw)[83]
- Failure to test the system to find vulnerabilities[84]
- Failure to monitor data recipients' activity (which also provides similar relation of data controllers monitoring activities of data processors as was discussed in GDPR section)[85]
- Lack of data minimization (which also provides a guideline that the companies should follow some of the guideline in respect to purpose limitation and storage limitations)[86]

In many ways those limitations are used from one of the specific documents described above such as HIPAA. In it, it is stipulated that organization is required to "*assess and control risk by implementing security programs, testing the company's data security, ensuring that outside data vendors secure data, training employees in data security, and implementing authentication3 and access- control procedure"*[87]

[79] UNITED STATES DISTRICT COURT FOR THE SOUTHERN DISTRICT OF OHIO EASTERN DIVISION, CASE NO. 2:10-cv-169, 2010, https://www.ftc.gov/sites/default/files/documents/cases/2010/03/100303creditcollectioncmpt.pdf

[80] UNITED STATES DISTRICT COURT DISTRICT OF ARIZONA – PHOENIX DIVISION, STIPULATED FINAL JUDGMENT AND ORDER FOR CIVIL PENALTIES, PERMANENT INJUNCTION, AND OTHER EQUITABLE RELIEF in Case 2:10-cv-00696-LOA, 2010, https://www.ftc.gov/sites/default/files/documents/cases/2010/03/100330directmarketingstip.pdf

[81]UNITED STATES DISTRICT COURT FOR THE SOUTHERN DISTRICT OF CALIFORNIA, United States v. ValueClick, Inc., No. CV08-01711MMM, 2008, https://www.ftc.gov/sites/default/files/documents/cases/2008/03/080317judgment.pdf

[82] Supra see 70

[83] Supra

[84] UNITED STATES OF AMERICA FEDERAL TRADE COMMISSION, DOCKET NO. C-4331, 2011, https://www.ftc.gov/sites/default/files/documents/cases/2011/08/110809acranetdo.pdf

[85] UNITED STATES OF AMERICA BEFORE THE FEDERAL TRADE COMMISSION, Complaint DOCKET NO. C-4400, 2013, https://www.ftc.gov/sites/default/files/documents/cases/2013/05/130503cbrcmpt.pdf

[86] Supra

[87] HIPAA Compliance Assistance , SUMMARY OF THE HIPAA PRIVACY RULE, 05/03/2020, https://www.hhs.gov/sites/default/files/privacysummary.pdf

Additionally, FTC also has established that use of unclear and vague language when informing customers of data collection also constitutes an unfair and deceptive practice[88].

Compared to Data Protection laws in US, GDRP also applies only to living persons, which means that deceased person ceases to be under the scope of the document. However, in EU there are some countries that establish rules for processing data of deceased such as rules in Bulgaria, Estonia and France and others. GDRP as well does not apply to some types of personal data, which is used to purely household activities or limited companies[89].

While EU does provide a much more comprehensive approach to personal data protection for European citizens, it is however allowing for similar derogations to be made as in the US, as with the aforementioned case C-291/12, where the ECJ has decided that in questions of national security the government are eligible to gather and use the private information of its citizens.

In a similar way as in EU, US data protection laws require the company to ensure substantive safeguards and procedures in regard to data acquisition, process, storing and erasure. In essence it involves a certain degree of data security. For data security issues only, the FTC has an overall authority for enforcement of the laws for everything not related to financial institutions.

There are several documents that require that the sufficient data security procedures would be established such as aforementioned The Gramm-Leach-Bliley (GLB) Act in case of financial institutions for depositary information. Under Health Insurance Portability and Accountability Act the companies must ensure that the "protected health information" (PHI) stays secure onto their servers. Children's Online Privacy Protection Act also provides a clause for data security, however, due to US having many different documents governing data protection, not all of them are providing a clause for data security which therefore might still lead to gaps appearing in the law system as not all the types pf personal data might be covered with this safeguard[90].

Another substantive safeguard is a purpose limitation to data usage again in a similar fashion to the one provided in EU. In similar way any personal information that comes into possession of the actor should be used retained and disclosed in a way that only the most necessary information is kept. The purpose to which the data is gathered and kept should be clear, limited and relevant to the circumstance[91].

