universität wien

MASTER THESIS

Titel der Masterarbeit / Title of the Master‘s Thesis

„Schrems 2.0 and Cloud Computing: An Analysis of EU-U.S. Data Transfers“

verfasst von / submitted by

Mag.iur. Julia Bauer

angestrebter akademischer Grad / in partial fulfilment of the requirements for the degree of

Master of Laws (LL.M.)

Wien, 2019 / Vienna 2019

Studienkennzahl lt. Studienblatt Postgraduate programme code as it appears on the student record sheet:	UA 992 942
Studienrichtung lt. Studienblatt / Postgraduate programme as it appears on the student record sheet:	Informations- und Medienrecht
Betreut von / Supervisor:	Univ.-Prof. Dr. Nikolaus Forgó

Ehrenwörtliche Erklärung

Ich erkläre hiermit ehrenwörtlich, dass ich die vorliegende Arbeit selbstständig und ohne fremde Hilfe verfasst, andere als die angegebenen Quellen nicht benutzt und die den Quellen wörtlich oder inhaltlich entnommenen Stellen als solche kenntlich gemacht habe. Die Arbeit wurde bisher in gleicher oder ähnlicher Form keiner anderen inländischen oder ausländischen Prüfungsbehörde vorgelegt und auch noch nicht veröffentlicht. Die vorliegende Fassung entspricht der eingereichten elektronischen Version.

WIEN, Juni 2019 Mag. iur. Julia Bauer

List of Abbreviations

BCR	Binding Corporate Rules
CIA	Central Intelligence Agency
CFR	Charter of Fundamental Rights of the European Union
CJEU	Court of Justice of the European Union
Cloud Act	Clarifying Lawful Overseas Use of Data Act 2018
DoC	Department of Commerce
DoJ	Department of Justice
DOT	Department of Transportation
DNI	Director of National Intelligence
DPA	Data Protection Authority
DSGVO	EU-Datenschutz-Grundverordnung
ECHR	European Convention of Human Rights
ECJ	European Court of Justice
ECPA	Electronic Communications Privacy Act
EDPB	European Data Protection Board
EDRi	European Digital Rights
EO	Executive Order
EPOC	European Production Order Certificate
EPOC-PR	European Preservation Order Certificate
EPRS	European Parliamentary Research Service
FBI	Federal Bureau of Investigations
FISA	Foreign Intelligence Surveillance Act
FISC	Foreign Intelligence Surveillance Court
FISCR	Foreign Intelligence Surveillance Court of Review
FTC	U.S. Federal Trade Commission
GDPR	General Data Protection Regulation

ITA	International Trade Administration
NIST	National Institute of Standards and Technology
NSA	U.S. National Security Agency
PCLOB	Privacy and Civil Liberties Oversight Board
PPD-28	Presidential Policy Directive 28
SCA	Stored Communications Act
SCC	Standard contractual clauses
TFEU	Treaty on the Functioning of the European Union
U.S.A.	United States of America
U.S.C.	United States Code

Table of Contents

1. Introduction

The use of cloud technologies has rapidly increased over the last decade.[1] Storing documents, photos, or videos on cloud services such as Dropbox, Apple iCloud, and Google Drive, has become a common practice in our daily lives. The term 'cloud computing' or 'cloud' refers to IT infrastructure, such as hardware, software applications, databases, and storage capacity, which is provided by third parties over the Internet.[2]

According to a report published in December 2018 by Eurostat, one out of four enterprises in the European Union (EU) uses cloud computing services to store files or to host their e-mail systems.[3] This emerging trend can be explained by the changes in working practices, such as the growth in mobile work, where flexible access to IT resources are in high demand.[4] Another reason for the adoption of cloud computing is efficiency and reduction of maintenance costs.[5]

The outsourcing of IT infrastructure to external operators does not only have benefits, but also poses many challenges with regard to data protection and data integrity. When using cloud technologies to store personal data in the cloud, risks to data security like data loss, destruction of data, and unauthorized access by third parties or authorities of countries outside the EU/European Economic Area (EEA) need to be taken into account.[6]

With respect to compliance with the General Data Protection Regulation (GDPR), it needs to be considered that the vast majority of cloud computing infrastructure is located in the United States of America (USA). U.S.-based cloud providers such as Amazon Web Services, Salesforce, Microsoft Azure, Google cloud, and IBM are among the top cloud providers in 2019.[7]

---

[1] *Der Standard.at* (2018, December 13): Österreichs Unternehmen bei Cloud Computing unter EU-Schnitt, Retrieved June 17, 2019, from https://derstandard.at/2000093856112/Oesterreichs-Unternehmen-bei-Cloud-Computing-unter-EU-Schnitt.
[2] *Raffling, Mag. Philip / Schock*, *Mag.a Sofie (2018):* Digitale Wirtschaft und Industrie 4.0, Manz 2018, p. 47.
[3] *Eurostat* (2018, December): Cloud computing - statistics on the use by enterprises - Statistics Explained. Retrieved June 17, 2019, from https://ec.europa.eu/eurostat/statistics-explained/index.php/Cloud_computing_-_statistics_on_the_use_by_enterprises.
[4] *Leschanz, Judith / Ehrnberger*, *Verena* (2015): Interne Nutzung von Cloud-Dienstleistungen in Unternehmen, Dako 2015/45, Heft 4/2015, p. 84.
[5] *Dürager*, Sonja (2017): Outsourcing in die Cloud. Ein (un-)beherrschbares Risiko aus datenschutzrechtlicher Sicht?, ipCompetence 2017, Heft 18, p. 36.
[6] *Djemame, Karim / Barnitzke, Benno / Corrales, Marcelo / Kiran, Mariam / Jiang, Ming / Armstrong, Django / Forgó, Nikolaus / Nwankwo, Iheanyi* (2013): Legal Issues in Clouds: Towards a Risk Inventory, Philosophical Transactions of the Royal Society A. Mathematical, Physical and Engineering Sciences, p. 2.
[7] *Dignan, Larry* (2019, May 12): Top cloud providers 2019: AWS, Microsoft Azure, Google Cloud; IBM makes hybrid move; Salesforce dominates SaaS, Retrieved June 17, 2019, from https://www.zdnet.com/article/top-cloud-providers-2019-aws-microsoft-azure-google-cloud-ibm-makes-hybrid-move-salesforce-dominates-saas/.

Especially in light of the revelations by Edward Snowden in 2013, about the U.S. National Security Agency's mass surveillance programme, it is not guaranteed that personal data transfers through U.S.-based cloud providers are subject to adequate data protection as defined by the GDPR.[8]

Moreover, under U.S. President Donald Trump the USA has recently implemented the Clarifying Lawful Overseas Use of Data Act, better known as the Cloud Act. This has raised a new challenge for cloud service providers to reconcile the Cloud Act with the European legal framework, in circumstances where data is accessible to the U.S. government under the Act.[9]

However, due to the ongoing process of new technologies, global data transfers, in particular through cloud technologies, have become an integral part of this world. There are legal issues regarding the compatibility of cross-border data transfers with the GDPR, especially between the EU and the USA, where the Privacy Shield framework provides a legal basis for data transfer to the U.S. The Privacy Shield replaced the previous Safe Harbour agreement, which was declared invalid by the European Court of Justice (ECJ) in 2015, because it had insufficient protection for EU citizens.[10]

But also the Privacy Shield framework is subject to intense criticism, such as "the doubtful independence of the proposed U.S. ombudsman, the remaining possibility for bulk collection of data, and the complex systems of redress mechanisms".[11] As a result of the invalidation of the Safe Harbour agreement, another case on EU-U.S. data transfer, which is referred to as "Schrems 2.0."[12], has been brought before the Court of Justice of the European Union (CJEU).[13] The case is the continuation of proceedings against Facebook Ireland Ltd., in which the plaintiff Maximilian Schrems is challenging the transfer of EU citizens' data between the subsidiary Facebook Ireland Ltd. and its American parent company, Facebook, Inc. This time, Facebook,

---

[8] *Macaskill, Ewen / Dance,* Gabriel (2013, November 1): NSA files decoded: Edward Snowden's surveillance revelations explained, Retrieved June 17, 2019, from https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/5.

[9] *Swire, Peter, / Daskal, Jennifer* (2018, March 26): What the CLOUD Act means for privacy pros, Retrieved June 17, 2019, from https://iapp.org/news/a/what-the-cloud-act-means-for-privacy-pros/.

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

[11] *European Parliamentary Research Service* (2018): The Privacy Shield. Update on the state of play of the EU-US data transfer rules, PE 625.151, p. 11, Retrieved June 17, 2019, from http://www.europarl.europa.eu/RegData/etudes/IDAN/2018/625151/EPRS_IDA(2018)625151_EN.pdf.

[12] *Matheson, Lee* (2017, October 3): Understanding 'Schrems 2.0', Retrieved June 17, 2019, from https://iapp.org/news/a/understanding-schrems-2-0/.

[13] Case C-311/18 Reference for a preliminary ruling from the High Court (Ireland) made on 9 May 2018 — *Data Protection Commissioner v Facebook Ireland Limited, Maximillian Schrems*, OJ C 249, 16.7.2018.

Inc. is referring to the EU standard contractual clauses (SCC) as a legal basis for the data transfer from the EU to the U.S.[14]

Apart from challenging the legitimacy of using SCCs, the Irish High Court also questioned the validity of the Privacy Shield on the basis of whether it had sufficiently adequate protections for EU citizens. In light of Snowden's revelations of the massive surveillance program, Schrems alleged in particular that U.S. law and practice did not guarantee an adequate level of data protection. Consequently, a data transfer to Facebook, Inc., which is subject to U.S. surveillance activities, would violate the rights EU citizens under the Charter of Fundamental Rights of the European Union (CFR).[15] Therefore, Schrems submitted an expert opinion from the attorney Ashley Gorski, on U.S surveillance law and intelligence practice. Facebook enlisted Stephen I. Vladeck, a professor of the University of Texas School of Law, and Professor Peter Swire of the Georgia Institute of Technology, to provide expert testimonies on systemic protections under U.S. law for foreign intelligence surveillance.[16] The CJEU's judgment is expected to be delivered sometime in 2019.

In light of the above, this thesis examines the legal issue of whether the transfer of personal data to a third country through a cloud technology complies with the GDPR's requirements. The main focus is on the written submissions on U.S. law and practice. By analysing the expert testimonies and the legal impacts of the Cloud Act, the thesis attempts to answer the question whether or not a European firm under the GDPR can conclude a contract with a U.S. cloud service provider.

First, this thesis shall give an overview of the technical definitions and aspects of Cloud computing (Part 2). Then, it will elaborate on the European legal framework for data protection (Part 3) and its layout regarding cross-border and transnational data transfer (Part 4). This is followed by an overview of U.S. law and practice (Part 5). Part 6 will then provide a discussion of the Cloud Act and its European equivalent, the e-evidence draft Regulation. Finally, to conclude the legal issue regarding EU-U.S. data transfers and cloud computing, it engages in a case study (Part 7).

---

[14] *Carolan, Mary* (2018, April 12): High Court sets out 11 questions for ECJ on EU-US data transfers, Retrieved June 17, 2019, from https://www.irishtimes.com/business/technology/high-court-sets-out-11-questions-for-ecj-on-eu-us-data-transfers-1.3459549.

[15] *International Association of Privacy Professional:* Schrems 2.0: Expert Testimony, Retrieved June 17, 2019, from https://iapp.org/resources/article/schrems-2-0-expert-testimony/.

[16] Id.

2. What is Cloud Computing?

To begin with, it is necessary to understand the various technical aspects before further exploring legal underpinnings. The U.S. National Institute of Standards and Technology (NIST) defines cloud computing as "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction".[17]

The essential characteristics of cloud computing are as follows: "on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service".[18]

The NIST model differentiates between three service models:

Software as a Service (SaaS): The consumer can use the provider's applications, which run on a cloud infrastructure. The cloud consumer is able to access the applications "from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface".[19] Examples of SaaS include salesforce.com,[20] Microsoft CRM online,[21] and SAP Business by Design.[22]

Platform as a Service (PaaS): This model enables the cloud user "to deploy onto the cloud infrastructure consumer-created or acquired applications, that were created using the programming languages, services, and tools supported by the provider".[23]

Infrastructure as a Service (IaaS): The purpose of this capability is to provide "the consumer with processing, storage, networks, and other computing resources, so that the

[17] *Mell, Peter / Grance, Timothy* (2011): The NIST definition of cloud computing. National Institute of Standards and Technology (NIST), U.S. Department of Commerce, p. 2, Retrieved June 17, 2019, from https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf.
[18] Id., p. 2.
[19] Id.
[20] SalesForce: Was ist SaaS? Grundlegendes zu "Software as Service", SalesForce Deutschland, Retrieved June 17, 2019, from https://www.salesforce.com/de/learning-centre/tech/saas/.
[21] Microsoft: Intelligente Geschäftsanwendungen - Microsoft Dynamics 365, Microsoft Deutschland, Retrieved June 17, 2019, from https://dynamics.microsoft.com/de-de/.
[22] SAP: SAP Business by Design, SAP Deutschland, Retrieved June 17, 2019, from https://www.sap.com/austria/products/business-bydesign.html.
[23] Mell / Grance (2011), p. 2f.

consumer is able to deploy and run arbitrary software".[24] Examples of IaaS include Oracle[25] or Amazon Web Services.[26]

Furthermore, there are four different deployment models:

Private cloud: the cloud infrastructure is exclusive for the use of a single organisation.[27]

Public cloud: the use of the cloud infrastructure is open to the general public.[28]

Community cloud: this model is dedicated for the "exclusive use by a specific community of consumers, from organizations with shared concerns".[29]

Hybrid cloud: "the cloud infrastructure is composed of two or more deployment models that remain unique entities, but are bound together by standardized or proprietary technology".[30]

After the main technical definitions and aspects of cloud computing, it is important to understand the legal framework for data protection in the EU and how it has evolved over time, before going deeper into the analysis of EU-U.S. data transfers though cloud infrastructures.

3. European Legal Framework for Data Protection

The rights to privacy and data protection are laid down in EU treaties (Article 16 of the Treaty on the Functioning of the European Union (TFEU)) and in Article 7 and 8 of the CFR, which became legally effective with the entry into force of the Lisbon Treaty in 2009. Moreover, the right to data protection is closely linked to the right to privacy or private life in Article 8 of the European Convention of Human Rights (ECHR).[31] On May 2018, a new legal framework on EU data protection, the GDPR,[32] entered into force and replaced the former Directive 95/46[33]

[24] *Mell / Grance* (2011), p. 3.
[25] Oracle: Infrastructure as a Service (IaaS) from Oracle, Retrieved June 17, 2019, from https://www.oracle.com/cloud/infrastructure.html#networking.
[26] Amazon: Was ist Cloud Computing, AWS, Retrieved from https://aws.amazon.com/de/what-is-cloud-computing/.
[27] *Mell / Grance* (2011), p. 3.
[28] Id.
[29] Id.
[30] Id.
[31] *European Data Protection Supervisor (EDPS)*: Data Protection, Retrieved June 17, 2019, from https://edps.europa.eu/data-protection/data-protection_en.
[32] 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, OJ 2119/1.
[33] 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 (DPD), [2016] OJ L281/31.

on data protection. To drive the analysis regarding the issue of transnational transfer of personal data it is important to understand the main aspects of GDPR relevant to the issue at hand:

According to Article 2 of the GDPR, "the regulation applies to the processing of personal data wholly or partly by automated means, and to the processing other than by automated means of personal data, which form part of a filing system or are intended to form part of a filing system".[34] Broadly speaking, if personal data is processed, the GDPR is applicable.

