Personal Data Protection: Norms concerning transfers of data from the EU to the US

Naima Mammadova

LLM. Final Thesis

SUPERVISOR: Professor Tommaso Soave

Central European University - Private University

17 June 2022

TABLE OF CONTENTS

ABSTRACT

The aim of this thesis is to ascertain the possibility, promises, and pitfalls of establishing a new legal framework for cross-border data transfer from the EU to the US. In the modern world, international data transfers between countries have significant importance for crime investigation, companies, and organizations which operate their business at the international level and use cloud technology. This thesis focuses on the investigation of legal issues and collisions related to the cross-border data transfer from the EU to the US, which is one of the topical problems in the personal data protection field. When personal data is transferred from one state to another one conflicts occur because of different jurisdictions and data protection regimes.[I] One such example of this kind of disagreement is the incompatibility between the EU General Data Protection Regulation (GDPR) and the Clarifying Lawful Overseas Use of Data (CLOUD) Act[II]. Therefore, this research aims to identify the collision between the CLOUD Act and the GDPR on data transfer from the EU to the US, the limits of their respective authority, and the scope of their jurisdictions[III]. The central problem in this thesis is to find a solution to transfer personal data from the EU to the US. International executive agreements may be offered as a solution, but the problem is, that these kinds of agreements were invalidated by CJEU two times. After the invalidation of Safe Harbor and Privacy Shield, there is no sufficient instrument to apply in cross-border data protection. Thus, this thesis also analyzes legal issues raised in Schrems I and Schrems II and the situation in the US after invalidatio

[I] Reed Smith, Potential conflict and harmony between GDPR and the Cloud Act,2018

[II] https://www.lexology.com/library/detail.aspx?g=e39c3d27-e8f5-4a55-b343-dff88341437f

[III] Ibid.

Introduction

Background

In the big data era, one of the most important problems in personal data protection law is cross-border data transfers, in particular from the European Union to the United States. Significant number of data is transferred from the EU to the US for business, research and crime investigation purposes and that data includes personal data too.[4] The collection and transfer of personal data by non-EU private and governmental organizations lead to increase in concerns about safety and privacy, especially in light of the disparity of approaches to personal data protection regimes and security breaches. Personal data transfer is a necessary concept for both governmental and private organizations, therefore there was a need to establish adequate safeguards, requirements for data transfers and guaranties. Enacting new regulations also brings some problems such as conflicts of laws, because every state has their own jurisdiction and law, clash among their subject scope, territorial scope, and safeguards. Therefore, transatlantic data transfer is very complicated issue because of collisions unless there is not an international agreement or regulation to determine adequate ways of personal data transfer. It is also possible that there can be a tension between international agreement and national law.

This thesis explores transatlantic conflicts of laws in respect of data protection by focusing on two regulations enacted in 2018: the General Data Protection Regulation (GDPR) adopted by the EU and the Clarifying Lawful Overseas Use of Data Act (Cloud Act) enacted by the US. Because both regulations have an extra-territorial scope, sometimes they can concurrently

[4] Congressional Research Service, 'Digital Trade and U.S. Trade Policy' (2017), 20 <https://epic.org/crs/R44565.pdf> accessed on 26 March 2021.

apply to US-EU data transfers, thus giving rise to potential normative conflicts and creating uncertainties for users, companies, and public authorities alike.

At first glance, current conflict seems exist the US companies and their subsidiaries in the EU because of exterritoriality of the US Law Enforcement Authorities' orders and the GDPR. According to territorial scope of the GDPR, location of the personal data and the location of headquarter of the company does not matter.[5] Therefore, even a data provider or processor in the US territory should comply with the provisions of the GDPR during the personal data transfer to third countries, however that companies are subject to the US law at the same time. New international agreement can be suggested as a solution to solve collision between two jurisdictions. Because the CLOUD Act give opportunity US to enter international agreements and it is stated in Art.48 GDPR that disclosing personal data can be recognized if it is based on international agreement. However, other problem is about that kind of agreement. There were agreement between the US and the EU such as Safe Harbor and Privacy Shield, but both of them invalidated by CJEU. Therefore, that thesis explain if new agreement is possible and requirements for this agreement. Besides international agreements, this thesis present other possible solutions such as rules and principles of international law, standard contractual clauses.

Research questions

The aim of this thesis to analyze collision between the GDPR and the CLOUD Act and to suggest solution to reconcile incompatibilities which can regulate obligation of data processor to disclose personal data and determine adequate way to transfer personal data from the EU to the US. Therefore, main research question is what is the possible way to solve collision and to

[5] Andreas Gruber, "Transatlantic challenges in access to electronic evidence: Conflicting obligations under the Stored Communications Act and the General Data Protection Regulation" 2019

reconcile obligation of data processor or provider to disclose user data under the CLOUD Act with the provisions for cross-border personal data transfer to third countries in the GDPR? There are sub-questions to help to give detailed answer to the main research question:

- what is the conflict between two regulation, where does it originate, and which are the incompatible provisions?
- How does the GDPR limits the US LEA to transfer personal data to third countries?[6]
- What can be offered as a solution to solve conflict and can new agreement such as the US-UK Biliteral Data Sharing Agreement be solution?

Methodology

The thesis analyses collection of existing material such as case law, statutes, opinions of regulatory bodies, Therefore, thesis is based on legal doctrinal research. After analysis of that material, systematic approach will be established in order to apply certain research questions. Furthermore, this thesis aims to find a solution for personal data transfer, so problem-based approach is observed in this research.

Roadmap.

The thesis comprises an introduction part, two chapters, and a conclusion. The first chapter focus on collision between the GDPR and CLOUD Act, legal background of CLOUD Act, the origins of conflict, and incompatible provisions. The second chapter analyses possible solutions for this tension such as biliteral agreements, international agreements, rules and principles of international law to solve conflicts of law. New Trans-Atlantic Data Privacy framework and the US-UK data sharing agreement are analysed in this chapter to offer the solution. Conclusion contributes findings on the reasons of collision about possible solutions

[6] https://blazecut.com/privacy-policy

Chapter 1- Collision between the CLOUD Act and the GDPR

Introduction

This chapter analyzes norms of cross-border data transfer under the GDPR and the CLOUD Act. The purpose of this analysis is identifying conflicts and their reasons, at the same time offering methods of reconciling of incompatibilities in next chapters. The first subchapter introduces the CLOUD Act, its history and policy rationales, with a particular focus on its extra-territorial dimensions. The second subchapter turns to the GDPR, which contains several provisions extending the coverage of data protection disciplines beyond the borders of the EU. The third subchapter focuses more directly on the conflicts of laws that arise from the concurrent application of the CLOUD Act and the GDPR to data transfers between the EU and the US.[7]

1.1. *Legislative background and policy rationales of the CLOUD Act*

The roots of the CLOUD Act can be traced back to the regulation of the powers US law enforcement authorities vis-à-vis the personal privacy of citizens. This regulation has a long history. The oldest law in the US which protects right to privacy is the Fourth Amendment. During the years, legislation of the US was upgraded because of the improvements in technology and data protection and the CLOUD Act was enacted as a result of improvements. Fourth Amendment was not able to provide adequate protection, because it was to general. The Fourth Amendment to the US Constitution states that "the right of the people to be secure in

[7] Basil Varughese, Cross- border data transfer in the context of the GDPR and CLOUD Act, Tilburg University (2019-2020)

their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." [8] If it is briefly said, fourth amendment is a protection for people's right to be safe in their papers, persons, houses against illegal and unreasonable seizures. It is sated in the Katz v. United State ruling, the amendment protect people from unreasonable seizures, so this amendment is applicable if the person's privacy expectation is reasonable.[9] Despite this, third-party doctrine changes the situation. In United States v. Miller case, court ruled that if data subjects submit his data voluntarily then data subject has not legitimated privacy expectation and Fourth Amendment can not protect that person.[10] Court stated in that case that bank owned the bank records to use them its business and transferred that data for crime investigation.[11] It means that when data subjects disclose their data to company to use their service and the company transfer data to third parties, then Fourth Amendment can not cover this situation because of lack of reasonable expectation.[12] Following this, Carpenter v. United State case also presented that Fourth Amendment is not enough to protects electronic communication if the communication and information is transferred to third party necessary like crime investigation purposes.[13] Therefore, the protection of Fourth Amendment was not sufficient to apply it to

[8] Fourth Amendment

[9] 389 U.S. 347 (1967).