FTCA however, while providing many ground rules in similar fashion as GDPR in EU, is still limited in its scope as its only application is for private companies that are collection the information of the individuals for sake of processing for commercial needs, however as was discussed before, FTA has jurisdiction over more than only this document. Additionally, while this document provides in many ways' similar requirements for the companies, there is no

---

[88] UNITED STATES DISTRICT COURT NORTHERN DISTRICT OF CALIFORNIA, CONSENT DECREE AND ORDER : FOR CIVIL PENALTIES, PERMANENT : INJUNCTION AND OTHER RELIE SAN FRANCISCO DIVISION, 2013, https://www.ftc.gov/sites/default/files/documents/cases/2013/02/130201pathincdo.pdf

[89] Gregg Latchams, A practical guide to the General Data Protection Regulation, Limited, 2017, https://www.gregglatchams.com/wp-content/uploads/A-Practical-Guide-to-the-GDPR-Gregg-Latchams-v1-Sept-2017-1.pdf

[90] *Supra* see 23

[91] *Supra* see 24

defined principles as in GDPR, which is especially true for issues of Accountability and Storage limitation[92].

However, in a way dissimilar to the EU, this Act provides that the unfair treatment towards data of the individual is not the one to which individual did not agree to, but rather the one that causes "substantial injury" to the individual where the individual was not able to avid this injury by their own means and where there is not outweighing factor (like criminal investigation) that required the company to disclose the information. [93] It is different from European approach in a way that unfair practices in EU is not about usage of data causing unnecessary injury, but also about purpose limitation, which means that the company should not be using the data for any other goals, other than the ones that were declared at the very beginning before the data was provided by the individual, therefore effectively providing the individual with a choice to whether he agrees to give his/her data for that purposes.

Additionally, Fair Credit Reporting Act also provides a right for the individuals to view and propose corrections to their information as well as subsequent obligation for credit institutions to disclose such information[94]. This right can be considered to be very similar to the one used in European Union, as companies are also obliged to disclose the data collected on the individual if requested.

To sum up, firstly, it is important to note that specific frameworks for data transfers between countries are required due to both the systems having very different approach towards data protection regulations. While as mentioned before US system for regulating data protection is distributed among many different documents, while EU has it centralized within one.

Secondly, the definition of the data breach is fairly different as mentioned before GDPR has a broader definition of it compared to the US, which in turn is not addressed in either Safe Harbor or Privacy Shield frameworks.

Thirdly, GDPR require companies to provide notification of substantive data breaches in limited amount of days, which would allow data protection authorities as well as in turn data subjects to be prepared for the consequences of such breach. There is no such requirement in either the framework or the US law, therefore this substantive safeguard is not yet provided by the framework and might require some amendments.

Fourthly, while US is centering its approach towards notifying the affected individuals, GDPR requires notification of the individuals in case of the data breach only in high-risk cases, which also lead to discriminatory approach towards different data subjects in case of the data breach, it is also unclear whether the data subjects from EU that have their data stored in US have the substantive safeguards provided by framework only, or by the US law itself as well[95].

Fifthly, it is important to note that US does not have unified principles of how the data protection should work in different kinds of institutions, and while the Trans-Atlantic framework in place provide some basic guideline on those, they are much more stipulated and

---

[92] *Supra* see 28
[93] Federal Trade Commission Act Incorporating U.S. SAFE WEB Act amendments, Federal Trade Commission ,2006
[94] *Supra*
[95] PWC, Data breach notification: 10 ways GDPR differs from the US privacy model, available on: https://www.pwc.com/us/en/services/consulting/cybersecurity/library/broader-perspectives/gdpr-differences.html, Accessed on 20 November, 2019

detailed in GDPR, which in turn leaves it to the question whether the framework will be relevant if it will again come under the scrutiny of ECJ.

Current EU-US data transfer framework (Privacy Shield) and its challenges

During the proceedings of the aforementioned Maximillian Schrems case, the European Commission already published a set of recommendations on how to improve existing framework of data transfers between the two countries with already clear idea that they need to change the question of access for public authorities for the data transferred to the US from the EU.