The term "processing" means "any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, and erasure or destruction".[35]

In order to fall within the scope of the regulation, there has to be personal data as defined in Article 4 (1) GDPR. "'Personal data' means any information relating to an identified or identifiable natural person".[36] This may include a name and surname, home address, an identification card number, cookies, physical characteristics, and medical diagnosis.[37]

With regard to data transfer and data processing in a cloud platform, the concept of data controller and processor plays also a crucial role to determine who is subject to the obligations under the GDPR. Apart from the first essential element in determining "who shall be responsible for compliance with data protection rules, and how data subjects can exercise their rights in practice"[38], the concept of controller plays also an important role "in determining which national law is applicable to a processing operation".[39]

According to Article 4 (7) of the GDPR controller "means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data".[40] In this regard, the first element of the

[34] Article 2 GDPR.
[35] Article 4 (2) GDPR.
[36] Article 4 (1) GDPR.
[37] *Hödl* in *Knyrim (2018)*, Der DatKomm, Art 4 DSGVO, para. 9.
[38] Article 29 Data Protection Working Party (2010): Opinion 1/2010 on the concepts of "controller" and "processor", 00264/10/EN WP 169, p. 2.
[39] Id., p. 5.
[40] Article 4 (7) GDPR.

definition, natural or legal person, public authority, agency or other body, means that the legal form of the controller is irrelevant for the application of the data protection obligations.[41]

The second element "alone or jointly with others" makes it clear that cases occur "where multiple actors interact in the processing of personal data"[42] and act as controllers. In that respect, the term "jointly" means "together with" or "not alone" in different forms and combinations. In assessing joint control, the Article 29 Working Party proposes "that a substantive and functional approach should be taken" and to focus "on whether the purposes and means are determined by more than one party".[43] Joint control may take different forms: multiple actors "may have a very close relationship (sharing, for example, all purposes and means of a processing) or a more loose relationship (for example, sharing only purposes or means, or a part thereof)".[44]

In order to assess the essential element "determines", the Article 29 Working Party created the following three categories[45]:

1) ***Control stemming from explicit legal competence*** *(when the controller or specific criteria for his nomination are designated by national or Community law).*
2) ***Control stemming from implicit competence*** *(for example, "the employer in relation to data on his employees" or "the publisher in relation to data on subscribers").*[46]
3) ***Control stemming from factual influence.*** *In this regard the capability to determine is assessed on factual circumstances. This involves for example contractual relations or the degree of actual control exercised by an actor).*[47]

Lastly, the term "purpose" is defined as "an anticipated outcome that is intended or that guides your planned actions". The term "means" is understood as "how a result is obtained or an end is achieved".[48]

In case of joint control, it is further noted that the controllers shall in a transparent manner by means of an arrangement determine their respective responsibilities for compliance with the

[41] WP 169, p. 15ff.
[42] Id., p. 17.
[43] Id., p. 18.
[44] Id., p. 19.
[45] Id., p. 10ff.
[46] Id., p.10.
[47] Id., p. 10ff.
[48] Id., p. 13.

obligations under the GDPR, in particular to make clear which controller is competent for which data subject's rights.[49] In order to ensure effective compensation of the data subject in case of joint control, Article 82 (4) of the GDPR stipulates that each controller shall be held liable for the entire damage.[50]

Finally, it is now to determine the role of the processor. According to Article 4 (8) of the GDPR "'processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller".[51] Two conditions have to be met for the qualifying as processor: (1) "being a separate legal entity with respect to the controller"; (2) "processing personal data on his behalf", which means serving someone else's interest. [52] Because it is the duty of the processor to implement the instructions by the controller, the "lawfulness of the processor's data processing activity is determined by the mandate given by the controller".[53] Therefore, a processor who goes beyond its mandate and determines "the purposes or the essential means of processing, is a (joint) controller rather than a processor". [54]

In order to ensure the standard of data protection in case of outsourcing and delegation, the controller and the processor have to conclude a written contract, "providing sufficient guarantees to implement appropriate technical and organisational measures" for an adequate protection of data subject's rights.[55]

Having introduced the concept of data controller and processor above, it is now to determine who is controller and processor in the context of a cloud computing constellation. In general, the user of the cloud service acts as the controller, because he makes the final decision on the purpose of the processing of personal data and the choice to outsource or delegate the processing of data to an external organisation. Therefore, the cloud user bears the responsibility for the compliance with the data protection regulations and the liability for any damages resulting from unlawful processing.[56] On the other hand, the cloud service provider, who allocates the infrastructure, is qualified as the processor, when processing the personal data on behalf of the cloud user. However, the qualification as processor or (joint) controller should be assessed on a case-by-case basis. It is also entirely possible, that the cloud service provider acts

[49] Article 26 GDPR.
[50] Article 82 (4) GDPR.
[51] Article 4 (8) GDPR.
[52] WP 169., p. 25.
[53] Id, p. 25.
[54] Id.
[55] Article 28 GDPR.
[56] *Raffling* / *Schock* (2018), p. 48.

as a joint controller, when the provider acquires a relevant role in determining the purpose or essential means of processing. Moreover, if a cloud service provider processes and utilises the data for its own purposes, he may act as a separate controller.[57]

With regard to the territorial scope of the GDPR, Article 3 (1) says that the "regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not".[58] According to recital 22 of the GDPR, it applies regardless of whether or not the processing itself takes place within the EU.[59] This is especially relevant, in cases where the location of cloud infrastructures are outside the EU.

Further, the GDPR is applicable pursuant to Article 3 (2):

> *"to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:*
>
> > *(a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or*
> >
> > *(b) the monitoring of their behaviour as far as their behaviour takes place within the Union."*[60]

Because Article 3 (2) effects equally the controller and the processor, the GDPR is also applicable to processors without establishment in the EU, who offer cloud services to controller in the EU.[61] Recital 22 suggests certain "factors such as the use of a language or a currency generally used in one or more Member States with the possibility of ordering goods and services in that other language, or the mentioning of customers or users who are in the Union," that "make it apparent that the controller envisages offering goods or services to data subjects in the Union".[62]

---

[57] *Voigt, Paul / Von dem Bussche*, Axel (2018): EU-Datenschutz-Grundverordnung (DSGVO). Praktikerhandbuch unter vollständiger Berücksichtigung des DSAnpUG-EU, Springer 2018, p. 315.
[58] Article 3 (1) GDPR.
[59] Recital 22 of the GDPR.
[60] Article 3 (2) GDPR.
[61] *Feiler, Lukas / Forgó, Nikolaus* (2017): EU-DSGVO: EU-Datenschutz-Grundverordnung, Kurzkommentar, Verlag Österreich 2017, p. 60.
[62] Recital 22 of the GDPR.

Third, the European data protection regulations apply to data processing outside the EU, where by virtue of public international law, the GDPR applies.[63] In conclusion, for the application of the GDPR it is not necessary that the cloud service provider or the data controller have to be established in the EU.

3.1. International Transfers of Personal Data

In light of the legal framework for data protection established by the European Union, the challenges of globalisation and cross-border business relationships become immanent. As introduced at the beginning, there is an ongoing trend to store or transfer data through the Cloud and as a consequence, service are outsourced to external cloud providers located outside the EU. In order to analyse EU-U.S. data transfers through clouds, certain conditions for the international data transfer have to be met.

The first precondition for the transfer of personal data to a third country (cross-border transfers), that is outside of the European Economic Area, is that the data processing is GDPR compliant (requirements under Articles 5 ff.) and would be permissible within the EU. In particular, the principles of data processing set out in Article 5 need to be fulfilled, all processing must be based on a legal permission pursuant to Articles 6, 9 or 10 (consent, performance of a contract, legal responsibility or explicit consent when sensitive data is affected) and personal data must be protected against unauthorised or unlawful processing.[64]

In a second step, the cross-border data transfer hast to meet further requirements set out in Articles 44 ff. The purpose of these additional requirements is to ensure an adequate level of data protection in the third country and that the level of protection to data subjects, as guaranteed throughout the Union, should not be undermined, "when personal data is transferred from the Union to controllers, processors or other recipients in third countries".[65] In order to guarantee an adequate level of data protection in the third country the GDPR stipulates the use of special safeguards such as adequacy decisions, SCCs adopted by the Commission, binding corporate rules (BCR), approved certifications mechanism and code of conducts.[66] Only if the two cumulative conditions above are met, the transfer of personal data to a third country is

[63] Article 3 (3) GDPR.
[64] *Graf, Ferdinand / Križanac, Marija* (2017): GDPR compliance. Sonderheft Datenschutz-Grundverordnung, ecolex 9a/2017, p. 945ff.
[65] Recital 101 of the GDPR.
[66] *European Commission* (2018, July): Rules on international data transfers, Retrieved June 17, 2019, from https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/rules-international-transfers-personal-data_en.

permitted under the GDPR. These mechanisms described will be examined now in more detail:

3.1.1. Adequacy Decision

On the basis of Article 45 of the GDPR, the European Commission can decide whether a country outside the EU offers an adequate level of protection for EU citizens.[67] As a result of such an "adequacy decision", personal data can be transferred to a third country without any further safeguards or specific authorisation. So far, the Commission has adopted adequacy decisions for Andorra, Argentina, Canada, Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland, Uruguay and the USA.[68]

3.1.2. Standard Contractual Clauses (SCC)

Besides adequacy decisions, SCCs represent another essential and popular safeguard under the GDPR for international data transfer. Pursuant to Article 46 (2) lit. c and d of the GDPR, the data exporter and the data recipient abroad can conclude such SCCs. When contractual partners use SCCs, it only means that the data recipient has guaranteed an adequate level of data protection. It does not imply that the third country is assumed to be a "safe data protection" country.[69]

Pursuant to Article 46 (5) of the GDPR, "decisions adopted by the Commission on the basis of Article 26(4) of Directive 95/46/EC shall remain in force until amended, replaced, or repealed".[70] The European Commission has so far issued two sets of SCCs for data transfers from data controllers in the EU to data controllers established outside the EU or EEA (decision 2001/497/EC [71] and decision 2004/915/EC [72]), and "one set of contractual clauses for data transfers from European controllers to processors established outside the EU or EEA" [73]

---

[67] *European Commission* (a): Adequacy decisions, Retrieved June 17, 2019, from https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en.
[68] Id.
[69] *Voigt / Von dem Bussche* (2018), p. 159.
[70] Article 46 (5) GDPR.
[71] 2001/497/EC: Commission Decision of 15 June 2001 on standard contractual clauses for the transfer of personal data to third countries, under Directive 95/46/EC, OJ L 181, 4.7.2001.
[72] 2004/915/EC: Commission Decision of 27 December 2004 amending Decision 2001/497/EC as regards the introduction of an alternative set of standard contractual clauses for the transfer of personal data to third countries, OJ L 385, 29.12.2004.
[73] *European Commission* (e): Standard Contractual Clauses (SCC), Retrieved June 17, 2019, from https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/model-contracts-transfer-personal-data-third-countries_en.

(decision 2010/87/EU [74]).

3.1.3. Binding Corporate Rules (BCR)

Another alternative to providing appropriate safeguards may be to use BCRs, pursuant to Article 46 (2) lit. b and 47 GDPR. Binding corporate rules are internal rules, like a code of conduct, for data transfers within multinational companies. The competent supervisory authority must approve the BCR before it can be used among the multinational corporations. These rules constitute a sufficient guarantee for the transfer of personal data, "within the same corporate group", to companies in other "countries that do not provide an adequate level of protection".[75]

Binding corporate rules have to fulfil minimum requirements pursuant to Article 47 (1) and (2) GDPR. They have to specify the application of general privacy principles (such as the purpose limitation, data security, and data minimisation), tools of effectiveness (complaint handling systems), and the proof that the BCR are legally binding, both internally and externally.[76]

So far, approximately 130 companies have successfully applied for approval of their BCRs.[77] The procedure of approval by the competent supervisory authority is costly in terms of time and money.[78]

In the absence of an adequacy decision or of other appropriate safeguards pursuant to Article 46 of the GDPR, cross-border data transfers are only permitted when the data subject has explicitly consented to the proposed transfer.[79]

After the overview of the European legislation governing data protection and privacy, the next section explains how the legislation interacts with different legal systems - specifically the U.S. - with regard to the issue of personal data transfer and its protection in the context of cloud

[74] 2010/87/: Commission Decision of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council, OJ L 39, 12.2.2010.
[75] *European Commission* (c): Binding Corporate Rules (BCR), Retrieved June 17, 2019, from https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/binding-corporate-rules-bcr_en#bindingcorporaterules.
[76] Article 47 (2) GDPR.
[77] *European Commission* (b): BCR overview until 25th May - List of companies for which the EU BCR cooperation procedure is closed, Retrieved June 17, 2019, from https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/binding-corporate-rules-bcr_en#approval-of-binding-corporate-rules.
[78] *Voigt / Von dem Bussche* (2018), p. 171.
[79] Article 49 (1) GDPR.

computing.

4. EU-U.S. data transfers

The U.S. is one of the most important economic and political partners for the EU and an undeniable driver in technological innovation. Therefore, the interaction of their legal system and the transatlantic relationship in general are of particular interest. With respect to the transatlantic data flow, on 12 July 2016 the European Commission adopted the adequate decision on the EU-U.S. Privacy Shield,[80] which replaced the former Safe Harbour framework.[81] The following overview of the Privacy Shield is of particular interest for U.S. cloud service providers, who participated in this framework.

The Privacy Shield framework is based on specific representations and assurances made by the U.S. government and consists of the Commission's decision itself and seven Annexes.[82] The Privacy Shield framework includes two Arbitral Models, the EU-U.S. Privacy Shield Principles, and the EU-U.S. Privacy Shield Ombudsperson Mechanism. It also includes the FTC's 2015 Privacy & Data Security Update, several letters from people such as the former Under Secretary for International Trade Stefan Selig, the former U.S. Secretary of State John Kerry, the former Federal Trade Commission Chairwoman Edith Ramirez, as well as letters from the Office of the Director of National Intelligence (DNI), and the U.S. Department of Justice (DoJ).[83] The Privacy Shield is administered by the International Trade Administration (ITA) within the U.S. Department of Commerce (DoC), and like the former Safe Harbour agreement is based on a voluntarily self-certification mechanism.[84]

In order to participate in the Privacy Shield Framework, a U.S.-based organisation has to self-certify its adherence to the Privacy Shield Principles to the DoC, and publicly commit to comply with the Framework's requirements.[85] Once it joins the Privacy Shield program, the

[80] Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield (notified under document C(2016) 4176) [2016], OJ L 207/1.
[81] 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 safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce (notified under doc.no. C(2000) 2441) [2000], OJ L 215/7.
[82] *Georgieva*, *Ludmilla* (2017): EU-US-Privacy Shield - eine Gesamtbetrachtung, in Baumgartner, Gerhard (Hrsg.): Öffentliches Recht. Jahrbuch 2017, p. 217.
[83] C(2016) 4176.
[84] *The International Trade Administration (a)*, U.S. Department of Commerce: Privacy Shield Program Overview, Retrieved June 17, 2019, from https://www.privacyshield.gov/Program-Overview.
[85] *The International Trade* Administration *(b),* U.S. Department of Commerce: The EU-U.S. and Swiss-U.S. Privacy Shield Frameworks, Retrieved June 17, 2019, from https://www.privacyshield.gov/servlet/servlet.FileDownload?file=015t0000000QJdg.

commitment becomes enforceable under U.S. law by the U.S. Federal Trade Commission (FTC) or the U.S. Department of Transportation (DOT).[86] The organisation has to renew its self-certification annually in order to stay in the Privacy Shield program.[87]

There are seven main EU-U.S. Privacy Shield Principles that govern the data protection are as follows:

(1) ***Notice*** – The self-certified organisations have to provide the individuals with certain information such as types of personal data collected, the purposes for which they collect and use information, and how to contact the organisation with any inquiries or complaints. The organisations are also obliged to inform the individuals about the "independent dispute resolution body designated to address complaints".[88]

(2) ***Choice*** - An organisation "must offer individuals the opportunity to opt out of whether their personal information is to be disclosed to a third party or to be used for a purpose that is materially different from the purpose(s) for which it was originally collected".[89]

(3) ***Accountability for onward transfer*** – When dealing with third-party controllers, organisations must enter into a contract that provides specific requirements regarding the data protection of the individuals.[90]

(4) ***Security*** – Organisations are obliged to "take reasonable and appropriate measures to protect personal information from loss, misuse, unauthorised access, disclosure, alteration, and destruction".[91]

(5) ***Data Integrity and Purpose Limitation*** - Personal information "must be limited to the information that is relevant for the purposes of processing", and "organisations must take reasonable steps to ensure that personal data is reliable for its intended use, accurate, complete, and current".[92]

(6) ***Access*** – Organisations have to give individuals access to the personal data the organisation holds on them. Individuals have to be "able to correct, amend, or delete inaccurate information".[93]

(7) ***Recourse, Enforcement and Liability*** – Organisations have to ensure robust

[86] *The International Trade Administration (c)*, U.S. Department of Commerce: How to Join Privacy Shield (part 1), Retrieved June 17, 2019, from https://www.privacyshield.gov/article?id=How-to-Join-Privacy-Shield-part-1.
[87] The list of all registered US organisations is available on the website www.privacyshield.gov/list. Currently, over 4,600 organisations have joined the Privacy Shield Framework, Retrieved June 17, 2019.
[88] C(2016) 4176, Annex II. Principle 1.
[89] C(2016) 4176, Annex II. Principle 2.
[90] C(2016) 4176, Annex II. Principle 3.
[91] C(2016) 4176, Annex II. Principle 4.
[92] C(2016) 4176, Annex II. Principle 5.
[93] C(2016) 4176, Annex II. Principle 6.