[10] United States v. Miller

[11] 425 U.S. 435 (1976)
8 Secil Bilgic, Something Old, Something New, and Something Moot: The Privacy Crisis under the CLOUD Act, 32 HARV. J. L. & TECH. 321 (2018).

[12] Ibid

data which stored online. The fourth amendment determines right to be secure therefore, direct application of that amendment to reasonable expectation of privacy about online or digital issues was difficult. This difficulty is understandable because the US constitution was ratified in 1787 when there was not internet, technology or need to transfer data which stored digitally. But personal data transfer is one of the important problems of modern life and there is a need for developed legislation for developed technology.

In 1986 Electronic Communications Privacy Act (ECPA) was created to deal with recent problems in electronic communication field and enactment of the ECPA was a response to ruling of Smith v. Maryland.[14] In that case, the Court ruled that application of the Fourth Amendment to data in electronic communication is not possible because required disclosure of the data to third party and inexistence of the reasonable expectation. [15] After this ruling, Congress adopted the ECPA to upgrade standards of the federal privacy protection about recent communication technology. [16] ECPA applies if electronic communication is reviewed or intercepted by third party, and if there is not legitimate interest, ECPA makes these kinds

[14] Smith, 442 U.S. at 746

[15] *See* Smith, 442 U.S. at 746

[16] *n re* Application of U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to Gov't, 620 F.3d 304, 313 (3d Cir. 2010) (citing S. Rep. No. 99-541, at 1 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3555) (discussing the legislative history of the ECPA, in which it is clear that Congress enacted the ECPA "to protect against the unauthorized interception of electronic communications .... [and] update and clarify Federal privacy protections and standards in light of dramatic changes in new computer and telecommunications technologies.")

of actions crime. Definition of electronic communication in ECPA is transfer of images, signals, data, writing, photoelectronic system affecting foreign commerce.

The ECPA involved three titles: first one is Wiretap Act and prohibits to intercept wire, electronic or oral communication intentionally.[17] Second title is called Stored Communication Act and it aims to protect stored communication data and it is the source of the collision between jurisdictions. [18] Finally, Title III is Pen Register Act which sets an obligation for government to get court order for disclosure of data which pen register, trap and trace devices involve. [19]

Usually, crime is considered as interception of electronic communication in the absence of exemption. ECPA determine difference between communication obtained in transmission and communication reached final destination. [20] ECPA was enacted to give clarity during monitoring electronic communication, but law is criticized for lacks in clarity.[21] Source of the criticism is the difference of standards of evidence and requirements to get records by government between Title I and Title II. It led do disagreement among courts. Most of the courts consider that under Title I interception of e-mail must be at the same time with the communication transmission, but courts disagreed that if the e-mail in transient electronic storage qualifies under Title I prior delivery.[22] Privacy advocates claims that ECPA can not

[17] Electronic Communications Privacy Act of 1986 (ECPA), 18 U.S.C. §§ 2510-22 (2018)

[18] Lisa V. Zivkovic, 'The Alignment between the Electronic Communications Privacy Act and the European Union's General Data Protection Regulation: Reform Needs to Protect the Data Subject' (2018) 28 Transnat'l L & Contemp Probs 189

[19] 18 U.S.C. §§ 3121-27 (2009)

[20] https://www.lexisnexis.com/legalnewsroom/lexis-hub/b/legal-technology-and-social-media/posts/should-the-electronic-communications-privacy-act-ecpa-be-reformed-is-it-still-adequate-protection

[21] Ibid

[22] Ibid

protects e-mail if it is in temporary storage. One of the drawbacks of the ECPA was that it is easy for governments to ask from service providers to disclose personal data which stored on servers of service providers.[23] All government enforcement agencies need to do is just written statement which certifies relevance of information for investigation and there is not need for judicial review to get this statement.

The purpose of the Stored Communication Act (SCA), which is Title II of ECPA, is to provide digital communication with protection by depriving unreasonable government influence.[24] The privacy protection of the SCA was codified in 18. U.S.C. §§ 2702 and 2703.[25] The conditions which determine when service provider can disclose data are described in the section 2702.[26] Section 2703 involves the procedures which government should follow to request from service providers to disclose data. [27] The SCA govern Electronic Communication Service (ECS)

[23] Schwartz, Ari; Mulligan, Deirdre; Mondal, Indrani (2004–2005). "Storing Our Lives Online: Expanded Email Storage Raises Complex Policy Issues". *I/S: A Journal of Law and Policy for the Information Society*. **1**: 597.

[24] Orin S. Kerr, *A User's Guide to the Stored CommunicationsAct, and a Legislator's Guide to Amending It*, 72 GEO. **WASH.** L. REv. 1208, 1212 (2004).

[25] ordan A. Klumpp, International Impact of the Clarifying Lawful Overseas Use of Data (CLOUD) Act and Suggested Amendments to Improve Foreign Relations, 48 GA. J. INT'l & COMP. L. 613 (2020).

[26] 18. U.S.C. § 2702

[27] 18. U.S.C. § 2703

provides and Remote Computing Service (RCS) providers.[28] Referring to 18. U.S.C. § 2510, an electronic communication service is stated as 'any service provides to users the opportunity to send and receive wire or electronic communications', which includes not only Internet access and e-mail services, but also text messaging services and social media websites.[29]

Although the SCA provides with the protection measures and the procedure rules for government, it also involves some accessibility related problems. One of the features of SCA is that U.S companies are not allowed to turn over data to Legal Enforcement Agencies in foreign countries.[30] Due to this rule, when foreign governments needs data to investigate a crime in their territory and they have to request disclosure of data from the US. [31] The SCA also limits providers to transfer data to the US government. This situation is a significant hinderance for crime investigation and the US received significant number of requests to disclose data to other countries.[32]

---

[28] Secil Bilgic, Something Old, Something New, and Something Moot: The privacy Crisis Under the Cloud Act, 32 Harvard Journal of Law and Technology 1 (2018)

[29] Michael E. Lackey, Oral D. Pottinger, 'Stored Communications Act: Practical Considerations' (*LexisNexis,* 22 June 2018) < https://www.lexisnexis.com/lexis-practice-advisor/the-journal/b/lpa/archive/2018/06/22/stored-communications-act-practical-considerations.aspx> accessed 20 May 2019

[30] U.S.C.A. § 2702 (1986); Chris Cook, *Cross-BorderDataAccess and Active Cyber Defense: Assessing Legislative Optionsfor A New Internationa lCyber security Rulebook,* **STAN.** L. **&** POL'Y REv. 205, 222 (2018).

[31] Cook, *supra*note 22, at 223, 225

[32] Ibid

Another unclear point is about obligation of the US companies to disclose data which is stored another country to the US government. It is unclear that if the SCA has exterritorial effect regarding to US based companies in other countries.[33] Microsoft Corp v. United States is a good example of this problem.[34] Legal issue in this case was exterritoriality of warrant which was issued u der SCA and its applicability to data which was stored in foreign location[35]. Second Circuit decided that this kind of warrant is not enforceable in foreign countries.[36]

Because of these reasons some critics consider the SCA is hinderance for crime investigation because it can not provide international data flow between the US and other countries because in modern world investigation requires digital evidences and some of these evidences can be stored in foreign states.[37] The SCA was enacted thirty six years before and great part of the personal data was located domestically so there was not a notable need to transfer data.

The Mutual Legal Assistance Treaties are instrument under the SCA for cooperation in international crime investigation.[38] MLAT applies to data sharing and the domestic law of the

[33] Ibid at 223.

[34] Hogan Lovells 2019 Demiystifying the U.S. CLOUD Act Assessing the law's compitability with international normas and the GDPR

[35] Jennifer Daskal, Microsoft Ireland, the CLOUD Act, and international lawmaking 2.0, 71 Stan. L. REV. ONLINE 9 (2018-2019)

[36] MICROSOFT

[37] Ibid 222-23.