Privacy shield was created in 2015 followed by the Commission's decision 2016 (2016/4176/EC) rendering it a measure that would provide adequate protection to the transferred data between the countries. The Commission has re-considered the protection levels represented by the US data protection legislation and implemented new practices that would provide a sufficient level of legal protection to the transferred data. In the similar way to the Safe Harbor, the companies are self-certifying themselves as compliant with EU-US Privacy shield and the process and complaints are supervised by the US Department of Commerce and FTC. Privacy Shield was a document that was implemented pretty hastily due to the risk of US companies not being able to operate on the territory of the Union, due to there being no agreement to how the data flow should be managed[96].

In many ways Privacy Shield is similar to the previously adopted Safe Harbor framework. Its principles are as follows:

Choice Principle – in a similar way as with the Safe Harbor agreement, the individual's data must not be transferred to any third party, unless the individual is informed about such information transfer and has given his/her consent for that

Security Principle and Data Integrity and Purpose Limitation Principle – As this document was being created with GDPR Regulation in mind it has Principles that are called and work similarly to that, as those principle enshrine that any self-certified company must ensure that the data that comes into its hands is protected against "loss, misuse and unauthorized access, disclosure, alteration and destruction"[97]. Additionally, information that is gathered and transferred should be relevant and up-to-date as well as proportional according to the purpose to which it is going to be used, as the company should not gather more information that is necessarily required to perform the purpose to which data subject agrees. As was discussed previously the GDPR provides recognition of the principles "privacy by design" and "privacy by default" which requires data controllers implement appropriate technical and organizational measures to ensure data privacy. This is where this document does not provide any requirements on the US companies as it does not require US companies to implement any IT or other solutions, as well as other organizational measures to prevent data protection violations[98].

---

[96] Antonia Lantz, The EU-US Privacy Shield An insufficient level of data protection under EU Fundamental Rights Standards, Stockholm University, 2016

[97] Supra see 2

[98] European Commission, Automated decision-making on the basis of personal data that has been transferred from the EU to companies certified under the EU-U.S. Privacy Shield, 2018, https://ec.europa.eu/info/sites/info/files/independent_study_on_automated_decision-making.pdf

Notice Principle and Access Principle - in many ways Notice principle is really similar to the one in Safe Harbor framework, the data controller is still required to inform the data subject about gathering data on him/her and inform about the purpose to which this data will be used. However, in contrast to the aforementioned Safe Harbor agreement, data controller should also provide data subject with information on his or her rights to access and correct the information held on them. Those principles however, while in many ways similar to what was discussed in chapter about GDPR, still do not provide the same degree of protection as the company is not required to notify the data subject about the legal basis that is used for processing of the data as well as notify the person about data retention policy of the company when asking for the consent[99].

It is additionally worth noting that compared to GDPR neither US legal acts, nor EU-US Privacy Shield contain any clauses about retention of the personal data and its erasure. As was discussed previously, failure to have a relevant retention policy might result in data being rendered obsolete and hence inaccurate, which might be one of the big challenges towards maintaining a free flow of information between the countries and avoiding legal complaints by EU national authorities[100].

Recourse, Enforcement and Liability Principle – the self-certified organization is responsible for all the actions with the data in course of its processing and is responsible to maintain proper amount of protection to the data. It is also responsible for the actions that its agents are taking with the data (principle of data controller being responsible for actions of data processor). The participation in EU US Privacy Shield should be renewed annually in the same way as Safe Harbor agreement and in the similar way as with accountability principle in GDPR, the company must be able to present effective mechanisms to deal with data protection themselves. GDPR does require assignment of a specified data protection officer within public body or body with large scale data operations, which should be the contact person for all the data related questions to the data subject. However, there is no such requirement in EU US Privacy Shield[101].

Accountability for Onward Transfer Principle – This principle involves that any information that was given from the organization to a third party should be given only for a limited time and for purpose specified in the contract. The company should also make sure that any third party maintains the principles of EU-US Privacy Shield and should stop any unauthorized access to the data[102].