> mechanisms for assuring compliance with the Principles, which includes an independent recourse mechanism for individual's complaints, and follow-up procedures for verifying that an organisation's claims about its privacy practices are true.[94]

In contrast to the Safe Harbour Decision, the European Commission is obliged to review the arrangement on an annual basis to assess if the level of data protection remains adequate.[95] The first annual report of the Commission suggested recommendations to improve the functioning of the Privacy Shield. The recommendations included for example a more proactive and regular search for false claims and "an ongoing monitoring of compliance with the Privacy Shield principles by the DoC".[96] Furthermore, it suggested the prompt appointment of a permanent Ombudsperson and the improving of the cooperation between the DoC and the DPAs.[97] In November 2017, the Article 29 Data Protection Working Party released a report that identified a number of important unresolved issues.[98] Overall, the Commission concluded in its first annual review that the U.S. continues "to ensure an adequate level of protection for personal data transfers under the Privacy Shield".[99]

Also, after the second annual review the European Commission found that an adequate level of protection is provided under the Privacy Shield. The implementation of the Commission's recommendations after the first annual review have improved aspects of the practical functioning of the Privacy Shield framework.[100] In particular, the DoC has improved the certification process and its monitoring and proactive oversight mechanisms. Regarding the monitoring mechanism, the DoC has implemented "spot checks, by which it randomly selects companies to verify their compliance with the obligation under the Privacy Shield".[101]

However, the Commissions is still awaiting the nomination of a permanent Ombudsperson and expressed concerns, among others, on the effectiveness of the handling and resolution of

---

[94] C(2016) 4176, Annex II. Principle 7.
[95] *European Commission* (d): EU-US data transfers, Retrieved June 17, 2019, from https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/eu-us-data-transfers_en.
[96] *European Commission* (2017): Report From The Commission To The European Parliament And The Council On The First Annual Review Of The Functioning Of The EU-U.S. Privacy Shield, SWD 611 final, p. 4ff.
[97] Id., p. 4ff.
[98] Article 29 Data Protection Working Party (2017): EU-U.S. Privacy Shield – First annual Joint Review, 17/EN WP 255.
[99] *European Commission* (2017), p. 4.
[100] *European Commission* (2018a), Report From The Commission To The European Parliament And The Council On The Second Annual Review Of The Functioning Of The EU.U.S. Privacy Shield, COM 860 final, p. 5.
[101] *European Commission* (2018b), COMMISSION STAFF WORKING DOCUMENT Accompanying The Document REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL On The Second Annual Review Of The Functioning Of The EU.U.S. Privacy Shield, SWD 497 final, p. 4ff.

complaints by the Ombudsperson. In this regard, the European Data Protection Board (EDPB) concluded in its report that the Ombudsperson cannot be considered as an effective remedy before a tribunal pursuant to Article 47 of the CFR. Currently Manisha Singh is acting under the Secretary of State for Economic Growth, Energy, and the Environment, as the Privacy Shield Ombudsperson. Nevertheless, as the EDPB stated in its report, the Ombudsperson is lacking "sufficient powers to access information and to remedy non-compliance".[102] Therefore, the EDPB recalls that a permanent independent Ombudsperson should be designated.[103]

Moreover, the EDPB expressed concerns on the lack of substantial checks performed by the DoC, because the checks do not go into substance of the Privacy Shield principles. Further concerns are the application of the Privacy Shield requirements regarding onward transfers and the recertification process.[104] With regard to collection and access of personal data for national security purposes under Section 702 of FISA and EO 12333, the EDPB encouraged the PCLOB to issue follow-up reports on PPD-28 and Section 702 FISA. Finally, the EDPB concluded that the reauthorization of Section 702 FISA did not contain any new guarantees for EU individuals.[105]

4.1. Schrems 1.0 - From Safe Harbour to Privacy Shield

It is important to understand, how and why the Privacy Shield emerged in order to truly grasp the magnitude of its potential consequences for the protection of EU data subjects, when using cloud services from U.S. providers. By analysing the cases Schrems 1.0 and 2.0 in more detail, the legal complexity of adapting to modern technologies and ensuring an adequate level of the data protection for EU citizens shall be illustrated.

In 2013, Edward Snowden revealed that "internet and telecommunications systems, operated by some of the world's largest technology companies" [106] such as Microsoft, Apple, and Facebook, were the subject of surveillance programmes run by the U.S. National Security

[102] *European Data Protection Board* (2019): EU-U.S. Privacy Shield – Second Annual Joint Review, p. 7, Retrieved June 17, 2019, from https://edpb.europa.eu/our-work-tools/our-documents/other/eu-us-privacy-shield-second-annual-joint-review-report-22012019_de.
[103] Id., p. 19.
[104] Id., p. 7.
[105] Id., p. 6.
[106] Judgement of Ms. Justice Costello, The High Court, Commercial, 2016, No. 4809 P., *The Data Protection Commissioner v Facebook Ireland and Maximillian Schrems*, 3 October 2017, p. 31, Retrieved June 17, 2019, from https://www.dataprotection.ie/sites/default/files/uploads/2018-12/High%20Court%20Judgment_03_10_2017.pdf.

Agency (NSA).[107]

Due to these revelations of the mass surveillance programmes, known as the PRISM and Upstream collections, Maximilian Schrems lodged a complaint with the Irish Data Protection Authority (DPA). In his complaint, he claimed that the transfer of personal data of all European Facebook subscribers to servers in the U.S.A. were not subject to adequate data protection, because the U.S. law and practice did not guarantee a protection equivalent to that provided by European regulations.[108]

It was in October 2015 then, when the Court of Justice of the European Union declared that the former Safe Harbour agreement was invalid, because it did not guarantee an adequate level of data protection for EU citizens.[109] The Grand Chamber of the CJEU made the following key points, which lead to the decision invalidating the Safe Harbour:

- The Commission is obliged to assess if the applicable rules in the third country resulting from its domestic law and practice ensures an adequate level of protection which is guaranteed in the EU legal order.[110]
- The requirements stemming from Article 25 (6) of Directive 95/46 should be read in the light of Articles 7 (the right to respect for private life), Article 8 (the right to the protection of personal data), and Article 47 (the right to effective judicial protection) of the CFR.[111]
- A self-certification system is not contrary to the requirement pursuant to Article 25 of Directive 95/46, as long as the third country ensures that there are "effective detection and supervision mechanisms" that can capture "any infringements of rules ensuring the protection of fundamental rights".[112] In this regard, it was a serious problem that the Safe Harbour principles were only applicable to self-certified U.S. organisations, but not to U.S. public authorities.[113]
- The adequacy decision enables interference with the fundamental rights of the persons whose personal data is transferred on grounds of national security and public interest

[107] Judgement of Ms. Costello, The High Court, Commercial, 2016, No. 4809 P, p. 31.
[108] *European Parliamentary Research Service* (2018): The Privacy Shield. Update on the state of play of the EU-US data transfer rules, PE 625.151, p. 3, Retrieved June 17, 2019, from http://www.europarl.europa.eu/RegData/etudes/IDAN/2018/625151/EPRS_IDA(2018)625151_EN.pdf.
[109] Case C–362/14 *Maximilian Schrems v Data Protection Commissioner* (2015), ECLI:EU:C:2015:650.
[110] C-362/14, para. 73-75.
[111] C-362/14, para. 67-95.
[112] C-362/14, para. 81.
[113] C-362/14, para. 82.

requirements, or pursuant to U.S. law.[114] Thus, the "national security, public interest, or law enforcement requirements have primacy over the safe harbour principles".[115] Broadly speaking, the Safe Harbour agreement lacked guarantees that interference with fundamental rights would be limited to instances where it was strictly necessary.[116]

- The Safe Harbour Agreement lacked effective legal protection against interference with fundamental rights.[117]
- National DPAs have the power to investigate into EU-U.S. data transfers, and such power is not precluded by an adequacy decision of the European Commission.[118]
- Furthermore, the CJEU declared that "legislation permitting the public authorities to have access on a generalised basis to the content of electronic communications" is incompatible with the "fundamental right to respect for private life, as guaranteed by Article 7 of the Charter".[119]

The CJEU's ruling had an immense impact on the legitimacy of the transatlantic data flow, taking into account that approximately 4,500 U.S. companies were using the Safe Harbour agreement as a legal basis for the EU-U.S. data transfer.[120]

4.2. Schrems 2.0

As a result of the invalidation of the Safe Harbour agreement, Schrems reformulated his complaint and the Irish DPC started its investigation into Schrems' original complaint.[121] The focus of the continued proceedings was an evaluation of third country law, in this case U.S. law.

In Schrems 2.0, Facebook, Inc. relied on the SCC decision of Commission 2010/877EU, to legitimise the personal data transfer of the Facebook subscribers to the U.S.[122] In his reformulated complaint, Schrems alleged that his personal data was processed in the USA due to the data sharing agreement between Facebook Ireland Ltd. and its American parent company,

---

[114] C-362/14, para. 87.
[115] C-362/14, para. 86.
[116] EPRS (2017): From Safe Harbour to Privacy Shield. Advances and shortcomings of the new EU-US data transfer rules, PE 595.892, p. 9, Retrieved June 17, 2019, from http://www.europarl.europa.eu/RegData/etudes/IDAN/2017/595892/EPRS_IDA(2017)595892_EN.pdf.
[117] C-362/14, para. 89.
[118] EPRS (2018), p. 4.
[119] C-362/14, para. 94.
[120] *Weiss, Martin A. / Archick, Kristin* (2016): U.S.-EU Data Privacy: From Safe Harbour to Privacy Shield, p. 3, Retrieved June 17, 2019, from https://epic.org/crs/R44257.pdf.
[121] Judgement of Ms. Costello, The High Court, Commercial, 2016, No. 4809 P, p. 34.
[122] Id., p. 35.

Facebook, Inc. The parent company was obliged by secret laws, rules, court decisions, and executive orders to disclose his personal data to U.S. authorities such as the NSA and the Federal Bureau of Investigations (FBI).[123] Moreover, Schrems said that there was no appropriate judicial remedy to complain against the legitimacy of his data being processed. In conclusion, Schrems stated that the PRISM program infringed Article 7 and 47 of the CFR, and the DPC should take all steps to suspend the data flow.[124]

As a result of the investigation, the DPC concluded in her draft decision on 24 May 2016 that the SCC did not provide sufficient protection to EU citizens. Due to well-founded concerns about U.S. law, the SCC did not ensure that data transfers to the U.S. enjoyed the same high level of protection as they did in the EU.[125] With regard to breaches of data protection rights, the DPC said that there was no effective remedy under U.S. federal law available to EU citizens that was compatible with the requirements of Article 47 of the CFR.[126]

Additionally, the DPC believed that it had no authority to suspend the transfers of data to the U.S. on her own and referred the case to the Irish High Court, with the expectation that the court would make a reference for a preliminary ruling to the CJEU, regarding the validity of the SCC decisions.[127] Before the questions were referred for preliminary ruling[128] to the CJEU, five experts gave evidence to the Irish Commercial High Court on U.S. law and practice.[129]

Maximilian Schrems submitted an expert report to the Irish High Court from an attorney from the American Civil Liberties Union, Ashley Gorski. The focus of Gorski's testimony was on the most significant U.S. government surveillance regulations, Section 702 of the Foreign Intelligence Surveillance Act (FISA), Executive Order (EO) 12333, and the Presidential Policy Directive 28 (PPD-28). [130]

Facebook Ireland Ltd. selected two experts, Professor Stephen I. Vladeck from the University of Texas and Professor Peter Swire from the Georgia Institute of Technology to provide

---

[123] Judgement of Ms. Costello, The High Court, Commercial, 2016, No. 4809 P, p. 34.
[124] Id., p. 36.
[125] Id., p. 78.
[126] Id., p. 38.
[127] *Matheson, Lee* (2017, October 3): Understanding 'Schrems 2.0', Retrieved June 17, 2019, from https://iapp.org/news/a/understanding-schrems-2-0/.
[128] Case C-311/18 *Reference for a preliminary ruling from the High Court (Ireland) made on 9 May 2018 — Data Protection Commissioner v Facebook Ireland Limited, Maximillian Schrems*, OJ C 249, 16.7.2018.
[129] Judgement of Ms. Costello, The High Court, Commercial, 2016, No. 4809 P, p. 85.
[130] *Gorski, Ashley* (2016): The Data Protection Commissioner and Facebook Ireland Limited and Maximillian Schrems, Expert Report of Ashley Gorski on behalf of the second named defendant, p. 4, Retrieved June 17, 2019, from https://iapp.org/media/pdf/resource_center/Schrems-testimony-Gorski.pdf.

testimony regarding U.S. law. Unfortunately, the testimonies of the two experts enlisted by the Irish DPC were not published.[131] The key aspects of Swire's expert opinion were the systemic safeguards in U.S. law and practice, individual remedies in U.S. privacy law, the existence of the Foreign Intelligence Surveillance Court (FISC) as an independent and effective oversight board over U.S. government surveillance, and the implications of an inadequacy finding for SCCs.[132]

In the expert opinion of Professor Vladeck, the author stated that the DPC Draft Decision's analysis gave an inaccurate picture of the U.S. protections and remedies available to EU citizens. Therefore, his expert report outlined the current U.S. data collection authorities relevant to the data of EU citizens held by U.S. companies, and the oversight mechanisms.[133]

After having elaborated the background of the legal framework for transatlantic data flows, it is important to first understand the basics of the legal framework in the U.S. governing surveillance before analysing the legal data protection and privacy mechanisms in place in the light of the Schrems 2.0.

5. Legal framework in the U.S.

Before going into detail on the legal basis for U.S. surveillance programmes, a brief overview of the constitutional framework in the U.S. regarding data protection is necessary. The constitutional framework, as interpreted by the U.S. Supreme Court, is essential for the protection of personal data against government access and intelligence surveillance.[134] The Fourth Amendment to the US Constitution states as follows:

> *"The right of the people to be secure in 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*

[131] *International Association of Privacy Professional:* Schrems 2.0: Expert Testimony, Retrieved June 17, 2019, from https://iapp.org/resources/article/schrems-2-0-expert-testimony/.
[132] *Swire, Peter* (2016, November 3): The Data Protection Commissioner and Facebook Ireland Limited and Maximillian Schrems, Affidavit of Peter Swire, Table of Contents, p. i, Retrieved June 17, 2019, from https://iapp.org/media/pdf/resource_center/Schrems-testimony-Swire.pdf.
[133] *Vladeck, Stephen* (2016, November 2): The Data Protection Commissioner and Facebook Ireland Limited and Maximillian Schrems, Affidavit of Stephen I. Vladeck, p. 3, Retrieved June 17, 2019, from https://iapp.org/media/pdf/resource_center/Schrems-testimony-Vladeck.pdf.
[134] *Council of the European Union* (2013): Report on the findings by the EU Co-chairs of the ad hoc EU-US Working Group on Data Protection, 16987/13, p. 4, Retrieved June 17, 2019, from https://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/jha/139745.pdf.

describing the place to be searched, and the persons or things to be seized."[135]

However, only U.S. nationals and non-U.S. citizens residing within the U.S. are subject to this protection under the Fourth Amendment.[136] According to the Supreme Court's ruling in *United States v. Verdugo-Urquidez*, non-U.S. citizens "only receive constitutional protections when they have come within the territory of the United States" and "voluntarily developed substantial connections to the United States".[137] Therefore, the Fourth Amendment will not play an important role for EU citizens when their data is held by U.S. companies, because it is very unlikely that EU citizens have voluntarily developed substantial connections to the United States.[138]

In contrast to the comprehensive data protection law in the EU, data protection regulations in the United States are sector-specific and arise out of particular occasions. Examples of sector-specific U.S. data protection law include the 1988 Video Privacy Protection Act, the 1971 Fair Credit Reporting Act, or the 1998 Children Online Privacy Protection Act.[139]

As a result of these sector-specific data protection regulations, the U.S. system is characterised by the basic principle that surveillance is legal unless forbidden.[140] This means that the U.S. system is based on the principle of "permission with the reservation of prohibitions" ("opt-out"), in contrast to the in the EU governing principle of "prohibition with the reservation of permission" ("opt-in").[141]

5.1. Legal framework governing U.S. government surveillance

One of the most important legal issues in the analysis of cloud computing and EU-U.S. data transfers, are the surveillance and retention of data by the U.S. intelligence agencies. Therefore, the main legal bases for the collection of personal data by U.S. intelligence agencies have to be introduced and are as follows:

---

[135] Fourth Amendment to the United States Constitution, Retrieved June 17, 2019, from https://www.govinfo.gov/content/pkg/GPO-CONAN-1992/pdf/GPO-CONAN-1992-10-5.pdf.
[136] *Council of the European Union* (2013), 16987/13, p. 4.
[137] *United States v. Verdugo-Urquidez*, No. 88-1353, 494 U.S. 259 (1990), Retrieved June 17, 2019, from https://supreme.justia.com/cases/federal/us/494/259/.
[138] *Vladeck* (2016, November 2), p. 16.
[139] *Wissenschaftliche Dienste. Deutscher Bundestag* (2015): Datenschutzrecht der Europäischen Union, Deutschlands und der USA, WD 3 – 3000 – 064/15, p. 10f., Retrieved June 17, 2019, from https://www.bundestag.de/resource/blob/409136/df3683ab30663377d240a9074e92c63f/wd-3-064-15-pdf-data.pdf.
[140] Judgement of Ms. Costello, The High Court, Commercial, 2016, No. 4809 P, p. 99.
[141] *Ludmilla Georgieva*, EU-US-Privacy Shield - eine Gesamtbetrachtung, in Baumgartner (Hrsg), Öffentliches Recht. Jahrbuch 2017 (2017), p. 216.