[38] Jordan A. Klumpp, International Impact of the Clarifying Lawful Overseas Use of Data (CLOUD) Act and Suggested Amendments to Improve Foreign Relations, 48 GA. J. INT'l & COMP. L. 613 (2020).

country where the data is stored.[39] For example if Austria request for data from the US under MLAT, then the US will have a responsibility for investigation and this investigation should comply with constitutional requirements of US.[40]

MLAT has some disadvantages such as frustration and time consuming. Foreign country should request from Department of Justice Office of International Affairs to disclose the personal data.[41] This request should be approved by the US judge, and it takes a lot of time.

Another challenge about the SCA is about limited application scope of the warrants. In the United States v. Microsoft Corp ruling, court stated that it is not possible to request to disclose the data which is stored outside of the US. Therefore, the CLOUD Act was enacted as a response to ruling.

The US enacted the new law – CLOUD Act to solve the legal issue which occurred in Microsoft Ireland case in 2018. The purpose of establishment of the CLOUD Act was to provide SCA warrants with exterritorial power. In that case SCA warrant was obtained for crime investigation for emails of the US citizen which was stored on remote servers of Microsoft in Ireland, but Microsoft refused to disclose and transfer personal data.[42] United States claimed that Microsoft had a control of the personal data and should provide data because of warrant. But Microsoft responded that warrant is applicable only for data which is

[39] Ibid

[40] Ibid

[41] Tiffany Lin & Mailyn Fidler, *Cross-BorderDataAccess Reform: A Primeron the Proposed**U.S.-U.K.** Agreement*, BERKMAN KLEIN CTR. FOR INTERNET **&** SOC'Y AT HARV.U. (2017)

[42] Microsoft Corp. v. United States, 829 F.3d 197, 202 (2d Cir. 2016), available at

stored within the US. It cannot have a power on personal data which stored in third countries. The Court of Appeals for the Second Circuit overturned decision and said that provisions of Standard Communication Act (SCA) do not have exterritorial application, therefore, warrant can be applied to data which is stored in the US. Because of it, Microsoft gets access to personal data in accordance with SCA warrant, then Microsoft acts as representative of government and it leads to violation of privacy.[43]After establishment of the CLOUD Act, SCA warrants got exterritorial power. The Cloud Act is codified at 18 U.S. §2713 and states: A provider of electronic communication service or remote computing service shall comply with the obligations of this chapter to preserve, backup, or disclose the contents of a wire or electronic communication and any record or other information pertaining to a customer or subscriber within such provider's possession, custody, or control, regardless of whether such communication, record, or other information is located within or outside of the United States.[44] It means that SCA warrants have exterritorial power and data processor are obliged to disclose and transfer data which under possession, custody or control and location of data does not matter.[45] It is seen from this provision that the Cloud Act has exterritoriality because it is mentioned that US companies should provide a data when warrant requests regardless the location of stored data. It means that if LEA request data with warrant and if data stored in the EU member state, data processor or provider is obliged to transfer the personal data because that data is under control of the company. The Act does not gives the definition of possession,

[43] Microsoft Corp. v. United States, 829 F.3d 197, 202 (2d Cir. 2016), available at <https://www.scotusblog.com/case-files/cases/united-states-v-microsoft-corp/>

[44] 18 U.S. §2713

[45] Ibid

custody or control, but it means having ownership and actual possession like legal right to receive the personal data.[46] The US established new method of international lawmaking via domestic law and regulation.[47] It can be define right of the parent company to get the data.[48] Because it has exterritorial power like international agreements, but the CLOUD Act is just part of domestic law, it is not international agreement.

One of the interesting points about the different decisions of courts in other cases after Microsoft Ireland case. Judges used the provisions of Stored communication Act, therefore it can be said that Microsoft Ireland case is an expectation, it is not a rule about cross-border data transfer. Just after a week second Circuit rejected ruling in the case of Microsoft Ireland.[49] Google Pennsylvania case is one of these kinds of cases. Federal judge rejected claim of Google to quash a warrant however data was still under the SCA. [50] Judge rejected Microsoft ruling and stated that data transfer from outside of United States to California was not covered by

[46] In re Bankers Trust, 61 F.3d 465,469 (6th Cir. 1995)

[47] Jennifer Daskal, "Microsoft Ireland, the CLOUD Act and International Lawmaking 2.0," Stanford Law Review Online 71 (2018-2018):9-16

[48] Tess Blair, Tara S. Lawler, 'Possession, Custody or Control: A Perennial Question Gets More Complicated' *The Legal Intelligencer* (Philadelphia, 5 February 2018)

[49] Google Pennsylvania

[50] Re Search Warrant No. 16-960-M-01 to Google, 232 F.Supp.3d 708, 709 (E.D. Pa. 2017)

Fourth Amendment seizure, because his data transfer is not an obstacle for data subject's possession right.[51]

Another case is Yahoo Wiscosin which rejected Microsoft ruling. Judge stated that custody or control of information must be accepted as domestic request regarding the control not location test and this test makes location criteria irrelevant.[52] If jurisdiction of court civers service provider then courts has a right to order to disclose the personal data referring to SCA warrant.[53] The CLOUD Act gives opportunity to companies to challenge the SCA warrant.[54] The company or provider can challenge the warrant if data subject is not the US citizen or is not living in the US[55]; if data transfer is unlawful under jurisdiction of qualifying government and data providers would violate the law.[56]

Besides exterritoriality, CLOUD Act has another important function. Another important function of CLOUD Act is giving executive branch of government to enter agreement with other states which is qualifying foreign governments about data sharing. Because of exterritoriality of the CLOUD Act, it is possible that provisions of the CLOUD Act collide

---

[51] Hogan Lovells 'Demystifying the U.S. CLOUD Act: Assessing the law's compatibility with international norms and the GDPR, 15th January 2019, available at

[52] Re: Information associated with one Yahoo email address that is stored at premises controlled by Yahoo, Case No. 17-M-1234 (E.D. Wis. 21 Feb. 2017)

[53] Ibid

[54] 18 U.S.C.A. § 2703(h)(2) (2019)

[55] 18 U.S.C.A. § 2703(h)(2)(A)-(B) (2019)

[56] 18 U.S.C.A. § 2703(h)(2)(I)-(ii) (2019)

with international law and domestic law of other states.[57] Therefore, the CLOUD Act also create an opportunity such as to enter biliteral agreements to eliminate this kind of collisions between different jurisdictions. It is too advantageous because of time efficiency and less formality. Governments which enter agreement do not have an obligation to follow each another privacy protection law to get the personal data.[58] Terms and conditions of these agreement will be explained in second chapter regarding to US-UK data sharing agreement.

1.3.1. Cross-border data transfers under the GDPR

The GDPR sets out comprehensive requirements for data controllers processing the data of EU data subjects.[59] Those requirements seek to protect the privacy of EU users against unwarranted intrusions. One of the difference between the GDPR and The 95 Directive is GDPR has more clarified scope of application.[60] There are two criteria which allow to determine territorial scope of the GDPR: Establishment criteria and targeting criteria. Exterritorial power of GDPR is explained in Article 3(1). This article presents that GDPR applies to the companies which established in the EU, regardless of whether the processing

---

[57] Jean Galbraith, 'Contemporary practice of the United States relating to international law' (2018) 112 American Journal of International Law 490

[58] Camille Fischer, *The CLOUD Act: A Dangerous Expansion of Police Snooping on Cross-Border Data,* ELEC. FRONTIER FOUND. (Feb. 8, 2018),

[59] Ibid.

[60] *GDPRKey Changes,supra*note 139.

takes place in the Union or not.[61] Same as with CLO CLOUD Act, location where data is processed, it does not matter to determine territorial scope of the GDPR . It means, if headquarter of company in the US but has a branch in Hungary, then that branch is considered as establishment in EU, that's why territorial scope of GDPR includes that branch. At the same, time the GDPR applies to companies established outside of the EU but offer service to the EU citizens or monitoring their behavior.[62] Aim of this article to provide individuals with data protection in case establishment is not in EU territory. For ex: if the US company which locates in Delaware, collects personal data of EU resident, then that company is target to GDPR too despite its location.