As was mentioned previously, EU-US Privacy Shield does require limitations of access from public bodies to EU data. It includes "letters from The Office of the Director of National Intelligence, the US Secretary of State and the Department of Justice"[103] that are meant as safeguards against the similar charges as were represented in the Maximillian Schrems case, which in turn might make this framework more stable despite many differences between the legal systems[104].

In general, as discussed above, US is taking a different approach compared to the EU in terms of data protection as it is using more of a sectorial approach to such regulation, which in turn makes those laws harder to follow and comply to and especially hard to harmonize as each

[99] *Supra* note 72
[100] *Supra* note 72
[101] Gentian Zyberi, Transatlantic data flow under the EU-U.S. Privacy Shield: An adequate protection of the fundamental right to protection of personal data?, University of Oslo, 2017
[102] *Ibid*
[103] *Supra* note 72
[104] *Ibid*

sphere requires a different approach. For EU-US Privacy Shield many sectors does not represent any difficulties as it is meant (for now at least) to only cover commercial companies, which in turn does not maintain a free data flow between the countries yet[105].

As was discussed in Maximillian Schrems case for the country to have an "adequate level" of data protection, legal systems of the countries in respect to data protection should be "essentially equivalent" to the ones in EU, which means that the country should require very specific reasons to access personal data of the data subjects and generalized data access should not be legal.

The EU-US framework is a complex document with several annexes and requirements being distributed among them with referrals from one to another which makes it harder for this document to be clarified and understood. The lack of clarity of the document was already discussed by the European Commission, which might be the reason why European Parliament pushed for abolishment of the framework[106].

One of the main principles that EU-US Privacy tries to convey is an increased transparency of actions of the data controllers in accordance to data received by them from data subjects from the Union. This document does a much better job in respect to that than the previously mentioned Safe Harbor framework[107].

The Commission has also required the companies to include information about the extent to which data controllers within US would have to allow public authorities to access the data, since it believes that many of the data subjects within the Union would not be able to gather such information on their own. It is however important to note that all the limitations that are imposed on US government in respect to processing personal data are contained within official letters in the annexes of the document, the legal power of which was not yet questioned, therefore it is quite unclear whether those commitments provide a sufficient legal certainty for European Union[108].

In general it is very hard to compare those two legal systems, as EU has a very big history of protection of private data, which is also indicated as constitutional right in many of the countries, which is not the case in the US, especially it is not regarded as a fundamental right and is therefore hardly applicable irrespective of citizenship[109].

To sum up, while EU-US Privacy Shield is really similar to Safe Harbor there are several differences as already mentioned above. Those are additional declarations in terms of government taking responsibility to not use the data of EU data subjects apart from several controlled exceptions. EU citizens have more options to file a claim for violation of their privacy rights such as US ombudsman, EU Data Protection Authorities or by suing the offending entity. The organizations will now be responsible to maintain the same protection as provided by the framework even in the event they don't renew their self-certification, but still have the data of EU data subjects and to report each year on the steps taken to promote data integrity and security, which was not present in Safe Harbor.

---

[105] *Ibid*
[106] *Ibid*
[107] *Ibid*
[108] *Ibid*
[109] Franziska Boehm, DIRECTORATE GENERAL FOR INTERNAL POLICIES, A comparison between US and EU data protection legislation for law enforcement purposes, 2015, https://www.europarl.europa.eu/RegData/etudes/STUD/2015/536459/IPOL_STU(2015)536459_EN.pdf

As of 16 July 2020, the current framework is being abolished because of inefficient redress mechanisms related to violation of lawfulness and transparency principles enshrined in GDPR by the US government. The main problem as seen by the European Commission is that US government has very vague definition of national interest relating to surveillance programs in place by US authorities. Under the current legal background, irrespective of framework in place, third parties (in this case government sanctioned surveillance) can access data of EU citizens without concern for data minimization, meaning that the US authorities take more data than is required by safeguarded principle of national interest. Additionally, as mentioned earlier, there is no effective way for EU citizens to redress the unlawful use of their data where national authorities are in question. This is also why the introduction of SCCs (Standard Contract Clauses) would not help as they would only bind the company that processes the data of the EU citizens[110].