- **Section 702 of the FISA** (as amended by the 2008 FISA Amendments Act, 50 U.S.C. § 1881a),
- **Section 215 of the USA PATRIOT Act 2001** (which also amended FISA, 50 U.S.C. 1861), and
- **Executive Order (EO) 12333**.[142]

5.2. FISA

In 1978, the U.S. Congress enacted FISA, due to a series of surveillance abuses by U.S. intelligence agencies during the 1960s and 1970s.[143] The FISA created the Foreign Intelligence Surveillance Court (FISC), that has the exclusive jurisdiction to issue orders for all foreign-intelligence surveillances carried out on U.S. soil.[144] In addition, the FISC exercises judicial oversight over intelligence activities. The Foreign Intelligence Surveillance Court of Review (FISCR), and the U.S. Supreme Court may review the FISC's decisions.[145] As part of the judicial branch, the FISC is independent of who executive branch and the intelligence agencies.[146] The FISC is composed of 11 judges "which are selected from the federal district courts by the Chief Justice of the U.S. Supreme Court".[147] The FISC's federal judges serve for one term lasting seven years.[148]

There are two types of surveillance authorisations under the FISA, the so-called traditional FISA orders and the conducted surveillances under Section 702 of FISA.[149]

In order to obtain permission to conduct electronic surveillance on U.S. soil, the government has to obtain an individualised FISA order from the FISC. For this purpose, the government has to demonstrate to the FISC that, among other things, there is "probable cause to believe that the target of the electronic surveillance is a foreign power or an agent of a foreign power", and "each of the facilities or places at which the electronic surveillance is directed is being used, or is about to be used, by a foreign power or an agent of a foreign power".[150] The terms "foreign power or an agent of a foreign power" broadly include foreign governments whether or not

[142] *Council of the European Union* (2013), 16987/13, p. 4 ff.
[143] *Vladeck* (2016, November 2), p. 4.
[144] *Swire* (2016, November 3), Chapter 1, p. 9.
[145] *United States Foreign Intelligence Surveillance Court* (2018)*:* United States Foreign Intelligence Surveillance Court of Review, Retrieved June 17, 2019, from https://www.fisc.uscourts.gov/FISCR.
[146] *Swire* (2016, November 3), Chapter 3, p. 12.
[147] *Vladeck* (2016, November 2), p. 7.
[148] *Swire* (2016, November 3), Chapter 3, p. 12.
[149] *Gorski* (2016), p. 4.
[150] Id*.,* p. 5ff.

recognised by the U.S., international terrorist groups, people who engage in international proliferation of weapons of mass destruction, or in international terrorism, or in preparatory activities for terrorism.[151]

According to the Vladeck's opinion, there is no requirement that the targeted person should receive notice of the FISA-authorized surveillance, unless the government seeks to introduce evidence derived from the search in a criminal prosecution of the target.[152]

Pursuant to Section 702 of FISA, the Attorney General and the DNI may jointly authorize, "for a period of up to 1 year from the effective date of the authorisation, the targeting of persons reasonably believed to be located outside the United States, in order to acquire foreign intelligence information".[153]

Because this authorisation allows for the collection of information from non-U.S. persons, Section 702 FISA is of particular importance regarding the protection of personal data of EU citizens.[154] In this regard, a non-U.S. person is defined "as an individual who is neither a citizen nor a lawful permanent resident of the USA".[155]

In contrast to traditional FISA orders, surveillance conducted under Section 702 of FISA does not require individualized judicial authorisation. In order to authorise the government to acquire foreign intelligence information under Section 702, the Attorney General and the DNI have to submit annual certifications to the FISC for approval. It is not necessary to specify the targeted non-U.S. person to the FISC.[156] In addition, the certifications do not require the "identification of the specific facilities, places, premises, or property at which an acquisition authorised under Section 702 will be directed or conducted".[157] Unlike traditional FISA orders, there is also "no requirement that the government" has to "demonstrate probable cause to believe that an individual targeted is an agent of a foreign power".[158] The only limitation on the government's authority under Section 702 is that intentional targeting of U.S. persons or acquisition of "any

---

[151] *Vladeck* (2016, November 2), p. 6ff.
[152] Id., p. 6.
[153] Section 702 of the Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008, Pub. L. 110-261 (codified in scattered sections of 50 U.S.C.). Retrieved June 17, 2019, from https://www.congress.gov/110/plaws/publ261/PLAW-110publ261.pdf.
[154] *Council of the European Union* (2013), 16987/13, p. 5.
[155] *Privacy and Civil Liberties Oversight Board* (2014): Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act, p. 81, Retrieved June 17, 2019, from https://www.pclob.gov/library/702-Report.pdf.
[156] PCLOB Report (2014), p. 6.
[157] 50 U.S.C. § 1881a(h)(4).
[158] PCLOB Report (2014), p. 6.

communication as to which the sender and all intended recipients known at the time of acquisition to be located in the U.S." is forbidden.[159]

Furthermore, an authorisation under Section 702 requires that the Attorney General, in consultation with the DNI, has adopted specific "targeting" and "minimisation" procedures.[160] The purpose of these procedures is to limit the incidental and inadvertent collection, retention, and dissemination of personal data of U.S. persons. Apart from approving the government's annual certifications, the FISC must confirm that these procedures comply with Section 702 FISA and the Fourth Amendment of U.S. Constitution.[161] As mentioned above, non-U.S. persons located outside of the US are not protected by the Fourth Amendment.

After the FISC approves the certifications, the government sends written directives to an electronic communication service provider to "provide the government with all information, facilities, or assistance necessary to accomplish the acquisition".[162] These directives can be challenged by the companies before the FISC, on grounds of procedure or practical effects (disproportionate burden). The FISC's decision can be appealed to the FISA Court of Review. However, during the FISC proceedings, the interests of the data subject are not represented.[163]

The information obtained from the provider can comprise different kinds of personal information such as "emails, photographs, audio and video calls, messages, documents, and internet browsing history". Collection methods can include "wiretaps and other forms of interception of electronically stored data and data in transmission". [164]

Overall, it is apparent that the FISC does not play a meaningful role in authorising section 702 surveillances, because its role mainly consists of reviewing the "targeting" and "minimisation" procedures.[165]

According to Gorski's report, an authorisation under Section 702 FISA means that the government can "warrantlessly monitor communications between people inside the United States and non-U.S. persons abroad".[166] The only conditions for the authorisation to monitor communications are that "at least one party to a phone call or internet communication is a

[159] 50 U.S.C. § 1881a(b)(4).
[160] *Vladeck* (2016, November 2), p. 12.
[161] Id., p. 12.
[162] 50 U.S.C. § 1881a(i)(1)
[163] *Council of the European Union* (2013), 16987/13, p. 25.
[164] Id., p. 5.
[165] *Gorski* (2016), p. 6.
[166] Id.

non-U.S person abroad", and that the acquisition's "significant purpose" is "foreign intelligence" collection".[167]

In contrast, the US Privacy and Civil Liberties Oversight Board (PCLOB) explained in its July 2nd 2014 report that acquisitions under Section 702 are "not based on the indiscriminate collection of information in bulk," but "consists entirely of targeting specific persons about whom an individualized determination has been made".[168] The PCLOB is an independent agency within the Executive Branch, that was established by the Implementing Recommendations of the 9/11 Commission Act of 2007. [169] The PCLOB's responsibilities are to review and analyse the implementation of the executive branch's policies, procedures, regulations, and acts that protect the nation from terrorism, in order to ensure the protection of privacy and civil liberties.[170]

Pursuant to a statistical transparency report regarding the use of National Security Authorities by the DNI, approximately 89,138 targets were affected by Section 702 in 2013.[171] The number of targets increased to 106,469 in 2015. The term "target", provided in these reports, refers to the estimated number of non-United States persons who were the users of tasked selectors.[172] In addition, a "target" could be "an individual person, a group, an organisation composed of multiple individuals, or a foreign power that possessed or was likely to communicate foreign intelligence information".[173]

However, the authorisation under Section 702 FISA serves as the legal basis for the so-called "PRISM" and "Upstream" collection programs.[174] PRISM is a database maintained by the NSA to collect information from Internet service providers.[175] The PCLOB describes the PRISM program as follows:

---

[167] *Gorski* (2016), p. 6.
[168] PCLOB Report (2014), p. 111.
[169] *The Privacy and Civil Liberties Oversight Board*: History and Mission, Retrieved June 17, 2019, from https://www.pclob.gov/about/.
[170] Id.
[171] *Office of Director of National Intelligence* (2014, June): Statistical Transparency Report regarding use of National Security Authorities - Annual Statistics for Calendar Year 2013, Retrieved June 17, 2019, from https://www.dni.gov/files/tp/National_Security_Authorities_Transparency_Report_CY2013.pdf.
[172] *Office of Director of National Intelligence* (2017, April): Statistical Transparency Report regarding use of National Security Authorities - Annual Statistics for Calendar Year 2016, Retrieved June 17, 2019, from https://icontherecord.tumblr.com/transparency/odni_transparencyreport_cy2016.
[173] Statistical Transparency Report regarding use of National Security Authorities of the Office of Director of National Intelligence, Annual Statistics for Calendar Year 2013.
[174] PCLOB Report (2014), p. 7.
[175] *Council of the European Union* (2013), 16987/13, p. 5.

> *"in PRISM collection, the government sends a selector, such as an email address, to a United States-based electronic communications service provider, such as an Internet service provider ("ISP"), and the provider is compelled to give the communications sent to or from that selector to the government".*[176]

According to the PCLOB, the PRISM program does not collect telephone calls. Apart from the NSA, the Central Intelligence Agency (CIA) and the FBI also have access to the PRISM collection.[177]

Edward Snowden and Media reports disclosed that Facebook has participated as one of the Internet service providers in the PRISM program.[178] Other internet service providers who have been compelled to provide communications to the government, but whose identity was not confirmed by the U.S.[179], were Microsoft, Yahoo, Google, Facebook, PalTalk, AOL, Apple, Skype, and YouTube.[180]

In contrast to the PRISM program, in the Upstream collection "the government compels the "assistance of providers that control the telecommunications 'backbone' over which telephone and internet communications transit".[181] The government thereby £acquires communications that are "to", "from", or "about" a tasked selector, as they travel through the internet backbone."[182] According to Professor Swire's report, only the NSA receives data from the Upstream program.[183]

As Swire explains in his report, most of the Internet backbone has been built in the U.S. because of the rise of the internet.[184] Consequently, a large portion of the Internet backbone routs through the U.S., and due to growing use of U.S.-based providers (for webmail, social networks, cloud services), foreign-to-foreign communications could be subject to surveillance conducted in the U.S.[185]

---

[176] PCLOB Report (2014), p. 7.
[177] Id.
[178] *Gorski* (2016), p. 10.
[179] *Council of the European Union* (2013), 16987/13, p. 5.
[180] *Gellman, Barton / Poitras, Laura* (2013, June 7): U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program, Retrieved June 17, 2019, from https://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html?utm_term=.7a7af18c4f09.
[181] PCLOB Report (2014), p. 7.
[182] Id., p. 7.
[183] *Swire* (2016, November 3), Chapter 5, p. 31.
[184] Id., Chapter 3, p. 19.
[185] Id., Chapter 3, p. 24.

The Upstream program comprises two different two acquisition forms, the acquisition of so-called "about" communications, and of so-called "multiple communications transactions" ("MCTs").[186] Multiple communications transactions are internet transactions that contain emails or other communications sent to or from a tasked selector. In its report, the PCLOB stated that upstream collection can "result in the acquisition of some communications that are unrelated to the intended targets".[187]

An "about" communication describes an acquisition of internet communications that are neither to nor from a tasked selector (such as an email address), but instead may include a reference to that selector.[188] The targeted person is not necessarily a participant in the communication, but the communication may contain the selector of a targeted person (email address) in the body of the communication, and thus be "about" the targeted selector.[189]

5.3. USA PATRIOT Act 2001

Under Section 215 of the US Patriot Act, the FBI was allowed "to make an application for a court order requiring a business or another entity to produce 'tangible things', such as books, records or documents, where the information sought is relevant for an investigation to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities".[190] In order to apply for an court order, the FBI just had to "specify reasonable grounds to believe that the records are relevant to an authorized investigation to obtain foreign intelligence information not concerning a U.S. person or to protect against international terrorism".[191]

As the U.S. has confirmed, Section 215 of the USA Patriot Act 2011 served as a legal basis for bulk collection of telephone metadata maintained by specified telecommunications service providers. In this regard, an acquisition under Section 215 included telephone metadata or call detail records, such as telephone numbers dialled, the numbers from which calls were made, and the date, time and duration of calls. The collection did not include the content of calls, or the names, address, or financial information of any subscriber or customer.[192]

---

[186] PCLOB Report (2014), p. 7.
[187] Id., p. 41.
[188] Id., p. 119.
[189] Id., p. 7.
[190] *Council of the European Union* (2013), 16987/13, p. 10.
[191] Id., p. 11.
[192] Id.

This metadata program concerned both the data of U.S. and EU persons, "whenever they are party to a telephone call made to, from, or within the U.S. and whose meta-data is maintained and produced by a company to whom the order is addressed".[193] With the implementation of the USA Freedom Act on June 2, 2015 parts of the provisions of the USA Patriot Act, including the bulk collection of telephony metadata pursuant to Section 215, expired. At the same time, the USA Freedom Act stipulated a new mechanism, enabling the government to acquire data held by the providers, when the government proves to the court that "there is a reasonable, articulable suspicion that the selection term is associated with an approved international terrorist organization".[194]

5.4. Executive Order (EO) 12333

Executive Order 12333 is the third legal authority for surveillance programs, the scope of which is at the discretion of the President. The electronic surveillance under EO 12333 is conducted by the U.S. government, both inside and outside the U.S. This form of intelligence gathering does not require judicial approval, nor is it subject to judicial oversight.[195]

In the Report of the EU-US Working Group on Data protection, it was stated that the surveillance operations under the EO have to be conducted according to guidelines that are approved by the head of the relevant agency and the Attorney General. It does not contain "any restriction on bulk collection of data located outside the U.S., except that all intelligence collection must comply with the US Constitution."[196] Moreover, the U.S. indicated that the limitations on this intelligence collection are not designed to limit the acquisition of the personal data of non-U.S. persons.[197]

In her report, Gorski confirms that surveillance programs under EO 12333 are neither subject to meaningful oversight by the U.S. Congress nor by U.S. courts. She explicitly states that an EO order allows the U.S. government to engage in "bulk collection", which means the "indiscriminate collection of electronic communications or data".[198]

---

[193] *Council of the European Union* (2013), 16987/13, p. 11.
[194] Office of the Director of National Intelligence, Retrieved June 17, 2019, from https://www.intel.gov/index.php/ic-on-the-record-database/results/780-joint-statement-by-the-office-of-the-director-of-national-intelligence-and-the-department-of-justice-on-the-declassification-of-the-renewal-of-collection-under-section-215-of-the-usa-patriot-act-50-u-s-c-sec-1861-,-as-amended-by-the-usa-freedom-ac.
[195] *Council of the European Union* (2013), 16987/13, p. 12.
[196] Id.
[197] Id.
[198] *Gorski* (2016), p. 12.