One of the important issue to determine application scope is connection between GDPR and criminal investigation. The CLOUD Act is a regulation which offers opportunity to make crime investigation easier, personal data transfer is about crime investigation. However Article 2 and recital 19 GDPR states that GDPR is not applicable to protection of people with regards to investigation, detection of criminal offences execution criminal penalties.[63] Directive (EU) 2016/680 of the European Parliament and of the Council regulates personal data transfer related to crime investigation.[64] Article 36 of that Directive claims that there are two condition to

[61] *Article 3 EU General Data Protection Regulation (EU-GDPR). Privacy ...,*

[62] art. 3(2). GDPR

[63] Recital 19

[64] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of

transfer personal data to third countries: first, the European Commission issued an adequacy decision; second, there is a legally binding instrument.[65]But the problem is there is not this kind of decision in the US especially for crime investigation. However, the US has an instrument such as the CLOUD Act. But it is not an international agreement despite having exterritorial power. As there is not an agreement transatlantic personal data transfer can be a subject to the GDPR, and the GDPR is most improved and extensive regulation in the EU any kind of personal data transfer is regulated by the GDPR. Assessments of European Data Protection Board about computability between the GDPR and the CLOUD Act can confirm that idea.[66] It is highlighted in that opinion that the EU can transfer personal data if SCA warrants are based on the international agreement which is suitable requirement in chapter V of GDPR.[67] Therefore, however it is stated that the GDPR is not applicable data related issues in crime investigation, anyway it is connected and the agreement should follow the requirements of the chapter V. In addition, when the US LEA demands US company established in US to disclose personal data for crime investigation then that company requests subsidiary in the EU. Practically there is not a difference between transferring data for crime investigation or other purposes such as research, statistical purposes. It is possible that there

criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA [2016] OJ L119/89.

[65] Basil Varughese, Cross-border data transfer in the context of the GDPR and CLOUD Act 2019-2020

[66] European Parliament resolution of 5 July 2018 on the adequacy of the protection afforded by the EU-US Privacy Shield

[67] Article 48 GDPR

are some differences such as freely given consent but in general they are not completely different from each another. Therefore, practically it is possible to apply the GDPR to data transfer for crime investigation purpose. It is also possible that the US LEA can demand to disclose personal data which has been transferred before issuing that warrant.

1.3.2. Tension between the provisions of the GDPR and the CLOUD Act.

The conflict started even before the CLOUD Act and The GDPR.[68] The difference is the different attitude and different law system of the US and the EU. One of the different aspect of the US law is having sectoral data protection regimes. Comprehensive and single regulation is not available in the US law. Therefore, the US law protects personal data and data subjects in specific areas. Following this, as a fundamental right , right to privacy can get constitutional protection against the US. But in the EU law, constitutional protection of right to privacy extends to private sectors.[69] The US law does not give the detailed definition of privacy because keeping balance between individual rights and state interest is complicated under the US law. The US law has several legal acts which supports surveillance. There is a difference between the US law and the EU law regarding to surveillance.[70]The US law considers that surveillance

[68] Basil Varughese, Cross- border data transfer in the context of the GDPR and CLOUD Act, Tilburg University (2019-2020)

[69] Siyuen Chen, Cross-border Data Transfer After *Schrems II*: The Globalization of EU Standards of Data Protection Through Adequacy Decisions or Trade Agreements? 2021.

[70] Lokke Moerel Binding Corporate rules, Fixing the regulatory patchwork of data protection 2011

is allowed if it is not forbidden. [71] But the EU law states that surveillance is legal if it is provided with any legal basis. In addition, the US law has double track system regarding to surveillance. So regarding to this track, the US law has some distinctions between the US and non-US persons. This different treatment is considered legal referring to the Fourth Amendment and this situation makes finding adequacy level of protection difficult. Because priority of the EU to find adequate level protection is individual rights while the US is more willing to protect the state during the data transfers and shows reluctant attitude toward limitation of intelligence and surveillance activities. It is quite significant problem because even the all requirements which article 45 states are satisfied, receiving the adequate level of protection will be impossible because of the double- track system in surveillance.

Conflicts starts to become deeper after the CLOUD Act. This collision is seen from Article 3 of the GDPR and § 27713 of the CLOUD Act due to their exterritorial effect. The GDPR was enacted in the same year with the CLOUD Act. As it is mentioned previous sub chapter, the Cloud Act enacted as a reply to legal issues were raised in Microsoft Ireland v. US case to provide the SCA warrants with exterritoriality. The US established new method of international lawmaking via domestic law and regulation. [72] Because it has exterritorial power like international agreements, but the CLOUD Act is just part of domestic law, it is not international agreement. It is stated in § 27713, location is does not matter, if the personal data under the custody of the company, then this Act applies. Because of the exterritorial influence of both

[71] Anna Dimitrova and Maja Brkan, 'Balancing National Security and Data Protection: The Role of EU and US Policy-Makers and Courts before and after the NSA Affair' (2018)

[72] Jennifer Daskal, "Microsoft Ireland, the CLOUD Act and International Lawmaking 2.0," Stanford Law Review Online 71 (2018-2018):9-16

regulation there is a tension between them. the GDPR applies if data subject in the EU, even processor is in outside of the EU. It means that, subsidiary companies in EU which gets SCA warrant to disclose data and obliged to transfer data under the US law, face conflicting obligations, since subsidiaries of the US based company targets GDPR at the same time, however these subsidiaries belong to US company.

The GDPR allows data to be freely transfer across EU member states, where the protections afforded by the Regulation are in force, while conflicts occur when there is a need to transfer data to third countries. Recital 101 of the GDPR demonstrates a good example of ground for conflict. Protection of individuals and personal data are protected by the GDPR and it should not be undermined when data is transferred from EU to controllers in third countries and international organizations.[73] As it is seen from recital 101, the GDPR establishes requirements for data transfers from the EU to international organizations as third countries. But there is a great possibility jurisdiction of third countries regulates cross-border data transfer with different criteria and rules which are mandatory for data processor in third countries. This problem occurs because in the GDPR, location of processor and controller is not considered as a factor which can leads to invoke provision. As it is explained in previous subchapter, referring to Article 3 of GDPR, data processors in third controllers are target to GDPR.

Because of the importance of protection of personal data GDPR has strict requirements for data transfer from EU to third countries. Firstly, cross-border data transfer must fulfill at least one lawful ground for processing according to article 6. Secondly, transfer should be appropriate one of the rules which are presented in Chapter V. At first glance, attitude of the GDPR looks too conservative. However highest standards of data protection can be a hinderance for companies and crime investigations, it is still possible to understand strict criteria of the GDPR. There is a great possibility that company which are not subject to the GDPR, can request for

[73] Recital 101, GDPR

data transfer of individuals who are subject to the GDPR. If the GDPR could not regulate this situation, individuals might suffer from lacks in third countries' jurisdictions which can not offer high quality data protection. That's why, aim of the GDPR is to protect data protection in any kind of danger possibility.

First requirement for data transfer is appropriateness of transfers to Article 6 of GDPR. Initially, transfer of personal data based of US LEA warrants is allowed if processing is carried out because of legal obligation. It can said that CLOUD Act determine obligation of providers to disclose personal data, but the problem that CLOUD Act is not international or bilateral agreement between US and EU. It is problem because if a state establish a regulation which has exterritoriality then, this situation can lead to violence of fundamental principles of international principles such as sovereignty. This obligation is recognized only by US. As there is not an agreement between Eu and US legal obligations of fata processors are not recognized by EU. In this point importance of agreement between US and EU is observed.