While EU-US Privacy Shield was criticized on many occasions, that Department of Commerce together with FTC did go a long way on ensuring that companies comply with the EU-US Privacy Shield certifications as there was a system of obligatory and systematic checks of companies infrastructure and premises to see whether they are according to the framework[111].

[110] JUDGMENT OF THE COURT (Grand Chamber), 16 July 2020 In Case C-311/18, REQUEST for a preliminary ruling under Article 267 TFEU from the High Court (Ireland), made by decision of 4 May 2018, received at the Court on 9 May 2018, in the proceedings Data Protection Commissioner v Facebook Ireland Ltd, Maximillian Schrems, http://curia.europa.eu/juris/document/document.jsf?docid=228677&mode=req&pageIndex=1&dir=&occ=first&part=1&text=&doclang=EN&cid=14348306&fbclid=IwAR19sNjoVLWrZWGpTgLx8QaeMBzUnJ8HvySYfm9UbWBp14Rt2o32aJVQmPc

[111] REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL on the third annual review of the functioning of the EU-U.S. Privacy Shield, EUROPEAN COMMISSION, 2019, https://ec.europa.eu/info/sites/info/files/report_on_the_third_annual_review_of_the_eu_us_privacy_shield_2019.pdf

CONCLUSION

Firstly, it is important to note that throughout this thesis we saw how two of the data protection frameworks and systems collide with each other due to both of them having entirely different approach to structuring the data protection regulations. On the one side we can see current EU framework which harmonized data regulations among all the European countries with introduction of GDPR, allowing a quick and easier overview for the companies in respect to what to follow to be compliant from data protection perspective. On the other side we see US, where data protection is not given its own regulatory environment, instead it being a supplement to many other regulations to how the companies should behave in the market. It by itself create dissimilarities that are hard to manage between the countries, as US does not also have a single body that has jurisdiction over data protection questions, leaving EU-US Privacy Shield in vulnerable position when it comes to enforcing rights of the individuals. Additionally, US uses an absolutely different legal system(common law), which creates additional problems in analyzing how the court would interpret specific cases, especially considering, that in contrast to UK, US does not have a unified document (DPA in UK) that would be able to provide comprehensive information on the subject.

Secondly, as the paper provides, there was already an attempt to harmonize the two legal systems, however, the attempt was a failed one, mainly due to the concerns of data subjects with public authority access to their data in the US. While EU-US Privacy Shield does address this problem, as was mentioned previously, the legal strength of the commitment letters is questionable, and it is unclear whether there are actually any safeguard mechanisms instituted (at least not before world sees another leak of information from public institutions).

Thirdly, it is important to note that it is required by European Commission and hence by CJEU that the country has an “essentially equivalent” personal data protection system as it is within the Union. As was analyzed in the paper, in essence it is not so, as the laws of the US by themselves provide a much lesser extent of data protection and EU-US Privacy Shield does not cover all the provisions and requirements of the GDPR such as requirements to appoint a specific Data Protection Officer within the company to address the data protection concerns, working out retention and data erasure policies that are instated within the EU as well as it requires much less information to be provided to the data subject when acquiring his/her consent to data processing (such as legal basis on which the data will be processed, retention policy, etc.).

To sum up, it seems that in many way, due to hastily adoption of the EU-US Privacy Shield framework, it might not be sufficient to withstand scrutiny of the CJEU in case of assessment of framework’s validity in the question of it being “essentially equivalent” to the data protection regulations within the EU. The analysis of the two legal systems shows that by themselves, in absence of other regulations, the data protection regime in US is more lenient than in EU, therefore, if the document would be abolished, many companies would be at risk to cease any business activities that involve gathering personal data of EU subjects. There are however alternatives to the document, which might be introduced by many companies, such as Binding Corporate Rules, which would allow EU to allow the companies to operate within EU on case by case basis, providing a more flexible approach and allowing them to adopt stricter requirements faster on the company level.