Furthermore, the EO order permits so-called "'*bulk searching'*, in which the government searches the content of vast quantities of electronic communications for '*selection terms*'".[199] Simply put, it means that the NSA can subject the communications content of the global population to real-time surveillance, in order to look for specific items of interest. In order to search communications in bulk, the NSA can use a wide range of keywords. The selectors do not have to be associated with particular targets, such as an email address. As a consequence, the Gorski believes that the government can use selectors that lead to a collection of even larger amounts of information, such as the names of countries or political figures. In conclusion, Gorski argues that EO 12333 surveillance orders are extremely permissive, due the fact that the EO order permits "the government to target non-U.S. persons abroad for virtually any 'foreign intelligence' reason".[200]

5.5. Presidential Policy Directive (PPD) 28

In 2014, then-President Barack Obama issued PPD-28, which imposes certain constraints on the U.S. government's collection or retention of the personal data of non-U.S. persons.[201] With regard to the privacy of non-U.S. persons, PPD-28 states that "signal intelligence activities must take into account that all persons should be treated with dignity and respect, regardless of their nationality or wherever they might reside, and that all persons have legitimate privacy interests in the handling of their personal information".[202] Furthermore, PPD-28 set out certain principles regarding how signal intelligence activities should be conducted, such as "privacy and civil liberties shall be integral considerations in the planning of U.S. signal intelligence activities", and "signals intelligence activities shall be as tailored as feasible".[203]

One of the significant reforms by PPD-28 are the limitations on the use of bulk collections.[204] According to the PPD, bulk collection means "the authorized collection of large quantities of signals intelligence data which, due to technical or operational considerations, is acquired without the use of discriminants (e.g., specific identifiers, selection terms, etc.)".[205]

---

[199] *Gorski* (2016), p. 12.
[200] Id., p. 13.
[201] Id., p. 15.
[202] The White House, Office of the Press Secretary (2014, January 17): Presidential Policy Directive -- Signals Intelligence Activities, Retrieved June 17, 2019, from https://obamawhitehouse.archives.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities.
[203] Id.
[204] *Gorski* (2016), p. 16.
[205] The White House, Office of the Press Secretary (2014, January 17): Presidential Policy Directive -- Signals Intelligence Activities, Retrieved June 17, 2019, from https://obamawhitehouse.archives.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities.

Under the PPD, bulk collection of signals intelligence is only allowed when the signals intelligence is not publicly available, and the U.S. shall use that data only for six specific purposes, such as to detect and counter espionage and other threats directed by foreign powers, threats to the United States from terrorism, proliferation, or the use of weapons of mass destruction, or threats cybersecurity. Nonetheless, pursuant to footnote 5 of the PPD, these limitations "do not apply to signals intelligence data that is temporarily acquired to facilitate targeted collection".[206]

Furthermore, for transparency purposes the intelligence agencies (NSA, CIA and FBI) have to publicly release their implementation procedures.[207] These procedures stipulate, for example, that agencies must delete information collected through signals intelligence concerning non-U.S. persons five years after collection.[208]

However, as Gorski correctly pointed out, the reforms of PPD 28 could easily be modified or revoked by the next or present U.S. president.[209] Moreover, Professor Swire states that "as with any other U.S. Executive Order or Presidential Policy Directive, the President's announcement cannot create a right of action enforceable in court".[210] On the other hand, he says that in his experience, agencies go to great length to comply with directives from the US President.[211]

5.6. Individual Remedies for Violations of Privacy

This chapter gives a short overview of the most significant remedies for abuses of government surveillance authorities which are available for EU citizens under U.S. law. The availability of sufficient remedies for data subjects are of particular importance for the analysis of an adequate level of data protection regarding EU-U.S. data transfers.

5.6.1. Privacy Act, Judicial Redress Act and Umbrella Agreement

The Privacy Act of 1974 granted U.S. persons the right to access, review, and correct data held by U.S. federal agencies, and to obtain injunctions or monetary damages for the improper

[206] The White House, Office of the Press Secretary (2014, January 17): Presidential Policy Directive -- Signals Intelligence Activities, Retrieved June 17, 2019, from https://obamawhitehouse.archives.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities.
[207] *Swire* (2016, November 3), Chapter 3, p. 46.
[208] Id., Chapter 2, p. 15.
[209] *Gorski* (2016), p. 15.
[210] Id., p. 3-46.
[211] *Swire* (2016, November 3), Chapter 3, p. 46.

handling of covered records.[212] With the enforcement of the Judicial Redress Act of 2016, the U.S. government extended the protections of the Privacy Act to EU citizens.[213]

Under the Judicial Redress Act, EU citizens are able to seek judicial redress before U.S. courts when a U.S. governmental agency wilfully or intentionally discloses covered records in violation of the Privacy Act.[214]

Nevertheless, the Privacy Act allows agencies to exempt their records from the Privacy Act, on grounds of national security.[215] In this regard, the NSA has made use of this exemption.[216] This exemption seems to be controversial, but as Professor Vladeck emphasises in his report, the provision to exempt records of disclosure exists for a good reason.[217] For example, "if the NSA obtains data belonging to a terrorist who is in Paris and may be planning an attack, it should not have to provide the target with access to his files and the ability to correct them".[218]

However, taking into account that the NSA is the primary agency responsible for foreign surveillance activities,[219] the exception means that the Privacy Act does not provide meaningful redress to EU citizen with respect to records maintained by the NSA.[220]

With regard to personal data transfers between EU and U.S. law enforcement authorities, the so-called "Umbrella Agreement" provides safeguards and remedies for EU citizens whose data is transferred. Under the Umbrella Agreement, data can only be transferred between the EU and the U.S. for the purpose of the prevention, detection, investigation, and prosecution of criminal offences, including terrorism.[221]

5.6.2. Redress under Section 2712 of Title 18 of the U.S. Code

Under section 2712 of Title 18 of the U.S. Code, any person can sue the U.S. government for damages when the individual is aggrieved by a wilful violation of certain statutory

[212] *Swire* (2016, November 3), Chapter 1, p. 21.
[213] Id.
[214] *Swire* (2016, November 3), Chapter 1, p. 21.
[215] *Vladeck* (2016, November 2), p. 19.
[216] *Edgar, Timothy* (2015, October 19): Redress for NSA Surveillance: The Devil Is in the Details, Retrieved June 17, 2019, from https://www.lawfareblog.com/redress-nsa-surveillance-devil-details.
[217] *Vladeck* (2016, November 2), p. 20.
[218] *Edgar, Timothy* (2015, October 19): Redress for NSA Surveillance: The Devil Is in the Details, Retrieved June 17, 2019, from https://www.lawfareblog.com/redress-nsa-surveillance-devil-details.
[219] Judgement of Ms. Costello, The High Court, Commercial, 2016, No. 4809 P, p. 104.
[220] *Edgar, Timothy* (2015, October 19): Redress for NSA Surveillance: The Devil Is in the Details, Retrieved June 17, 2019, from https://www.lawfareblog.com/redress-nsa-surveillance-devil-details.
[221] *European Commission* (2016b): Press release - Questions and Answers on the EU-U.S. Data Protection "Umbrella Agreement", Retrieved June 17, 2019, from, http://europa.eu/rapid/press-release_MEMO-16-4183_en.htm.

provisions.[222] This individual right of action applies to a violation of the Electronic Communications Privacy Act (ECPA), and to three sections of the FISA (Section 1806, 1825 and 1845).[223]

The ECPA consists of two parts, the Wiretap Act (codified at 18 U.S. Code Chapter 119 §2510-2522), and the Stored Communications Act (SCA codified at 18 U.S. Code Chapter 121 §§ 2701-2712).[224]

The SCA sets out conditions on how the government can access stored communications held by a technology provider, such as an Internet service provider.[225] Under the SCA, any person, including EU citizens, can bring an action against an individual government actor or US agency on the grounds of unlawful access. In case of a successful claim, the affected person can recover monetary "damages of at least $1,000 USD, equitable or declaratory relief, reasonable attorney's fees, reimbursement of legal fees, and/or punitive damages".[226]

In contrast to the SCA, the Wiretap Act governs the interception of electronic communications in real-time and represents the statutory authority for U.S. law enforcement officials to engage in such interceptions.[227] Like the SCA, the Wiretap Act "provides a remedy to data subjects whose communications have been unlawfully intercepted by the U.S. government".[228] Under the Wiretap Act, the interception of communications is a criminal offense, unless exemptions apply. For both claims, the plaintiff has to prove that the violation of the ECPA was "wilful".[229]

In addition, under the ECPA a data subject can bring suit against private companies that unlawfully disclose personal data or violate the statute in intercepting data.[230]

Section 1806 and 1824 of FISA both provide individual remedies for data subjects against unlawful acts by Federal officers or employees. While Section 1806 refers to information

---

[222] Judgement of Ms. Costello, The High Court, Commercial, 2016, No. 4809 P, p. 100.
[223] Id.
[224] *Swire* (2016, November 3), Appendix A, p. 9.
[225] *Lackey, Michael E. / Pottinger, Oral D.* (2018): Stored Communications Act: Practical Considerations. Lexis Practice Advisor Journal, 3(3), 43–52, pp. 43–48, Retrieved from https://www.mayerbrown.com/-/media/files/news/2018/10/stored-communications-act-practical-considerations/files/stored-comm-with-checklist/fileattachment/stored-comm-with-checklist.pdf.
[226] *Swire* (2016, November 3), Chapter 7, p. 8.
[227] *Daskal, Jennifer* (2018, October 15): Setting the Record Straight: The CLOUD Act and the Reach of Wiretapping Authority Under US Law, Retrieved June 17, 2019, from https://www.crossborderdataforum.org/setting-the-record-straight-the-cloud-act-and-the-reach-of-wiretapping-authority-under-us-law/?cn-reloaded=1.
[228] *Swire* (2016, November 3), Chapter 7, p. 18.
[229] Id., Chapter 7, p. 9.
[230] Id., Chapter 7, p. 17ff.

acquired from electronic surveillance, Section 1825 concerns the acquisition of information from physical searches within in the U.S.[231]

5.6.3. Doctrine of Standing

When filing an action, the plaintiff has to demonstrate that he or she has "standing" to sue before the U.S. federal courts.[232] The doctrine of standing, which stems from Article III of the U.S. Constitution, requires the following elements to be met when filing a suit: an injury in fact, "a sufficient causal connection between the injury and the conduct complained of, and a likelihood that the injury will be redressed by a favourable decision".[233]

As Gorski explains in her report, the Article III standing requirement has proven to be a significant obstacle to challenging the lawfulness of conducted surveillances before U.S. courts. Due to the fact that individuals do not receive any notice that they are subject to Section 702 or EO 12333 surveillances, it is unlikely for them to be able to establish sufficient standing.[234] In *Clapper v. Amnesty International USA*, the U.S. Supreme Court ruled that a number of private plaintiffs lacked standing to challenge Section 702 of FISA, because "they could not demonstrate that collection of their communications was certainly impending or fairly traceable".[235]

In contrast to Gorski, Professor Vladeck says that "the obstacles posed by the 'standing' doctrine are substantially overstated".[236] With regard to the Snowden disclosures, Prof. Vladeck stresses that an EU citizen is today more likely to have standing to challenge U.S. data collection. He also argues that the Clapper decision "might well have come out differently had it been decided after the Snowden disclosures".[237]

Nevertheless, Prof. Vladeck notes that there is "significant uncertainty in the lower courts over exactly when Clapper does and does not foreclose standing".[238] Despite that uncertainty, he asserts that "this uncertainty is not nearly as categorically hostile to standing as suggested in

[231] Judgement of Ms. Costello, The High Court, Commercial, 2016, No. 4809 P, p. 100.
[232] Id., p. 107.
[233] *Gorski* (2016), p. 19.
[234] Id., p. 18ff.
[235] *Vladeck* (2016, November 2), p. 26.
[236] Id., p. 32ff.
[237] Id., p. 26ff.
[238] Id., p. 29.

the DPC Draft Decision, and is instead more reflective of the case-specific vagaries of individual lawsuits".[239]

Prof. Swire also claims that the *Clapper* decision does not "create a per se ban on cases involving US foreign intelligence or counterterrorism programs".[240] To support this statement, Prof. Swire highlights some court decisions where US courts have accepted that the plaintiffs had standing to challenge Section 215 telephone metadata programs.[241] Nevertheless, Judge Costello concluded in her decision that the necessity to establish standing "is a very complex matter in the context of secret government surveillance" [242], and that all the evidence on the record indicated the standing requirement as a substantial obstacle for the plaintiff.[243]

5.6.4. The Ombudsperson Mechanism

In the context of judicial protection of EU citizens, the Ombudsperson mechanism plays an important role. In the course of the negotiations between the U.S. and the EU over the Privacy Shield, the U.S. executive branch created the Ombudsperson mechanism in order "to facilitate the processing of requests relating to national security access to data that is transmitted from the EU to the US pursuant to the Privacy Shield", SCCs and BCRs.[244]

The Ombudsperson is a senior official within the US Department and is independent from US national security services.[245] In order to bring a complaint before the Ombudsperson, the individual has to first submit the request to the EU supervisory authority, which verifies the requester's identity and ensures that the request is complete. A complaint to the Ombudsperson does not require the requester to demonstrate that "personal data have been in fact accessed by the U.S. Government through signal intelligence activities".[246] After the review, the request will be submitted to the Ombudsperson by the EU centralised body.

A response by the Ombudsperson will confirm:

> *"(i) that the complaint has been properly investigated, and (ii) that the U.S. law, statutes, executives orders, presidential directives, and agency policies, providing the*

[239] *Vladeck* (2016, November 2), p. 29.
[240] *Swire* (2016, November 3), Chapter 7, p. 39.
[241] Id.
[242] Judgement of Ms. Costello, The High Court, Commercial, 2016, No. 4809 P, p. 107.
[243] Id. p. 107.
[244] C(2016) 4176.
[245] *European Commission* (2016a): GUIDE TO THE EU-U.S. PRIVACY SHIELD, Retrieved June 17, 2019, from https://ec.europa.eu/info/sites/info/files/2016-08-01-ps-citizens-guide_en.pd_.pdf.
[246] C(2016) 4176, Annex A.

limitations and safeguards described in the ODNI letter, have been complied with, or, in the event of non-compliance, such non-compliance has been remedied".[247]

The response "will neither confirm nor deny whether the individual has been the target of surveillance nor will the Privacy Shield Ombudsperson confirm the specific remedy that was applied".[248]

Although remedies from the Ombudsperson do not require the requester to have standing, the Ombudsperson mechanism is subject to intense criticism.[249] Schrems and Gorski argue that the Ombudsperson's position is not completely independent from the intelligence community, because the Ombudsperson is acting under the Secretary of State and is therefore bound by instructions from the executive. Moreover, there is no possibility to appeal or enforce the decision of the Ombudsman. Consequently, Mr. Schrems asserts that the Ombudsperson mechanism does not comply with Article 47 of the CFR, which guarantees the right to an effective remedy before an independent tribunal.[250]

5.7. Discussion of the Legal Remedies under U.S. Law

Firstly, Swire and Vladeck's testimonies obviously expressed the opinion that under U.S. Law and practice, there are sufficient remedies available to EU citizens to protect them from unlawful seizure by the U.S. government.