Secondly, lawful process means that processing is essential for public interest and exercise official authority.[74] CLOUD Act claims, US LEA can request cloud service providers to disclose information for crime investigation. It is obvious, providing LEA with evidence is essential for public interest and exercise of official authority. However, there is a problem that , as it is mentioned above, due to non-existence of agreement between US and EU, public interest in US and exercises of official authorities have no legal meaning for EU. At the same time, Article 29 Data Protection Working Party claims that data can be shared in specific situations. In case of transnational crimes such as terrorism, if both countries are interested in

[74] Article 6.1(e) of GDPR

solution and data protection rules are complied, then data can be transferred.[75] Despite this fact, it is not enough to say that the CLOUD Act is applicable despite conflict with GDPR. As purpose of thesis is to find common ground for cross-border data transfer generally, not specially for transnational crimes, it is just exclusion which can be used in case of transnational crime.

Following requirement for legal processing is legitime interest. Article 6.1 (f) states that processing should be necessary due to purposes of legitime interest pursued by the controller or third party.[76] According to this provision, legitimate interest of data controller and legitimate interest of data subject are compared. It is fact that if data processor does not transfer data to US despite warrant, there is a great possibility that processor or controller will face sanction. In addition, recital 50 states that if data controller indicates threats or criminal acts to public security and transfers data related to criminal acts or threats to public security, it should be considered as legitimate interest which is pursued by controller. On the other hand, EDPB affirmed that due to absence of international framework, US LEA are not considered component authority.[77] Therefore, it is impossible to use legitimate interest as legal basis for cross-border data transfer between US and EU.

---

[75] Article 29 Data Protection Working Party , 'Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC' WP 217 19.

[76] Article 6.1(f) of GDPR

[77] EDPB OPNION: Initial legal assessment of the impact of the US CLOUD Act on the EU legal framework for the protection of personal data and the negotiations of an EU-US Agreement on cross-border access to electronic evidence, 2019

Article 6 of GDPR is not enough to determine protection measures in cross-border data transfer from EU to US. The rules stated in Chapter V of the GDPR should be satisfied in order to provide cross-border data transfer with high level of protection. Regarding to the Article 44 personal data can be transferred to third county if transfer s subject to the GDPR, and if the controller and the processor follow the obligation this regulation[78]. A it is explained above, because of the differences between legal system of the US and the EU, it is difficult to say that the US would follow requirement of the GDPR, especially because of the derogations of law in the US. This article makes deeper the collision because the US wants to get acces to the data in third countries but this provision hinders it. Article 45 demands adequacy decision which focuses on the fundamental values and human rights founded by the EU. Commission should take into consideration that if the third country respect rule of law, and if legislation of the third country cover human rights and standards enough.[79] There were two adequacy decision and they were invalidated because of the same reasons. In addition, article 46 provides free data transfer to non-EU countries and ensures equivalent level of protection.[80] Data controller or processor can transfer the personal data to the third country if the country can offer adequate level protection measures.[81] If there is not an adequacy decision The CJEU stated in Schrems I that if there is adequate level of protection, it demonstrates that there is sufficient level of protection of fundamental freedoms and rights.[82] In case of absence of adequacy decision,

[78] Article 45 the GDPR

[79] Recital 104 GDPR

[80] Article 46 GDPR

[81] Ibid

[82] C-362/14, Maximiilian Schrems v, Data Protection Commissioner, (2015) ECLI:EU:C:2015:650.

standard contractual clauses and binding corporate rules can be used for data transfer but these SCCs always have pre-determined purposes, so they can not be appropriate solution to support SCA warrants.[83]. Especially Article 46 states that data can be transferred to third countries if data processor can offer essential safeguards. But the problem is that even if country provides adequate level of protection, transfers should have predefined purpose. If there should be a predefined purpose of data transfer, it means that there is a need for agreement between US and EU.

Article 48 also highlights importance of international agreement between EU and US for cross-border data transfer. It is stated that judgement of courts or decision of administrative authority of non-EU countries which require to disclose data cannot be recognized under EU law without international agreement.[84] As it is not international agreement, CLOUD Act is not accepted as a basis for cross-border data transfer however it defines obligation of cloud service providers to disclose data. In this article the GDPR aims to prevent legislation of third countries from regulating data processing which is under the EU law.[85]

Article 49 states derogation for specific situation and narrowly identify requirements for third party for data transfer in case of absence of standard contractual clauses and adequacy decision.[86] Despite this, CLOUD Act warrant is not suitable to narrowly identified exemption in article 49. Reason is that, service provider may not determine purpose of warrant, therefore

[83] European Union Agency for Fundamental Rights (FRA) *Handbook on European data protection law* (2nd edn Publications Office of the European Union 2018) 257

[84] Article 48 GDPR

[85] Recital 168 GDPR

[86] Article 49 GDPR

it becomes impossible to identify warrant is appropriate to which requirements of article 49. In addition, problem is to find common ground for regular cross-border data transfer from EU to US. Article 49 is not appropriate for daily use, it can be used only in urgent situation.[87]

1.4 Arguments about sovereignty and extraterritorial law enforcement

The sovereignty principle is one of the fundamental principles of international law.[88] That principle means that every state is independent to determine its destiny, relations. That principle has dense relation with non-intervention rule which is another fundamental principle of international law. That principle means that every country is independent in to solve their internal affairs and other states cannot intervene in other states' internal affairs. What happens to these principles if a regulation has an exterritorial power? As it is mentioned above, the CLOUD Act is not international agreement or regulation. It can be said that the US established new kind of rule. Because it is part of domestic law of the US but can influence on other countries because of its exterritoriality. It means that the CLOUD Act gives an opportunity to the US legal enforcement authorities to violate principles of international law. International agreements mean formal commitments among states and states can determine terms and condition of this agreement and they should be free to enter agreement and nobody can force states to enter agreement. If we look current situation, as the CLOUD Act part of domestic law and the US established it, it was not negotiated with other states. However, the CLOUD Act has influence on these states. Therefore, some collisions occur between different jurisdiction. The CLOUD Act gives opportunity to the provider for challenging a warrant as per the concept of "common law comity analysis and under the same, courts may consider the factors stated in

[87] European Data Protection Board (n 127) 5

[88] Daniel Halvarsson The suspect and mutual legal assistance 2015

Société Nationale Industrielle Aerospatiale:[89] (1) the value of the requested information;[90] (2) the extent of specificity of the concerned request;[91] (3) whether the source of the information can be traced to the United States;[92] (4) the existence of alternative means of obtaining the requested information;[93] and (5) the interests of the United States and foreign countries concerned."[94] Despite that, It does not mean that the CLOUD Act does not infringe principles of international law.

In addition, however the GDPR has international importance it can be said that the GDPR also infringe fundamental principles of international law which mentioned above. The territorial scope of the GDPR is determined with location of establishments and EU citizens, so it is not only applicable in the member states, but also in the outside of the EU. If the US company to process personal data of the EU citizen and if situation is suitable to targeting principle, then that company should follow provisions of the GDPR.

[89] Société Nationale Industrielle Aérospatiale, 482 U.S. 522 (1987), available at < https://supreme.justia.com/cases/federal/us/482/522/>.

[90] Ibid

[91] Ibid

[92] Ibid

[93] Ibid

[94] Ibid

Chapter 2- Possibility of suggested solutions

This chapter focuses on the research of suggested solutions to the legal collisions between the CLOUD Act and the GDPR, and analyzes the possibility of application of these solutions. Initially, the possibility of an international agreement between the US and the EU is explained. Such an agreement would be one of the most suitable solutions, but the question is what *kind* of agreement is needed: an international agreement between the EU as a whole and the US, or individual bilateral agreements between every EU member state and the US? Guidance can be found in the US-UK agreement, which is based on CLOUD Act. That agreement was signed when UK was a EU member state, and it creates an opinion that if one member states can transfer personal data according to bilateral agreement why there is not an agreement for all member states. So far, there have been two agreements between the EU as a whole and the US, namely the Safe Harbor and Privacy Shield, which were both invalidated. This chapter also includes most recent steps about personal data transfer like Transatlantic Data Privacy Framework. It is stated that the EU and the US have agreed in principle on a new framework for trans-Atlantic data flows. However, it is difficult say that it is exact and permanent solution for data transfer because this kind of agreements were invalidated. Therefore, current situation and situation before enactment of Privacy Shield is compared in this chapter to determine that new framework can be a permanent solution, or it is just trick a trick to get more time to find real solution. In addition, agreements are not the only solution to solve collision, therefore, role of international private law is also explained referring to the conflict between two jurisdictions.