However, due to some of the deficiencies of the US system which allows governmental oversight over private data in a very broad terms, it might be a better solution for the European Union to request American companies to store data on servers that are situated in European Union or in countries that are "essentially equivalent" to EU in data protection terms, to continue operation within European Union.

Therefore, to answer the first research question "Why the EU-US framework for data transfers was found to be irrelevant and not compliant with requirements of the EU law?" it would be important to note that during our work we have seen that while EU-US Privacy Shield had a good progress towards eliminating problematic areas between two countries, it still lacked in terms of many mechanisms, such as redress mechanism for EU citizens. We have also seen that with Data Privacy regulation advancing (with introduction of GDPR) some of the things mentioned in the document were not as valid anymore and since we can expect technology to go further in terms of automation and marketing research, we can also assume that new changes will have to be introduced and EU-US Privacy Shield was proving itself not to be as future-proof as such framework needs to be. Although the main reason for rendering the framework not valid was the risk of government access to the data with close to none redress mechanism towards US government in such case, author of this work would like to argue that it was by far not the only reason and that EU and US have a long way to go to create a stable and unified framework. Which is the reason why in conclusion of this research the author comes to understanding that as of current political background, there might not be a good way to harmonize two legal systems and the only good way for EU to act in current environment would be to require US companies to save their data on servers in countries within EU or countries with "essentially equivalent" data protection frameworks (such as Canada).

This conclusion have been introduced on the assumption that this is unlikely that the US will change their laws regarding surveillance and information gathering by the government, as well as the fact that the country lacks a unified system of data protection, where all the relevant safeguards that are enshrined in GDPR would be introduced. Additionally, while you could lawfully challenge the company for violating Privacy Shield, there are several problems for EU citizens, such as any arbitration will be taking place in the US and your only redress is cease of data violation as any monetary damages can be claimed only under US laws[112].

[112] European Commision, GUIDE TO THE EU-U.S. PRIVACY SHIELD, 2016, https://ec.europa.eu/info/sites/info/files/2016-08-01-ps-citizens-guide_en.pd_.pdf

BIBLIOGRAPHY

1. Antonia Lantz, The EU-US Privacy Shield An insufficient level of data protection under EU Fundamental Rights Standards, Stockholm University, 2016

2. Challenges For The Business When Complying With The General Data Protection Regulation, Vyara Gocheva, June 2017

3. Christine S. Wilson, A Defining Moment for Privacy: The Time is Ripe for Federal Privacy Legislation, US Federal Trade Commission, 2020

4. Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce, European Commission, 2000

5. Communication From The Commission To The European Parliament And The Council, on the Transfer of Personal Data from the EU to the United States of America under Directive 95/46/EC following the Judgment by the Court of Justice in Case C-362/14, European Commission

6. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Strasbourg, , ETS 108, 1981.

7. Daniel J. Solove∗ & Woodrow Hartzog, The Ftc And The New Common Law Of Privacy, Columbia Law Review, 2014

8. Data Protection Law in the USA, Robert Hasty, Dr. Trevor W. Nagel and Mariam Subjally White and Case, August 2013

9. Data Protection Law: An Overview, Congressional Research Service, March 25, 2019,

10. Data protection regulations and international data flows: Implications for trade and development, United Nations, 2016

11. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal L 281 , 23/11/1995 P. 0031 – 0050, October 1995

12. Federal Trade Commission Act Incorporating U.S. SAFE WEB Act amendments, Federal Trade Commission ,2006

13. Franziska Boehm, DIRECTORATE GENERAL FOR INTERNAL POLICIES, A comparison between US and EU data protection legislation for law enforcement purposes, 2015

14. Gentian Zyberi, Transatlantic data flow under the EU-U.S. Privacy Shield: An adequate protection of the fundamental right to protection of personal data?, University of Oslo, 2017

15. Gert Vermeulen, Eva Lievens, Data Protection and Privacy under Pressure, Maklu, 2017

16. Gregg Latchams, A practical guide to the General Data Protection Regulation, Limited, 2017

17. Harpo Vogelsang, An analysis of the EU data protection policy and the significance of the Maximillian Schrems case, University of Twente, July 2019