In this regard, Judge Costello in her ruling agreed that there is a large variety of possible remedies available to EU citizens, but they nevertheless have to face significant obstacles to obtain any legal remedy for unlawful processing of their personal data in the U.S.[251] One of the main obstacles is the difficulty of establishing standing in the U.S. According to the DPC's submissions, the standing requirement to establish U.S. jurisdiction over a claim in the U.S. "effectively undermines the right to effective judicial protection" as guaranteed by Article 47 of the CFR.[252] The U.S. standing doctrine in the area of national security is far more stringent than the standing doctrine established by the ECHR.[253]

---

[247] C(2016) 4176, Annex A.
[248] Id.
[249] *Swire* (2016, November 3), Chapter 1, p. 28.
[250] *Schrems*, *Maximilian* (2016): Privacy Shield: Politisch gewollte Totgeburt mit Anlauf? (Teil II). Öffentlicher Bereich, Dako 2016/52, Heft 4/2016, p. 85.
[251] Judgement of Ms. Costello, The High Court, Commercial, 2016, No. 4809 P, p. 116.
[252] Id., p. 126.
[253] Id., p. 128.

Further, Judge Costello determined that "is a significant limitation on the right to seek a remedy", when for some causes of actions the "plaintiff has to establish that he or she has suffered damage" (pecuniary damage).[254] Another barrier to individual EU citizens obtaining claims under Section 2712 is the requirement that he or she must prove that the violation of the statute by an individual actor was wilful.[255]

Moreover, in her ruling, Judge Costello expressed that claims for violation of the provisions of the Fourth Amendment, which constitute the foremost protection under U.S. law against unlawful government surveillance, are not available to most EU citizens, because in most cases they lack substantial voluntary connections with the U.S..[256] In addition, because there is no notification obligation under U.S. law, it is extremely difficult for surveillance targets to challenge secret government surveillance or obtain rectification or erasure of their data.[257]

Although the Irish High Court acknowledged that the U.S. "has extensive rules to ensure that data is obtained in accordance with the law" [258], "it cannot be said that US law provides the right of every person to a judicial remedy for any breach of his data privacy by its intelligence agencies".[259]

Even Facebook's appointed expert, Professor Swire, stated that "individual remedies were sometimes difficult to provide in the intelligence setting, because of the risk of revealing classified information to hostile actors".[260] In his testimony, he said that "the desirability of individual remedies in intelligence systems must be weighed against the risks that come from disclosing classified information".[261]

In conclusion, the Irish High Court agreed with the Irish DPC's opinion that U.S. law and practices "do not respect the essence of the right to an effective remedy before an independent tribunal, as guaranteed by Article 47 of the CFR".[262] Because of the well-founded concerns with respect to the adequacy of the protection afforded to EU data subjects whose personal data is wrongfully interfered with, the High Court referred the issue (*Data Protection Commission*

[254] Judgement of Ms. Costello, The High Court, Commercial, 2016, No. 4809 P, p. 117.
[255] Id., p. 118.
[256] Id., p. 100.
[257] Id., p. 108ff.
[258] Id.
[259] Id.
[260] *Swire* (2016, November 3), Chapter 1, p. 20.
[261] Id., Chapter 8, p. 1.
[262] Judgement of Ms. Costello, The High Court, Commercial, 2016, No. 4809 P, p. 132.

v. Facebook and Schrems) to the CJEU for a preliminary ruling.[263]

6. Current Developments in the EU and U.S.: The Cloud Act and the e-evidence Draft Regulation

6.1. The Cloud Act

Another important legal framework for the analysis of EU-U.S. data transfers, is the enactment of the Clarifying Lawful Overseas Use of Data Act 2018 (Cloud Act) in March 2018. Due to its significant extra-territorial effect, it is of particular importance regarding the use of cloud computing. The Cloud Act enables U.S. law enforcement agencies to have worldwide access (via warrant or subpoena) to data stored within or outside of the US.[264] This affects all individuals, companies or organisations which are significant influenced by a U.S. company.[265]

The main purpose of the Cloud Act is to "support the U.S. Government's efforts to protect public safety and combat serious crime, including terrorism".[266] The background of the Cloud Act was the dispute between the DoJ and Microsoft Corp. in 2013. Federal agents obtained an 18 U.S.C. 2703 warrant, that required Microsoft to disclose all e-mails and other information associated with the account of a specific customer, who was suspected of illegal drug trafficking.[267] With respect to the e-mail contents, which were stored in Microsoft's data centre in Dublin, Microsoft refused to disclose the data to the U.S. Government and quashed the warrant. In course of the proceedings, the Second Circuit ruled that the disclosure of the data "would be an unauthorized extraterritorial application of section 2703" [268], and therefore reversed the Federal District Court's decision that Microsoft had to comply with the warrant.[269]

At the certiorari stage, the European Commission filed on behalf of the EU an *amicus curiae* brief in support of neither party, arguing that "any domestic law that creates cross-border obligations should be applied and interpreted in a manner that is mindful of the restrictions of

---

[263] Judgement of Ms. Costello, The High Court, Commercial, 2016, No. 4809 P, p. 152.
[264] Data Protection Day 2019 – the US CLOUD Act and what's at stake for UK and EU businesses (2019), LexisNexis, p. 1, Retrieved June 17, 2019, from https://www.lewissilkin.com/en/insights/data-protection-day-2019-the-us-cloud-act-and-whats-at-stake-for-uk-and-eu-businesses.
[265] *Thiele, Clemens (2018):* U.S. CLOUD Act - Danaergeschenk für den Europäischen Datenschutz, ZIIR 2018, p. 128.
[266] Data Protection Day 2019 – the US CLOUD Act and what's at stake for UK and EU businesses (2019), LexisNexis, p. 1, Retrieved June 17, 2019, from https://www.lewissilkin.com/en/insights/data-protection-day-2019-the-us-cloud-act-and-whats-at-stake-for-uk-and-eu-businesses.
[267] *United States v. Microsoft Corporation*, No. 17-2, 584 U.S.__(2018), Retrieved June 17, 2019, from https://supreme.justia.com/cases/federal/us/584/17-2/.
[268] Id.
[269] Id.

international law and considerations of international comity".[270] In particular, the Commissions addressed the compliance of the warrant with the additional rules for transfer of personal data to third countries, set out in chapter 5 of the GDPR. Further, the Commission noted that Article 49 of the GDPR permits "derogations for specific situations" and indicated that the following derogations seem to be relevant for the present case: "a transfer necessary for important reasons for public interest" and "a transfer necessary for the purposes of compelling legitimate interests pursued by the controller which are not overridden by the interests or rights and freedoms of the data subject"(could be the legitimate interest of a controller not being subject to legal action in a non-EU Member State).[271]

This issue of whether a section 2703 warrant would also cover data stored outside the U.S.[272] led to the U.S. Congress's enactment of the Cloud Act. The Cloud Act amended SCA by adding the following sentence:

> *"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."*[273]

Due to the amendments to the U.S. law, the Supreme Court vacated jurisdiction in respect of the dispute between Microsoft Corp. and the U.S., because the case had become moot. The Supreme Court also concluded that "no live dispute remains between the parties over the issue with respect to which certiorari was granted" [274], and "a new warrant replaced the original warrant."[275]

At present, under the Cloud Act the U.S. government has the ability to compel electronic communications service or remote computing service providers to give the government access

---

[270] *United States v. Microsoft Corporation,* No. 17-2, Brief of the European Commission on Behalf of the European Union as Amicus Curiae in Support of neither Party, Retrieved June 17, 2019, from https://www.supremecourt.gov/DocketPDF/17/17-2/23655/20171213123137791_17-2%20ac%20European%20Commission%20for%20filing.pdf.
[271] Id.
[272] *Bühlmann, Lukas / Reinle, Michael* (2019, March 24): Extraterritorial Reach of the CLOUD Act, Retrieved June 17, 2019, from https://www.mll-news.com/extraterritorial-reach-of-the-cloud-act/.
[273] Cloud Act, 18 U.S.C. §2713, Retrieved June 17, 2019, from https://www.congress.gov/bill/115th-congress/senate-bill/2383/text.
[274] *United States v. Microsoft Corporation*, No. 17-2, 584 U.S.__(2018).
[275] Id.

to data regardless of the data's location, when the service provider is subject to U.S. jurisdiction and has "possession, custody, or control" over the relevant communication or information.[276] A service provider is subject to U.S. jurisdiction when it is either headquartered or incorporated in the U.S. (general jurisdiction), or has "minimum contacts" with the U.S. (specific jurisdiction).[277]

The service provider can file a motion seeking to reject the disclosure request within 14 days, if the provider believes that "the customer or subscriber is not a United States person and does not reside in the United States" and "that the required disclosure would create a material risk that the provider would violate the laws of a qualifying foreign government."[278]

However, this right to challenge a disclosure request is limited to service providers that are subject to an executive agreement between the U.S. and the foreign state concerned.[279] To date, no executive agreement has been concluded between the U.S. and the EU.[280]

Even if an executive agreement existed, a disclosure request may only be modified or quashed, if the court finds that:

> *(i) "the required disclosure would cause the provider to violate the laws of a qualifying foreign government;*
> *(ii) based on the totality of the circumstances, the interests of justice dictate that the legal process should be modified or quashed; and*
> *(iii) the customer or subscriber is not a United States person and does not reside in the United States."*[281]

However, a violation of the foreign law, in particular of the GDPR, does not lead necessarily to a modification or cancelation of an 18 U.S.C section 2713 warrant, because it depends on the outcome of the second precondition, the so-called "comity analysis".[282]

---

[276] Cloud Act, 18 U.S.C. §2713.
[277] *Berengaut, Alexander / Goodloe, Katharine* (2019, April 5): Reaching for the CLOUD, Retrieved June 17, 2019, from https://www.insideprivacy.com/surveillance-law-enforcement-access/reaching-for-the-cloud/.
[278] Cloud Act, 18 U.S.C. §2713.
[279] Data Protection Day 2019 – the US CLOUD Act and what's at stake for UK and EU businesses (2019), LexisNexis, p. 2, Retrieved June 17, 2019, from https://www.lewissilkin.com/en/insights/data-protection-day-2019-the-us-cloud-act-and-whats-at-stake-for-uk-and-eu-businesses.
[280] As of June 2019.
[281] Cloud Act, 18 U.S.C. §2713.
[282] *Thiele* (2018), p. 130.

It is obvious that the Cloud Act is in conflict with the GDPR, in particular with Article 48, due to its extraterritorial effect.[283] Article 48 of the GDPR forbids data transfers to a third country based on a court judgment or any decision of an administrative authority of a third country, unless the transfer is "based on an international agreement, such as a mutual legal assistance treaty".[284]

The conclusion of executive agreements pursuant to 18 U.S.C. § 2523 may not constitute an international agreement under Article 48 of the GDPR, because the agreements may not satisfy the strict requirements of the GDPR.[285] In this regard, the Article 29 Working Party considers "that a public authority in a non-EU country should" only have direct access to data of individuals processed within the EU "through prior authorisation by a public authority in the EU"[286] and the "foreign requests must not be served directly to companies under EU jurisdiction".[287]

As has been already mentioned, the GDPR basically protects the data processing of all individuals by a European company equally, regardless of whether the personal data concerns EU or non-EU citizens. In contrast, the Cloud Act only protects the data of EU citizens if the US government has concluded a contract with an EU member state or a foreign government. This mutual and unrestricted exchange of data constitutes a condition sine qua non for a limited data protection under the Cloud Act.[288]

Judicial cooperation on electronic evidence between the EU and U.S. public authorities is based on Mutual Legal Assistance Agreements. Because it is often too slow (taking an average of 10 months to cooperate), the EU has a strong incentive to conclude an executive agreement with the U.S., in order to facilitate crime investigation.[289]

---

[283] *Knyrim* in *Knyrim* (2018), DatKomm, Art 48 DSGVO, para. 14.
[284] Article 48 GDPR.
[285] *Thiele* (2018), p. 132.
[286] Joint Statement of the European Data Protection Authorities assembled in the Article 29 Working Party (2014), 14/EN WP 227, p. 3, Retrieved June 17, 2019, from https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp227_en.pdf.
[287] Id.
[288] *Thiele* (2018), p. 132.
[289] *European Commission* (2019, February 5): Press release - Questions and Answers: Mandate for the EU-U.S. cooperation on electronic evidence, Retrieved June 17, 2019, from http://europa.eu/rapid/press-release_MEMO-19-863_en.htm.

As mentioned above, the Cloud Act "applies to data that is in the 'possession, custody or control' of any US company or foreign companies with a presence in the US".[290] In some scenarios, it seems unlikely that a U.S.-based service provider is required to disclose data held by a EU company, when the following facts apply:

- The European parent company has a subsidiary in the U.S. and the personal data is stored solely in the EU. Further, the affiliate is not the controller of the data.[291]
- The computer network of the U.S. affiliate is completely separated from the networks of its parent company.
- Due to technical reasons, the staff of the U.S. subsidiary is incapable of having remote access to the telecommunication infrastructure of the EU parent company to obtain the data.[292]

In order to minimize the risk of disclosing data to the U.S. government, service recipients (controller of the stored data) are advised to use an encryption key management that is fully under their control and not open to the U.S. cloud service provider.[293] Moreover, it would be reasonable if the cloud service agreement stipulates the obligation for the cloud service provider to notify the controller, when it receives a disclosure request by the U.S. government.

6.2. The e-evidence Draft Regulation

In response to the implementation of the Cloud Act, the European Commission proposed in April 2018 a Regulation on European Production and Preservation Orders for electronic evidence in criminal matters, in short, the e-evidence draft Regulation, and a Directive laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings.[294] The purpose of the proposals is to speed up "the process to secure and obtain electronic evidence that is stored and /or held by service providers established in another jurisdiction".[295] E-evidence means "evidence stored in electronic form

[290] Data Protection Day 2019 – the US CLOUD Act and what's at stake for UK and EU businesses (2019), LexisNexis, p. 2, Retrieved June 17, 2019, from https://www.lewissilkin.com/en/insights/data-protection-day-2019-the-us-cloud-act-and-whats-at-stake-for-uk-and-eu-businesses.
[291] Id.
[292] Artzt, Matthias / Delacruz, Walter (2019, January 29): How to comply with both the GDPR and the CLOUD Act, Retrieved June 17, 2019, from https://iapp.org/news/a/questions-to-ask-for-compliance-with-the-eu-gdpr-and-the-u-s-cloud-act/.
[293] Id.
[294] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on European Production and Preservation Orders for electronic evidence in criminal matters COM/2018/225 final - 2018/0108 (COD).
[295] Id. p. 2.

by or on behalf of a service provider" [296], including for example e-mails, IP addresses, user names, content data from messaging apps or photographs. According to the proposal, judicial authorities from EU member states would have direct access to e-evidence from a service provider in another jurisdiction.[297]

The current legal frameworks to obtain data from countries outside the EU, as already mentioned above, are the Mutual Legal Assistance Agreements and the European Investigation Order to obtain evidence within the EU. Due to the fact that these procedures are too slow to obtain evidence in the digital age, the Commission initiated this e-evidence package to give law enforcement and judicial authorities tools to investigate and prosecute crimes efficiently.[298]

The new proposed rules apply to service providers that offer services in the Union, enabling legal or natural persons in one or more Member States to use the service. At the same time the service provider needs to have a substantial connection based on specific factual criteria, which are "for example significant number of users in one or more Member States, or the targeting activities […] such as the use of language or a currency used in that Member State or the possibility to order goods or services".[299] In recital 16 of the draft Regulation the Commission considers that providers of electronic communications services (e.g. instant messaging and e-mail services) and specific providers of information society services that offer their users the ability to communicate with each other or services to process or store data in their behalf. In this regard the Commission explicitly mentions that hosting services, including services that are provided via cloud computing, should be included in the category of service providers under the draft Regulation.[300]

Under the Commission's proposal service providers would be compelled via an European Production Order Certificate (EPOC) to hand over stored data, regardless of where the data is stored, within 10 days or in emergency cases within 6 hours upon receipt of the EPOC.[301] In case of non-compliance, service provider might risk imposing of sanctions of up to 2% of the

[296] Article 2 (6) of the draft Regulation.
[297] COM/2018/225 final.
[298] *European Commission* (2018c): Factsheet: Facilitating Access to electronic evidence, Retrieved June 17, 2019, https://www.consilium.europa.eu/en/press/press-releases/2019/03/08/e-evidence-package-council-agrees-its-position-on-rules-to-appoint-legal-representatives-for-the-gathering-of-evidence/.
[299] Recital 28 of the draft Regulation.
[300] Recital 16 of the draft Regulation.
[301] Article 9 of the draft Regulation.

total world annual turnover.[302] The draft Regulation envisages also a European Preservation Order Certificate (EPOC-PR) to prevent the e-evidence from deletion.