2.1 History repeats: international agreements

Safe Harbor and Privacy Shield should be compared and analyzed to understand what is needed in personal data transfer agreement and what the New Framework suggests. Purpose of this comparison is to determine possibility of third *Schrems* decision and effectiveness of new

framework. Reasons of invalidation of Safe Harbor and Privacy Shield must be determined and compared in this subchapter.

2.1.1 Safe Harbor

Like the GDPR, one of the purposes of the European Data Protection Directive (the DPD) was to encourage free movement of personal data and protect individual rights at the same time. Article 25 of the DPD states that data can be transferred outside the EU if third countries can ensure high level of protection and guarantee adequate level protection measures.[95] The European Commission can determine third countries which can ensure adequate level of protection by adequacy decision. Adequacy is assessed 'in light of all the circumstances' related to data transfer operations including international agreements, domestic laws and 'the rule of law' in force in the third country.[96] It means, adequacy includes assessing the availability of similar or equivalent guarantees and protection measures for data protection in the third countries of a legal framework for data protection.

After examination procedure, the European Commission adopted adequacy decision and stated that Safe Harbour framework is adequate and transatlantic personal data transfer is allowed. In addition, companies are allowed to transfer personal data without any special assessment of the US data protection system under adequacy decision under adequacy decision.[97]

European Commission and the US authorities built a certification regime for companies in US to transfer personal data from the EU to the US by adopting this decision.[98] Under Safe Harbour

[95] Article 25 DPD

[96] .Article 25 (2) DPD)

[97] Adequacy decision 2000/520

[98] Commission Decision 2000/520/EC 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

framework organizations and companies could self- certify their compatibility to the principles of Safe Harbour and requirements of adequate level of protection for data transfer. But this self-certification led to criticism about Safe Harbour. Critics had other arguments related to voluntarily adherence and enforcement commitments.

In 2013, Max Schrems lodged a complaint questioning the lawfulness of transatlantic personal data transfer. Schrems claimed that the US does not provide adequate protection for personal data transfer to EU citizens. The Irish data protection Commissioner rejected Scherm's complaint because EU-US personal data transfers based on the Safe Harbour adequacy decision of Commission.[99] Following this, the Irish High Court requested to determine if the existence of the Safe Harbour adequacy decision hinders a Data Protection Authority investigation based on a complaint. In 2015, the Court of Justice of the EU (CJEU) invalidated the Safe Harbour adequacy decision.

In the Schrems v. Data Protection Commissioner case, the CJEU went further than the Irish Court Schrems and claims, and stated that:[100] national Data Protection Authority has the power to examine a claim and this power can not hindered by the adequacy decision of Commission; the findings of European Commission on the Safe Harbour voluntary scheme is not sufficient

safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce [2000] OJ L215/7 (Safe Harbour Decision)

[99] Shara Monteleone, Laure Puccio, From Safe Harbour to Privacy Shield: Advances and shortcomings of the new EU-US data transfer rules 2017

[100] Case C-362/14 Maximilian Schrems v. Data Protection Commissioner, of 6 October 2015.

to guarantee that EU citizens' personal data are appropriately protected in the US; derogations for security must be proportional and necessary.[101]

One of the reasons for invalidation of Safe Harbour Framework is that it **lacks in high level of protection**. Self-certification system in third countries is not contrary to the adequacy requirement in Article 25 (6) of Directive. But referring to adequacy requirement, this self-certification must be reliable. It means that that mechanism must enable to identify and punish any infringement of rules which protect fundamental rights related to personal data. Following this, principles of Safe Harbour are applicable for self-certified US organizations and companies which receives personal data, so public authorities do not have any obligation about following the principles. Application of this principle can be limited under US law.

Derogations for law enforcement is another reason led to invalidation of Safe Harbour. In the US, public interest, requirements of law enforcement and national security prevail over principles and requirements of the safe harbour framework. It means, if there is a **conflict** between that US companies and requirement of Safe Harbour, then companies can disregard Safe Harbour framework without limitation. For the US law, it does not matter that if the data is sensitive or data subject will be affected negatively. Therefore, this situation creates interference to protection of fundamental rights by US public authorities. Additionally, adequacy decision does not include any rules or law in the US which can eliminate this interference and does not mention and legal protection. The European Commission failed to present redress mechanism for EU citizens to protect them unlawful data processing. Therefore, the CJEU stated that if the legislation allow public authorities to access personal data on general basis then it jeopardizes fundamental rights. Following this, absence of remedies

[101] Case C-362/14 Maximilian Schrems v. Data Protection Commissioner, of 6 October 2015.

demonstrate disrespectful attitude to right to effective judicial protection which is stated in Article 47 of the Charter of Fundamental Rights.

2.1.2. From Safe Harbour to Privacy Shield

In 2016, following the CJEU's ruling in *Schrems*, the European Commission adopted adequacy decision and the new Privacy Shield framework had to comply with CJEU indications. As Safe Harbour was invalidated these reasons, new framework was supposed to involve remedies, ensure adequate level of protection and situation about derogation of law to avoid invalidation by the CJEU.

Some critics claim Privacy Shield is almost same with Safe Harbour, only name is different. Differences and similarities should be analyzed to decide if it is new framework or not.

Privacy Shield includes the same principles as Safe Harbour, but the difference is that individual rights of EU citizens are highlighted better in Privacy Shield and it contains stricter requirements for US companies and has a limitation for US government and hinders its access to data. One of the major changes is about onward Transfers principle. In Safe Harbour, a company or organization should provide consumer with a choice to share their personal data with third parties. But there is not a requirement if third party acts on behalf of third organization. In Privacy Shield, if companies transfer data to third parties they must follow principle of purpose limitation and they should ensure that third parties are able to provide same level of protection with original company.[102] Following this, organization has a liability if the other company (third party) does not follow requirement of Privacy Shield.

Although self-certification remained, there were some changes about this. The Department of Commerce had expanded authority and the department can hold compliance review periodically. Additionally, The department had a role like liaison with Data Protection

[102] https://www.otava.com/reference/how-does-safe-harbor-compare-to-the-eu-us-privacy-shield/

Authorities of EU. About the reporting issues, companies should keep records of privacy program and they should submit them to regulators if they request, while organization and companies had to provide compliance annually under Safe Harbour. Another difference of Privacy Shield is, if the company withdraws from Privacy shield, the company remain responsible for obtained data before withdrawn and the company should provide the department with compliance.

As a response of CJEU ruling in *Schrems*, Privacy Shield agreement includes remedies to protect EU citizens. EU citizens have different avenues to file complaints, including European Data Protection Authorities, or independent U.S ombudsman. Ombudsman must answer individual complains with compliance confirmation or non-compliance remediation. Ombudsperson must ensure sufficient investigation of complaints.

Despite changes and improvements, the CJEU again invalidated privacy shield agreement in 2020 in its ruling on the case *Schrems II*. Reasons of invalidation are almost same with invalidation of Safe Harbour. Firstly, Court stated that the US can not offer adequate level of protection as mentioned in the GDPR. Reason of this inappropriateness is derogation of law. The legal bases of surveillance programs (PRISM, UPSTREAM) in the US do not have any limits, so referring to requirements of article 45 (1) GDPR, this is unlawful interference with individual rights because they these programs do not limit the US authorities' power and it is significant disadvantage for EU subjects.[103] Another reason is related to US Ombudsman. This redress mechanism was established to protect Eu citizens, but it is not appropriate remedy because it hinders application of right to effective Judicial protection because of independence of the institution and the enforceability of decision of Ombudsman.[104]

[103] Hendrik Mildebrath, The CJEU judgment in the *Schrems II* case, 2020

[104] Hendrik Mildebrath, The CJEU judgment in the *Schrems II* case, 2020

2.2. The Cloud Act agreements.

If there is a collision, the agreement is the most appropriate way to solve it and this option is also recommended by the CLOUD Act. As it was explained previous chapter, one of the features of the CLOUD Act is giving opportunity to enter agreements with other states which are qualifying government for personal data transfer. There are four conditions which should be fulfilled to enter agreement under the CLOUD Act. Firs, the country which enter agreement with the US should provide civil liberties and privacy protection. Secondly, procedural standards for the US citizens' personal data transfer must minimize retention, dissemination, and information acquisition. Following this , third country cannot demand from data providers to decrypt data. Last requirement is about good faith.