18. HIPAA Compliance Assistance , SUMMARY OF THE HIPAA PRIVACY RULE, 05/03/2020

19. Information Commissioner Office, Guide to the General Data Protection Regulation (GDPR) August 2018

20. Judgment Of The Court (Grand Chamber), 6 October 2015 (*) n Case C-362/14, REQUEST for a preliminary ruling under Article 267 TFEU from the High Court (Ireland), made by decision of 17 July 2014, received at the Court on 25 July 2014, in the proceedings Maximillian Schrems V Data Protection Commissioner, joined party: Digital Rights Ireland Ltd

21. Judgment Of The Court In Case C-131/12, Request for a preliminary ruling under Article 267 TFEU from the Audiencia Nacional (Spain), made by decision of 27 February 2012, received at the Court on 9 March 2012, in the proceedingsGoogle Spain SL, Google Inc. V Agencia Española de Protección de Datos (AEPD),Mario Costeja González, 13 May 2014

22. JUDGMENT OF THE COURT, In Case C-73/07, REFERENCE for a preliminary ruling under Article 234 EC from the Korkein hallinto-oikeus (Finland), made by decision of 8 February 2007, received at the Court on 12 February 2007, in the proceedings Tietosuojavaltuutettu v Satakunnan Markkinapörssi Oy,Satamedia Oy, 16 December 2008

23. Judgment Of The Court, References to the Court under Article 234 EC by the Verfassungsgerichtshof (C-465/00) and the Oberster Gerichtshof (C-138/01 and C-139/01) (Austria) for preliminary rulings in the proceedings pending before those courts between Rechnungshof (C-465/00), 20 May 2003

24. Julie Brill, Two-Way Street: U.S.-EU Parallels Under the General Data Protection Regulation, Ghostery/Hogan Lovells Data Privacy Day, 2016

25. Leena Salolatva, Privacy Shield Redress Mechanisms Assessment in the Light of the Schrems Case, University Of Helsinki

26. Privacy by Design The 7 Foundational Principles Implementation and Mapping of Fair Information Practicesб Ann Cavoukian, Ph.D, 2011

27. PWC, Data breach notification: 10 ways GDPR differs from the US privacy model, https://www.pwc.com/us/en/services/consulting/cybersecurity/library/broader-perspectives/gdpr-differences.html

28. REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), Official Journal of the European Union, 27 April 2016

29. REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL on the third annual review of the functioning of the EU-U.S. Privacy Shield, EUROPEAN COMMISSION, 2019

30. United States Constitution Fourth Amendment, US Congress September 25, 1789. Ratified December 15, 1791

31. United States District Court District Of Arizona – Phoenix Division, Stipulated Final Judgment And Order For Civil Penalties, Permanent Injunction, And Other Equitable Relief in Case 2:10-cv-00696-LOA, 2010

32. UNITED STATES DISTRICT COURT FOR THE SOUTHERN DISTRICT OF CALIFORNIA, United States v. ValueClick, Inc., No. CV08-01711MMM, 2008

33. United States District Court For The Southern District Of Ohio Eastern Division, Case No. 2:10-cv-169, 2010

34. United States District Court Northern District Of California, Consent Decree And Order : For Civil Penalties, Permanent : Injunction And Other Relief San Francisco Division, 2013

35. United States Of America Before The Federal Trade Commission, Complaint DOCKET NO. C-4400, 2013

36. United States Of America Federal Trade Commission, Docket No. C-4331, 2011

37. European Commision, GUIDE TO THE EU-U.S. PRIVACY SHIELD, 2016, https://ec.europa.eu/info/sites/info/files/2016-08-01-ps-citizens-guide_en.pd_.pdf

38. Pasi Reini, GDPR implementation, School of Technology, Communication and Transport ,2019

39. Tossapon Tassanakunlapan, Protection of personal data in cyberspace:the EU-US E-market regime, University Of Barcelona, 2017

40. European Commission, Automated decision-making on the basis of personal data that has been transferred from the EU to companies certified under the EU-U.S. Privacy Shield, 2018