With regard to the addresses of production and preservation orders, the draft Directive comes into play, under which all service providers will have to appoint a legal representative in the EU for the purpose of gathering evidence in criminal proceedings, who will be the recipient of the EPOCs and EPOC-PRs.[303]

However, the draft Regulation is subject to intense criticism regarding fundamental rights breaches.[304] In this regard, the EDPB expressed concerns that data subjects' rights might be undermined, because under the draft Regulation the service providers acting as processor within the meaning of the GDPR does not have to notify the data controller, when addressed with an ECOP.[305] Further, the EDPB recommends to prolong the 10-day deadline for EPOC recipients, because service providers should have more time to assess whether the EPOC should be executed or not.[306]

Another big issue is the fact that no judicial or equivalent authority in the enforcing state would be involved in the first stages of the execution process of EPOCs. Only if the private company refuses to comply with the EPOC, the enforcing state would get involved.[307]

Moreover, one of the major points of criticism is the abandonment of the dual criminality principle under the draft e-evidence Regulation. According to Article 5 (2) of the draft e-evidence Regulation, EPOCs "may only be issued if a similar measure would be available for the same criminal offence in a comparable domestic situation in the issuing State" [308], whereas orders concerning transactional data or content data, data may only be issued "for criminal offences punishable in the issuing State by a custodial sentence of a maximum of at least 3

[302] Article 14 (1) of the draft Regulation.
[303] Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings, COM/2018/226 final - 2018/0107 (COD).
[304] Civil society letter urging Member States to seriously reconsider its draft position on law enforcement access to data or "e-evidence"(2018), Retrieved June 17, 2019, from https://edri.org/files/20181203_e-evidence_civilsocietyletter.pdf.
[305] EDPB (2018): Opinion 23/2018 on Commission proposals on European Production and Preservation Orders for electronic evidence in criminal matters (Art. 70.1.b), p. 9f., Retrieved June 17, 2019, from https://edpb.europa.eu/our-work-tools/our-documents/opinia-art-70/opinion-232018-commission-proposals-european-production_en.
[306] EDPB (2018): Opinion 23/2018, p. 6.
[307] *European Digital Rights (EDRi)* (2019): Recommendations on cross-border access to data. Position paper on the European Commission's proposal for a Regulation on European Production and Preservation Orders for electronic evidence in criminal matters, p. 7, Retrieved June 17, 2019, from https://edri.org/files/e-evidence/20190425-EDRi_PositionPaper_e-evidence_final.pdf.
[308] Article 5 of the proposed Regulation on e-Evidence.

years".[309] In this regard, the EDPB stresses out "that no harmonization within in the EU has taken place yet of criminal offences".[310]

Also, the German Association of Judges raised concerns regarding the justifications of issuing EPOCs.[311] According to Article 5 of the draft e-evidence Regulation, the only precondition for an EPOC is that it shall be "necessary and proportionate for the purposes of criminal proceedings".[312] Furthermore, the European Digital Rights association criticises that data may be retained for an unlimited period of time, when a subsequent EPOC has been launched.[313]

In conclusion the e-evidence draft Regulation is the counterpart to the Cloud Act, enabling competent judicial authorities from a Member State to obtain electronic data from service providers, regardless of whether the data is stored within the Union or not. As a result, the extraterritorial effect of this proposal will create more conflict of laws, because service providers, that have their cloud infrastructure in a third country, might violate foreign law, when complying with ECOPs.[314] Moreover, one of the major issues of the proposals lies in the fact that the draft e-evidence Regulation would give a EU Member States, where the EU doubts its rule of law (e.g. Poland and Hungary), direct access to data collected by providers in other Member State.[315] However, due to the emerge of cloud computing, where the data storage location can be chosen arbitrarily and changed daily, it is apparent that the current procedures to obtain evidence show weaknesses.[316]

With regard to the Cloud Act, the e-evidence package could serve as a basis for the settlement of an executive agreement between the EU and the U.S.[317] For this reason, the Commission has been authorised via mandates by the Council to start negotiations on behalf of the EU regarding

---

[309] Article 5 of the proposed Regulation on e-Evidence.
[310] EDPB (2018): Opinion 23/2018, p. 7.
[311] *Bundesrechtsanwaltskammer* (2018): Stellungnahme Nr. 28/2018, Registernummer: 25412265365-88, p. 5, Retrieved June 17, 2019, from https://www.brak.de/zur-rechtspolitik/stellungnahmen-pdf/stellungnahmen-deutschland/2018/september/stellungnahme-der-brak-2018-28.pdf.
[312] Article 5 of the proposed Regulation on e-Evidence.
[313] EDRi (2019a), p. 21.
[314] *Cole, Mark D. / Quintel, Teresa* (2018): Transborder Access to e-Evidence by Law Enforcement Agencies. A first comparative view on the Commission's Proposal for a Regulation on a European Preservation/Production Order and accompanying Directive, Law Working Paper No. 2018-010, p. 19, Retrieved June 17, 2019, from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3278780.
[315] *European Commission* (2019, April 3): Press release - Rule of Law: The Commission opens a debate to strengthen the rule of law in the EU, Retrieved June 17, 2019, from http://europa.eu/rapid/press-release_IP-19-1912_en.htm.
[316] *Kaudela, Carmen / Radl, Lena Kristin* (2019): Europäisches Strafrecht nach der österreichischen Ratspräsidentschaft, ZWF 3/2019, p. 105.
[317] *European Commission* (2019, February 5): Press release - Questions and Answers: Mandate for the EU-U.S. cooperation on electronic evidence, Retrieved June 17, 2019, from http://europa.eu/rapid/press-release_MEMO-19-863_en.htm.

an agreement with the U.S. facilitating the access to e-evidence for the purpose of judicial cooperation in criminal matters and to participate in the negotiations in the Council of Europe on a second additional protocol to the Cybercrime Convention.[318]

The analysis in Part 5, 6 and 7 has revealed the difficulty for EU data subjects to obtain any legal remedy for unlawful processing of their personal data in the U.S. and that the Cloud Act is in conflict with the GDPR. The practical legal business implications of transnational and cross-border partnerships, in particular between the EU and U.S., shall be analysed now within the framework of a hypothetical case study.

7. Case Study

To illustrate the conclusion on the legal issues regarding EU-U.S. personal data transfers through clouds, the following hypothetical scenario is considered.

Due to cost-saving measures, Company A opts for a cloud infrastructure to store files in electronic form. Company A is established within the EU. The files contain their customers' personal data, such as their first names and surnames, e-mail addresses, dates of birth and credit card information. For this purpose, the Company A concludes a cloud service agreement with a U.S. company, that provides the cloud infrastructure where the personal data is processed.

The data centre of the cloud platform is located in the U.S. We also assume that the U.S. cloud service provider, which operates the cloud infrastructure, participated in the Privacy Shield Framework. In light of the Schrems 2.0. proceedings, the question now arises as to whether or not a European firm can conclude a contract with a U.S. cloud service provider under the GDPR.

First, it is necessary to examine if the GDPR is applicable to the present case. It is evident that the material scope is applicable, because the storage of the clients' personal data in the cloud constitutes a processing as defined by Article 2 of the GDPR.

Considering the concept of data controller and processor, in the present case, Company A, which stores its clients' personal data and decides to outsource the data storage, acts as the "controller" pursuant to Article 4 (7) of the GDPR, while the U.S. company, which provides

[318] *Council of the European Union* (2019, June 6): Council gives mandate to Commission to negotiate international agreements on e-evidence in criminal matters, Retrieved June 17, 2019, from https://www.consilium.europa.eu/en/press/press-releases/2019/06/06/council-gives-mandate-to-commission-to-negotiate-international-agreements-on-e-evidence-in-criminal-matters/.

the necessary cloud infrastructure, is defined as the "processor" pursuant to Article 4 (8).[319] In the present case, we assume that provider does not play a relevant role in determining the purpose or essential means of processing. Otherwise, Company A and the cloud provider would be considered as joint controllers and each of them would have to comply with the relevant data protection obligations. Therefore, in the present scenario Company A as the "controller" has to comply with the obligations under the GDPR.

In addition, the case study falls within the territorial scope of the GDPR, because the controller is established in the EU. But as already mentioned in Chapter 3, the GDPR applies regardless of whether or not the processing itself takes place within the EU and it is not necessary that the cloud service provider or the data controller have to be established in the EU. Without an establishment of the controller or the processor in the EU, it is also sufficient for the application of the GDPR to the processing of personal data of data subjects who are in the Union, when the cloud service provider is offering its servicer to the controller in the EU.

Before data can be stored in the cloud of the U.S. cloud provider, the data processing has to be legitimate within the EU according to the requirements set out in the GDPR. In particular, the data processing has to be based on a legal permission pursuant to Articles 6, 9 or 10. In the present case, the consent of the data subject or the performance of a contract could serve as a legal basis for the lawful processing. Another requirement is the conclusion of a data processing agreement between the controller and the cloud service provider as the processor pursuant to Article 28 of the GDPR. Before the data can be stored in the cloud of an U.S. cloud service provider, it has to be assessed if the data transfer to the U.S. meet the requirements set out in Articles 44 ff. of the GDPR. As discussed above, on the basis of an adequacy decision of the European Commission personal data can be transferred to a third country without any further safeguards or specific authorisation. In the present case, the U.S. cloud service is certified under the EU-U.S. Privacy Shield. Other appropriate safeguards for the international data transfer according to Article 46 of the GDPR would be for example BCRs or SCCs.

Taking into account the testimonies on U.S. law and practice and the ruling of the High Court, it is not guaranteed anymore that the Privacy Shield provides an adequate level of data protection for EU citizens. There is a high chance that the Cloud service provider is subject to

[319] *Raffling* in *Schock* (2018), p. 47ff.

the directives by the U.S. government under Section 702, to assist or send communications to the government.

Even though the U.S. cloud service provider certified itself under the Privacy Shield framework, it is doubtful that U.S. law and practice provide adequate levels of data protection as laid down in the GDPR. Considering the expert opinions on U.S. law, the redress mechanism in the U.S. is highly complex. EU citizens whose data is transferred to the U.S. have to face many barriers in the U.S., before they can obtain any legal remedy for the unlawful processing of their personal data. For example, the requirement to have standing before U.S. courts is excessively difficult and it undermines the right to effective judicial protection, as guaranteed by Article 47 of the CFR. Even the introduction of the Ombudsperson mechanism does not eliminate the concerns regarding the adequacy of the data protection of EU individuals whose data is subject to unlawful U.S. intelligence surveillance.[320]

Additionally, the limitations on the use of bulk collections under PPD 28 does not effectively improve the data protection standard of EU individuals, because "PPD 28 is binding upon executive branch agencies as an instruction from the head of the executive branch" [321], and it does not grant a right of action that is enforceable in court.[322] In addition, the limitation on bulk collection under the PPD can easily be revoked by the current president.

However, what is even more detrimental to the present case study is the implementation of the Cloud Act. In any case, the U.S. cloud service provider will be subject the Cloud Act, as it is established on U.S. soil. Therefore, U.S. jurisdiction is a given, and it has custody over and is in control of the EU clients' personal data. Consequently, there is a high possibility that the U.S. cloud service provider might be compelled U.S. by law enforcement agencies via a warrant or subpoena to disclose the stored data to the U.S. government.

U.S.-based cloud service providers are not the only entities affected by the Cloud Act; data held by EU cloud service providers that are affiliates of U.S. companies could also be accessible under the Act. Since the Cloud Act entered into force, there is no longer any guarantee for the data protection of EU individuals, due to its extraterritorial effect. Even alternative tools like BCRs and SCCs between a U.S. cloud service provider and an EU company (cloud user) will not eliminate the conflict between the Cloud Act and the GDPR.

[320] Judgement of Ms. Costello, The High Court, Commercial, 2016, No. 4809 P, p. 152.
[321] *Swire* (2016, November 3), Chapter 3, p. 46.
[322] Id., p. 46.

Overall, *in my opinion* U.S. law and practice do not offer an adequate level of protection to EU data subjects, because EU individuals who are subject to U.S. surveillance do not enjoy the same level of data protection in the U.S. as they do in the EU. Therefore, if an EU company concludes a cloud service agreement with an U.S. cloud service provider, it will probably contradict the regulations of the GDPR. It is thus recommended that EU company opt for a European cloud service provider that has no U.S. parent company or data centres outside of the EU. In conclusion, at the present time the data transfer from the EU company to the U.S. cloud service provider will not comply with the GDPR's requirements.

8. Concluding Remarks

There are significant differences between the U.S. and the EU in respect of the fundamental concept of data protection. U.S. citizens do not have a "right to privacy" that is equivalent to Article 8 of the CFR / ECHR. The Fourth Amendment to the U.S. Constitution only confers the right to U.S. citizens to defend himself or herself against the state.[323] Moreover, there is no independent data protection authority in the U.S. comparable to the one in the EU, that enforces the "right to privacy". The Federal Trade Commission (FTC) does not correspond to European standards.[324]

Despite the large number of causes of actions open to EU citizens, in reality it is most unlikely for an EU citizen to be able "to obtain a remedy for unlawful acquisition or processing of his or her personal data"[325] in the U.S. Generally speaking, U.S. law lacks a redress mechanism that is comparable to EU standards.

With respect to the Cloud Act, companies that are subject to this legislation may be forced to choose whether to violate a U.S. order to disclose data, or to violate the GDPR's regulations, risking fines of €20 million or 4% of annual turnover.[326] EU cloud service providers that are subsidiaries of U.S. companies are advised to retain as much control over the data as possible, in order to keep it out of reach of any warrant or subpoena under the Cloud Act.[327]

The Cloud Act undermines the GDPR's requirements as set out in Article 48 of the GDPR, by

[323] *Thiele* (2018), p. 131.
[324] Id.
[325] Judgement of Ms. Costello, The High Court, Commercial, 2016, No. 4809 P, p. 117.
[326] *Bühlmann / Reinle* (2019, March 24): Extraterritorial Reach of the CLOUD Act, Retrieved June 17, 2019, from https://www.mll-news.com/extraterritorial-reach-of-the-cloud-act/.
[327] Data Protection Day 2019 – the US CLOUD Act and what's at stake for UK and EU businesses (2019), LexisNexis, p. 3, Retrieved June 17, 2019, from https://www.lewissilkin.com/en/insights/data-protection-day-2019-the-us-cloud-act-and-whats-at-stake-for-uk-and-eu-businesse.

compelling U.S. electronic communication service and remote computing service providers to allow access to data stored outside the U.S.[328] Therefore, the service recipient (controller of data) should encrypt the personal data in advance before uploading them to the cloud, in order to reduce the risk of disclosing the data to U.S. authorities. However, for the sake of the protection of personal data against the access by U.S. government, it would be better, to choose software solutions that operate exclusively in private in-house networks or European cloud service provider who have their data centres exclusively in the European Union and no connection to the U.S.[329]

Nevertheless, there is a pending risk for cloud service providers, who offer services in the European Union, to disclose personal data to another EU Member State, where its rule of law is being questioned. In case of the implementation of the e-evidence proposals, authorities from EU member states would have worldwide access to stored data from private cloud providers. There is no judicial review of the enforcing state in the first stages of the enacting process of an EPOC. Cloud service providers are required to decide themselves if ECOPs are legitimate or not. It is apparent that the e-evidence draft Regulation is the equivalent to the U.S. Cloud Act, enabling authorities to obtain data directly from private companies. Consequently, even if a company chooses a cloud infrastructure exclusively located within the EU, fundamental rights of the data subject might be at stake in future, when the e-evidence package is being implemented.

On the basis of the concerns expressed above and in particular the implementation of the Cloud Act, it is highly likely that the ECJ will consider the Privacy Shield to be invalid, because the framework and the U.S. law do not offer adequate level of protection to European data subjects. To conclude, it would be helpful, and of great interest, if the European Commission would make details of the evaluation of third country laws publicly available and provide explanations why that third country's law provides an adequate level of protection to EU data subjects and the public, when preparing adequacy decisions.[330]

---

[328] Artzt / Delacruz (2019), Retrieved June 17, 2019, from https://iapp.org/news/a/questions-to-ask-for-compliance-with-the-eu-gdpr-and-the-u-s-cloud-act/.