As it was analyzed previous sub chapter, balance between access to personal data and individual rights should be provided to receive sufficient agreement which will not be invalidated by the CJEU. One of the conditions to keep this balance is to have reciprocal access to personal data. But this condition does not involve the US citizens. As the EU law does not differentiate data subject regarding to nationality, this distinction should be mentioned in biliteral agreement between the US and qualifying government to be compatible with the EU law.

Another requirement is about necessity and proportionality. When order issued to get personal data, legal enforcement authorities should demonstrate that that order id suitable to requirement of necessity and proportionality and interference is understandable.[105] As the CJEU mentioned, existence of reasonable link between requested data and commitment crime is mandatory to claim that that personal data is necessary in the light of circumstance. Categories of seriousness

[105] Article 29 Data Protection Working Party, " Opinion 06/2014 on the notion of legitimate interest of the data controller under Article 7 of Directive 95/46/EC' WP 217 19

crimes should be provided because of the requirement of this principle. The definition of serious crime is not given in the CLOUD Act. It can be claimed that serious crimes are almost same in every legislation for example homicide, child, pornography. But it is not possible to say that all legislations have same serious crimes and have same criteria to determine which crime is more serious. Therefore, bilateral agreement should give explanation of serious crime to provide parties with egal certainty.

Judicial oversight is also necessary to get sufficiently drafted bilateral agreement. Judicial overviews help to ensure protection of individual rights. Another condition for biliteral agreements is notification and judicial remedy. Usually data subject do not have any information about disclosing of their personal data. Regarding to the article 14 (4) of the GDPR, legal enforcement authorities have to inform data subject about the transfer of their personal data. However, in case of criminal investigation notification can be limited.[106]

2.3 First CLOUD Act agreement: personal data transfer between UK and US.

The United Kingdom is the first country which entered an agreement with the US under the statute. [107] It can be estimated that citizenship is not mentioned because if the UK citizen is in another member state the GDPR applies and collision would occur. This agreement does not cover the UK citizen in other states to avoid collision. The UK implemented and edited some provisions of the GDPR and the GDPR became part of the domestic law of the UK. Now the UK is not member state anymore but when the US and the UK entered agreement UK was

[106] Art 23, 11(2) GDPR

[107] Drew Mitnick, *"hat Happened with the CLOUD Act (and What Comes Next),* ACCESS Now (Mar. 27, 2018), https://www.accessnow.org/what- happened-with-the-cloud-act-and-what-comes-next/ ("The first country that the U.S. will likely reach an agreement with is the United Kingdom...").

member country and despite the requirements of GDPR. It proves that entering agreement with the US is possible despite GDPR and this bilateral agreement can be a role model for future agreements between the US and other EU states. The Executive Agreement became into force after Congressional review, continued 180 days, and this period is required by the CLOUD Act.

Scope of application of agreement is determined in Article 1. The scope of application of this agreement is limited to data used by covered person, but there is not any limit toward data used by receiving party. Following, this Article 1(12) sates that receiving party includes permanent resident, US government official or person and corporations in the UK. [108] It means that the Agreement does not give an authority to the UK government to receive personal data of the US citizens unlike GDPR. The reason of this limitation is protection the US citizens under Fourth Amendment. It means that the US legal enforcement authorities also cannot receive or request personal data of the person in UK. But it is not explained that if the person in UK is citizen of UK.[109] These provisions help to eliminate possibility of conflicts of law. In the GDPR nationality does not matter and it increase exterritorial influence of GDPR. Therefore, conflicts of law, like between the GDPR and the CLOUD Act, can happen, so it means if there will be a collision between the agreement and domestic law of countries, agreement will apply. Unlike Safe Harbour and Privacy shield, this Agreement include provision against derogation of law. Article 3 states that domestic law of countries cannot prevent company from acting if the other country request for disclosure of data. If the bilateral agreement enters into force, then it demonstrate its lifting effect of every kind of restriction in US law which hinder companies

[108] Article 1 (12) U.S.-UK/Ir. Executive Agreement,

[109] Marcin Rojszczak, CLOUD act agreement from an EU perspective, Computer Law and Security Review 38 (2020) 105442

to disclose personal data to authorities of foreign countries.[110] Another issue which decreases to possibility of collision is about application of domestic law. For example, if the UK requests disclosure of personal data from the US based company within borders of UK, then domestic law of the UK applies. Article 5 of the agreement is about reasonable justification. This article hinders the orders issued to disclose personal data to the US.[111] Companies or data providers can reject if they consider that this order is not appropriate. [112] Additionally, data controller can also reject to disclose the personal data to the UK government. It looks like there is a possibility of conflicts of laws but in case of disagreement, the US tries to evaluate appropriateness, so it shows how collision is solved.

One of the most important parts of the agreement is Article 7. It sets a requirement for the UK to adopt appropriate minimization procedures to apply to elimination of data of US citizen which obtained incidentally when UK received personal data of target subjects. [113] This article states that the UK has to segregate or delete this kind of data if it is unnecessary for crime investigation. But the lack if the agreement is, it does not give an explanation what necessary means, so the UK should decide itself. Additionally, the UK and the US do not ask for permission to use data. The US need permission if the data which obtained from the UK leads to death penalty. The UK also need a permission only when it can lead to concerns about

[110] DOJ White Paper on CLOUD ACT, supra note 4, at 4.

[111] *Id.* art. 5(4).

[112] ***Id.*** art. 5(11) (12)

[113] ddie B. Kim, 'U.S.-UK Executive Agreement: Case Study of Incidental Collection of Data under the CLOUD Act' (2020) 15 Wash J L Tech & Arts 247

freedom of speech. Lastly, according to the Executive Agreement, the United Kingdom does not require permission to use data obtained unless it raises freedom of speech concerns.[114]

[114] ddie B. Kim, 'U.S.-UK Executive Agreement: Case Study of Incidental Collection of Data under the CLOUD Act' (2020) 15 Wash J L Tech & Arts 247

Conclusion

First chapter explained collision between two jurisdictions because of the exterritorial power of the GDPR and the CLOUD Act. That exterritoriality means that the GDPR can influence US based companies which locates in the US and their branches or subsidiaries in the EU and the CLOUD Acts states that SCA warrants have exterritorial power and branch, or subsidiary of the US based company has to disclose personal data despite restriction of the GDPR. Regarding to the principle of sovereignty both regulations have mistaken. Firstly, the CLOUD act is a part of domestic law therefore if it claims something which influence sovereignty of third country, application of this regulation becomes impossible. On the other hand, the GDPR has an international importance it is not a part of domestic law. However, this regulation belong to member states and the US do not have an obligation to follow the requirement of the regulation because it is not member state. It can be said that however the GDPR aim to protect individual rights of EU citizens regardless to location, because of the principles of international law, exterritorial effect is execrated a bit. In this situation it is impossible to determine the winner of the conflicts of law, therefore a solution should be offered to reconcile inculpabilities between two jurisdictions. One of the most efficient ways to solve the collision is agreements, so both parties can suggest their requirements and abilities to transfer data and to protect individual rights at the same time. But the crucial point is what kind of agreement is needed. Should it be an international agreement between the US and the EU or collision can be solved by using individual agreements between separate member states and the US. This thesis also analyzed the role of the CLOUD Act in agreements however its exterritoriality is invalid. Thesis also analyzed different and the same issues in safe Harbour and Privacy Shield agreements to determining effectiveness of new Trans-Atlantic Data Privacy Framework. Considering the comparison of two previous agreement to transfer the personal data between the US and the EU, New Framework does not look like permanent solution. The invalidation

reasons of Safe Harbour framework in the CJEU ruling had to be taken into consideration when Privacy Shield was enacted but it was not taken into consideration at all. Privacy Shield agreement had some changes and some new things such as remedies but there was not a material change. One of the main reasons was derogation of the law which was a danger for individual rights so it made to offer adequate level of protection impossible. Therefore Privacy Shield framework was invalidated because of the same reasons. The draft of the new framework is not ready but it was claimed what promises new framework. That promises is not no much different from Promises in privacy Shield framework :free and safe data flow, limitation of data access, new redress system, obligation of companies, monitoring mechanism. There is always a need for upgraded redress system, monitoring mechanism and other promised things. However, core problem is not about the redress system, obligations of companies and monitoring systems. The fundamental problem which hinder to get adequate level of protection for data transfer is derogation of law. It means that the domestic law of the US always has a priority and there is no promise about to limit this derogation in New Framework like the Privacy Shield framework. As The Cloud is domestic law , it means if there will be any conflict between new framework and the CLOUD Act, the act will prevail and the CJEU will invalidate the third framework and there will be Scherms III. The problem is not the remedy system or the provisions of the agreements. The commission is looking for a problem in a wrong place. The problem is the US law itself and EU does not want to compromise. In this collision EU looks more powerful side because the US always tries to offer adequate level of protection and it is seen from both Scherms rulings the US should be appropriate to criteria of the EU. It is understandable because the number of the data subjects who are in the EU is more than data controllers in the US. There is a danger that some companies can not continue their business without data transfer and can lead to close the market in the EU and the companies and a lot of people will not able to use social media platform and it will lead to complaints of EU citizens.

But isn't is also infringement of human rights? The argument in Scherms decisions was unviability of safeguards and danger for individual rights but that invalidation also lead to danger for EU citizen rights. This thesis leaves this question open end because it goes to another direction.

There are two possible solution to have sufficient agreement between the EU and US. First option is to add an article to the agreement that " if here is a collision between data transfer agreement and domestic law of states, then agreement applies. Another solution and more difficult one is to make changes to the US law and to remove the derogation issue from legislation. There is another open-end question " how to change the US law? And is it possible?"

Another possible solution is to have an agreement between the US and separate member states, how the US and the UK entered the agreement when the UK was member state. There are some provisions which hinder possible collision. Firstly the US-UK data sharing agreements limits the exterritoriality and the location is the main criteria to determine the limits of the power of the US and the UK government. Each government knows their territory exactly. Secondly there is an article which eliminate derogation and support application of the agreement in case of collision. But there is another problem about EU law. The UK-US data sharing agreement states that US warrants are not applicable to person in the UK. The absence of the using the term citizen of the UK helped the UK to have a conflict with the EU. But there is a still possibility of the conflict because person in the UK can be also UK citizen who subject to EU law. It means that if other member states want to enter agreement with the US it can lead to the conflict with the EU because it is against the functions of the EU. On the other hand, every member state is independent and regarding to the principles of the international law such as principle of non-intervention in internal affairs and sovereignty principles every member state has a right to enter agreement independently. For the application of the solution which

suggested by this thesis, balance between the function of the EU and the right of the states to enter agreement should be determined. After determination of this balance the agreement like the UK-US data sharing agreement can be used to transfer data and to solve collision between the GDPR and the CLOUD Act.

Bibliography

Case law

C-311/18 Data Protection Commissioner v Facebook Ireland Ltd (2020)

C-487/07 L'Oreal Sa and others v. Bellure NV and others [2009]

389 U.S. 347 Katz v. United States (1967).

389 U.S. 347 Katz v. United States (1967).

307 U.S. 174 United States v. Miller (1934)

425 U.S. 435 united States v. Miller (1976)

442 U.S. 746 Smith v. Maryland (1967)

ECLI:EU:C:2020:559

C-362/14, Maximilian Schrems v, Data Protection Commissioner, (2015) ECLI:EU:C:2015:650.

Clarifying Lawful Overseas Use of Data Act, (2018)

Electronic Communications Privacy Act (1986)

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (2016)

Fischer, Jordan L. “The U.S. Perspective on Schrems II: The Challenges of the Extraterritorial Application of the EU Perspective.” (2021)

Jennifer Daskal, Microsoft Ireland, the CLOUD Act, and international lawmaking 2.0, 71 Stan. L. REV. ONLINE 9 (2018-2019)

Jordan A. Klumpp, International Impact of the Clarifying Lawful Overseas Use of Data (CLOUD) Act and Suggested Amendments to Improve Foreign Relations, 48 GA. J. INT'l & COMP. L. 613 (2020)

Marcin Rojszak, CLOUD act agreements from an EU perspective (2020)

Secil Bilgic, Something old, something new, and something moot: The privacy crisis under the CLOUD Act, (2018)

EDPB OPNION: Initial legal assessment of the impact of the US CLOUD Act on the EU legal framework for the protection of personal data and the negotiations of an EU-US Agreement on cross-border access to electronic evidence, (2019)

Theodore Christakis ,“Transfer of EU Personal Data to U.S. Law Enforcement Authorities After the CLOUD Act: Is There a Conflict with the GDPR?”

Jordan A. Klumpp, "International Impact of the Clarifying Lawful Overseas Use of Data (CLOUD) Act and Suggested Amendments to Improve Foreign Relations," Georgia Journal of International and Comparative Law 48, no. 2 (2020): 613-644

Johannes Thumfart and Paul De Hert, “Both the US’s Cloud Act and Europe’s GDPR Move Far Beyond Geography, but Will Not Solve Transatlantic Jurisdictional ConFicts” (2019)

STEPHEN W SMITH, “Clouds on the Horizon: Cross-Border Surveillance Under the US CLOUD Act” (2019)

Ata Umur, Kalender, “Partly Cloudy: the Cloud Act and Its Effects” (2020)

Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters [2014] OJ L130/1.

European Data Protection Board, ‘Guidelines on derogations of Article 49 under Regulation 2016/679’ (2018) 2/2018

European Data Protection Board, ‘Guidelines on the territorial scope of the GDPR (Article 3) - Version for public consultation’ (2018) 3/2018

European Data Protection Board, ‘Opinion on Commission proposals on European Production and Preservation Orders for electronic evidence in criminal matters (Art. 70.1.b)’ 23/2018

Daskal J, ‘Microsoft Ireland, the CLOUD Act, and International Lawmaking 2.0’ (2018) 71 Stanford Law Review

Daskal J, ‘Unpacking the CLOUD Act’ (2019) 4 Eucrim The European Criminal Law Associations Forum

De Hert P, Czerniawski M, ‘Expanding the European data protection scope beyond territory: Article 3 of the General Data Protection Regulation in its wider context’ 6 International Data Privacy Law (2016)

Paul Schwartz, Karl-Nikolaus Peifer, “Data Localization under the CLOUD Act and the GDPR” (2019)

Siyuan Chen, “Cross-border data transfer after Schrems II: the globalization of EU standards of data protection through adequacy decisions or trade agreements?” (2021)

Genç, Sema Yılmaz, and Hassan Syed. 2019. “EU GDPR & US CLOUD Act: David versus Goliath,” January. doi:10.13140/rg.2.2.13373.72163.

“GDPR: What Next?” 2018. British Baker, July, 13. https://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=130661110&site=eds-live.

Mawhinney, Darren. 2017. “How The Cloud Can Help Your Business Get Compliant With GDPR: The Time to Act Is Now.”

Yakovleva, Svetlana. “Personal Data Transfers in International Trade and EU Law: A Tale of Two ‘Necessities.’” The Journal of World Investment & Trade 21, no. 6 (December 1, 2020): 881–919.

Michael E. Lackey, Oral D. Pottinger, ‘Stored Communications Act: Practical Considerations’ (LexisNexis, 22 June 2018) < https://www.lexisnexis.com/lexis-practice-advisor/the- journal/b/lpa/archive/2018/06/22/stored-communications-act-practical-considerations.aspx> accessed 20 May 2019

Wall D, ‘Crime, security and information communication technologies: The changing cybersecurity threat landscape and implications for regulation and policing’, in Brownsword, Scotford, Yeung (eds), The Oxford Handbook on the Law and Regulation of Technology (Oxford University Press 2017).