[329] *Thiele, Clemens / Wagner*, *Jessica (2019):* Umsetzung der DSGVO in der Personalpraxis. Fragen, Antworten, Muster, Verlag Österreich 2019, p. 35.

[330] *Kuner*, *Christopher* (2017, July 12): Third country law in the CJEU's data protection judgments. Retrieved June 17, 2019, from http://europeanlawblog.eu/2017/07/12/third-country-law-in-the-cjeus-data-protection-judgments/.

Abstract
Cloud Computing has become an emerging trend. However, since the revelations about the U.S. National Security Agency's mass surveillance programme by Edward Snowden in 2013 it is not guaranteed anymore that personal data transfers to the U.S. are subject to adequate data protection according to the GDPR. Considering expert opinions and submissions in the legal proceedings *Data Protection Commission v. Facebook and Schrems,* it is reasonable to assume that U.S. law and practice do not provide adequate data protection to EU citizens, who are subject to U.S. surveillance intelligence. Moreover, the implementation of the Cloud Act in March 2018 brought a new challenge for cloud service providers to reconcile with the European legal framework. In the light of the above, this thesis analyses whether or not a European firm can conclude a contract with a U.S. cloud service provider under the GDPR. Further, the thesis examines more generally how the transfer of personal data to the U.S. through a cloud technology can be brought into compliance with the GDPR's requirements. In general, under the Cloud Act, U.S. law enforcement agencies have worldwide access (via warrant or subpoena) to data stored within or outside of the U.S. Due to its extraterritorial effect, it is practically impossible for an EU business company to comply with the GDPR, when using a cloud application of cloud service provider that falls under the scope of the Cloud Act. As a result, cloud service provider may be either forced to violate U.S. orders to disclose data or the GDPR. Moreover, the proposal for a Regulation on cross-border access to e-evidence in criminal matters will bring a new challenge for cloud service providers. The e-evidence draft Regulation allows competent authorities from EU Member States direct access to data stored by or on behalf of the cloud service providers, regardless of the location of its storage facility. Non-compliance with the e-evidence proposal would result in sanctions up to 2% of the total word annual turnover. The analysis of this thesis generally suggests that it would be better to choose software solutions that operate exclusively in private in-house networks or European cloud service provider who have their data centres exclusively in the EU and no connection to the U.S. However, new emerging legislation such as the e-evidence Regulation would further complicate the usage of Cloud Computing even within the EU.

Abstract (Deutsch)
Cloud Computing wurde in den letzten Jahren zu einem immer mehr aufkommenden Trend. Allerdings ist seit den Enthüllungen von Edward Snowden im Jahr 2013 über die Massenüberwachungsprogramme der US National Security Agency nicht mehr garantiert, dass der transatlantische Datenverkehr und die Verarbeitung von personenbezogenen Daten in einer Cloud einem angemessenen Datenschutz gemäß der DSGVO entsprechen. Vor dem Hintergrund des laufenden Verfahrens *Data Protection Commissioner/Facebook Ireland Limited, Maximilian Schrems* (C-311/18) ist davon auszugehen, dass das US-amerikanische Recht keinen angemessenen Datenschutz für personenbezogene Daten, insbesondere von EU-Bürgern, bietet, um diese vor staatlicher Überwachung durch US-Behörden ausreichend zu schützen. Darüber hinaus brachte die Umsetzung des Cloud Acts im März 2018 eine neue Herausforderung für Cloud Provider. Angesichts dieser rechtlichen Rahmenbedingungen untersucht die vorliegende Arbeit die Frage, ob ein europäisches Unternehmen einen Vertrag mit einem US-amerikanischen Cloud-Anbieter im Rahmen der DSGVO abschließen kann bzw. ob die Übermittlung von personenbezogenen Daten in die USA über eine Cloud-Technologie den Anforderungen der DSGVO entspricht.Unter dem Cloud Act haben amerikanische Strafverfolgungsbehörden einen weltweiten Zugriff auf alle Daten, die innerhalb oder außerhalb der USA von Cloud Providern gespeichert werden. Aufgrund der extraterritorialen Wirkung des Cloud Acts können Cloud Provider folglich dazu gezwungen werden, entweder gegen US-amerikanische Herausgabeanordnungen oder gegen Bestimmungen der DSGVO zu verstoßen. Des Weiteren sieht der Vorschlag für eine E-Evidence-Verordnung europäische Herausgabe- und Sicherungsanordnungen für elektronische Beweismittel in Strafsachen vor. Der Verordnungsentwurf soll Behörden aus den EU-Mitgliedstaaten den direkten Zugriff auf elektronische Beweismittel, wie etwa auf Cloud gespeicherte Daten, ermöglichen. Die Nichteinhaltung der vorgesehenen Verordnung würde zu Sanktionen von bis zu 2% des gesamten weltweiten Jahresumsatzes führen. Die Analyse zeigt auf, dass es prinzipiell einfacher ist, Softwarelösungen, die ausschließlich in privaten Netzwerken betrieben werden, bzw. europäische Cloud-Service-Anbieter, deren Rechenzentren ausschließlich in der EU liegen, zu wählen. Die Nutzung von Cloud Computing könnte jedoch selbst innerhalb der EU durch zukünftige Entwicklungen, wie beispielsweise durch den Vorschlag für eine E-Evidence-Verordnung, erschwert werden.

References

Article 29 Data Protection Working Party (2010): Opinion 1/2010 on the concepts of "controller" and "processor", 00264/10/EN WP 169.

Article 29 Data Protection Working Party (2017): EU-U.S. Privacy Shield – First annual Joint Review, 17/EN WP 255.

Bundesrechtsanwaltskammer (2018): Stellungnahme Nr. 28/2018, Registernummer: 25412265365-88, p. 5, Retrieved June 17, 2019, from https://www.brak.de/zur-rechtspolitik/stellungnahmen-pdf/stellungnahmen-deutschland/2018/september/stellungnahme-der-brak-2018-28.pdf.

Civil society letter urging Member States to seriously reconsider its draft position on law enforcement access to data or "e-evidence"(2018), Retrieved June 17, 2019, from https://edri.org/files/20181203_e-evidence_civilsocietyletter.pdf.

Cole, Mark D. / Quintel, Teresa (2018): Transborder Access to e-Evidence by Law Enforcement Agencies. A first comparative view on the Commission's Proposal for a Regulation on a European Preservation/Production Order and accompanying Directive, Law Working Paper No. 2018-010, Retrieved June 17, 2019, from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3278780.

Council of the European Union (2013): Report on the findings by the EU Co-chairs of the ad hoc EU-US Working Group on Data Protection, 16987/13, Retrieved June 17, 2019, from https://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/jha/139745.pdf.

Data Protection Day 2019 – the US CLOUD Act and what's at stake for UK and EU businesses (2019), LexisNexis, Retrieved June 17, 2019, from https://www.lewissilkin.com/en/insights/data-protection-day-2019-the-us-cloud-act-and-whats-at-stake-for-uk-and-eu-businesses.

Djemame, Karim / Barnitzke, Benno / Corrales, Marcelo / Kiran, Mariam / Jiang, Ming / Armstrong, Django / Forgó, Nikolaus / Nwankwo, Iheanyi (2013): Legal Issues in Clouds: Towards a Risk Inventory, Philosophical Transactions of the Royal Society A. Mathematical, Physical and Engineering Sciences.

Dürager, Sonja (2017): Outsourcing in die Cloud. Ein (un-)beherrschbares Risiko aus datenschutzrechtlicher Sicht?, ipCompetence 2017, Heft 18, pp. 36-53.

European Commission (2017): Report From The Commission To The European Parliament And The Council On The First Annual Review Of The Functioning Of The EU-U.S. Privacy Shield, SWD 611 final.

European Commission (2018a), Report From The Commission To The European Parliament And The Council On The Second Annual Review Of The Functioning Of The EU.U.S. Privacy Shield, COM 860 final.

European Commission (2018b), COMMISSION STAFF WORKING DOCUMENT Accompanying The Document REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL On The Second Annual Review Of The Functioning Of The EU.U.S. Privacy Shield, SWD 497 final.

European Commission (2018c): Factsheet: Facilitating Access to electronic evidence, Retrieved June 17, 2019, https://www.consilium.europa.eu/en/press/press-releases/2019/03/08/e-evidence-package-council-agrees-its-position-on-rules-to-appoint-legal-representatives-for-the-gathering-of-evidence/

European Data Protection Board (2018): Opinion 23/2018 on Commission proposals on European Production and Preservation Orders for electronic evidence in criminal matters (Art. 70.1.b), Retrieved June 17, 2019, from https://edpb.europa.eu/our-work-tools/our-documents/opinia-art-70/opinion-232018-commission-proposals-european-production_en.

European Data Protection Board (2019): EU-U.S. Privacy Shield – Second Annual Joint Review, Retrieved June 17, 2019, from https://edpb.europa.eu/our-work-tools/our-documents/other/eu-us-privacy-shield-second-annual-joint-review-report-22012019_de.

European Digital Rights (EDRi) (2019): Recommendations on cross-border access to data. Position paper on the European Commission's proposal for a Regulation on European Production and Preservation Orders for electronic evidence in criminal matters, Retrieved June 17, 2019, from https://edri.org/files/e-evidence/20190425-EDRi_PositionPaper_e-evidence_final.pdf.

European Parliamentary Research Service (2017): From Safe Harbour to Privacy Shield. Advances and shortcomings of the new EU-US data transfer rules, PE 595.892, Retrieved June 17, 2019, from http://www.europarl.europa.eu/RegData/etudes/IDAN/2017/595892/EPRS_IDA(2017)595892_EN.pdf.

European Parliamentary Research Service (2018): The Privacy Shield. Update on the state of play of the EU-US data transfer rules, PE 625.151, Retrieved June 17, 2019, from http://www.europarl.europa.eu/RegData/etudes/IDAN/2018/625151/EPRS_IDA(2018)625151_EN.pdf.

Feiler, Lukas / Forgó, Nikolaus (2017): EU-DSGVO: EU-Datenschutz-Grundverordnung, Kurzkommentar, Verlag Österreich 2017.

Georgieva, *Ludmilla* (2017): EU-US-Privacy Shield - eine Gesamtbetrachtung, in Baumgartner, Gerhard (Hrsg.): Öffentliches Recht. Jahrbuch 2017, pp. 193-239.

Gorski, Ashley (2016): The Data Protection Commissioner and Facebook Ireland Limited and Maximillian Schrems, Expert Report of Ashley Gorski on behalf of the second named defendant, Retrieved June 17, 2019, from https://iapp.org/media/pdf/resource_center/Schrems-testimony-Gorski.pdf.

Graf, Ferdinand / Križanac, Marija (2017): GDPR compliance. Sonderheft Datenschutz-Grundverordnung, ecolex 9a/2017, pp. 945-952.

Joint Statement of the European Data Protection Authorities assembled in the Article 29 Working Party (2014), 14/EN WP 227, Retrieved June 17, 2019, from https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp227_en.pdf.

Kaudela, Carmen / Radl, Lena Kristin (2019): Europäisches Strafrecht nach der österreichischen Ratspräsidentschaft, ZWF 3/2019, pp. 105-108.

Knyrim, Dr. Rainer (Hrsg.) (2019): Der DatKomm: Praxiskommentar zum Datenschutzrecht, Manz 2018.

Leschanz, Judith / Ehrnberger, *Verena* (2015): Interne Nutzung von Cloud-Dienstleistungen in Unternehmen, Dako 2015/45, Heft 4/2015, pp. 84-85.

Mell, Peter / Grance, Timothy (2011): The NIST definition of cloud computing. National Institute of Standards and Technology (NIST), U.S. Department of Commerce, Retrieved June 17, 2019, from https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf.

Privacy and Civil Liberties Oversight Board (2014): Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act, Retrieved June 17, 2019, from https://www.pclob.gov/library/702-Report.pdf.

Raffling, Mag. Philip / Schock, Mag.a *Sofie (Hrsg.) (2018):* Digitale Wirtschaft und Industrie 4.0, Manz 2018.

Schrems, *Maximilian* (2016): Privacy Shield: Politisch gewollte Totgeburt mit Anlauf? (Teil II). Öffentlicher Bereich, Dako 2016/52, Heft 4/2016, pp. 83-85.

Swire, Peter (2016, November 3): The Data Protection Commissioner and Facebook Ireland Limited and Maximillian Schrems, Affidavit of Peter Swire, Retrieved June 17, 2019, from https://iapp.org/media/pdf/resource_center/Schrems-testimony-Swire.pdf.

Thiele, Clemens (2018): U.S. CLOUD Act - Danaergeschenk für den Europäischen Datenschutz, ZIIR 2018, pp. 128-132.

Thiele, Clemens / Wagner, *Jessica (2019):* Umsetzung der DSGVO in der Personalpraxis. Fragen, Antworten, Muster, Verlag Österreich 2019.

Vladeck, Stephen (2016, November 2): The Data Protection Commissioner and Facebook Ireland Limited and Maximillian Schrems, Affidavit of Stephen I. Vladeck, Retrieved June 17, 2019, from https://iapp.org/media/pdf/resource_center/Schrems-testimony-Vladeck.pdf.

Voigt, Paul / Von dem Bussche, Axel (2018): EU-Datenschutz-Grundverordnung (DSGVO). Praktikerhandbuch unter vollständiger Berücksichtigung des DSAnpUG-EU, Springer 2018.

Wissenschaftliche Dienste. Deutscher Bundestag (2015): Datenschutzrecht der Europäischen Union, Deutschlands und der USA, WD 3 – 3000 – 064/15, Retrieved June 17, 2019, from https://www.bundestag.de/resource/blob/409136/df3683ab30663377d240a9074e92c63f/wd-3-064-15-pdf-data.pdf.

Weiss, Martin A. / Archick, Kristin (2016): U.S.-EU Data Privacy: From Safe Harbour to Privacy Shield, Retrieved June 17, 2019, from https://epic.org/crs/R44257.pdf.

European Union Statutes

2001/497/EC: Commission Decision of 15 June 2001 on standard contractual clauses for the transfer of personal data to third countries, under Directive 95/46/EC, OJ L 181, 4.7.2001.

2004/915/EC: Commission Decision of 27 December 2004 amending Decision 2001/497/EC as regards the introduction of an alternative set of standard contractual clauses for the transfer of personal data to third countries, OJ L 385, 29.12.2004.

2010/87/: Commission Decision of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council, OJ L 39, 12.2.2010.

Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield (notified under document C(2016) 4176) [2016], OJ L 207/1.

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 safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce (notified under doc.no. C(2000) 2441) [2000], OJ L 215/7.

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 (DPD), [2016] OJ L281/31.

Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on European Production and Preservation Orders for electronic evidence in criminal matters, COM/2018/225 final - 2018/0108 (COD).

Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings, COM/2018/226 final - 2018/0107 (COD).

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, OJ 2119/1.

Court Decisions

Case C-362/14 *Maximilian Schrems v. Data Protection Commissioner,* 6 October 2015, ECLI:EU:C:2015:650.

Judgement of Ms. Justice Costello, The High Court, Commercial, 2016, No. 4809 P., *The Data Protection Commissioner v Facebook Ireland and Maximillian Schrems*, 3 October 2017, Retrieved June 17, 2019, from https://www.dataprotection.ie/sites/default/files/uploads/2018-12/High%20Court%20Judgment_03_10_2017.pdf.

Case C-311/18 Reference for a preliminary ruling from the High Court (Ireland) made on 9 May 2018 — *Data Protection Commissioner v Facebook Ireland Limited, Maximillian Schrems*, OJ C 249, 16.7.2018.

United States v. Verdugo-Urquidez, No. 88-1353, 494 U.S. 259 (1990), Retrieved June 17, 2019, from https://supreme.justia.com/cases/federal/us/494/259/.

United States v. Microsoft Corporation, No. 17-2, 584 U.S.__(2018), Retrieved June 17, 2019, from https://supreme.justia.com/cases/federal/us/584/17-2/.

United States v. Microsoft Corporation, No. 17-2, Brief of the European Commission on Behalf of the European Union as Amicus Curiae in Support of neither Party, Retrieved June 17, 2019, from https://www.supremecourt.gov/DocketPDF/17/17-2/23655/20171213123137791_17-2%20ac%20European%20Commission%20for%20filing.pdf.

United States Law and Practice

Clarifying Lawful Overseas Use of Data Act 2018, Retrieved June 17, 2019, from https://www.congress.gov/bill/115th-congress/senate-bill/2383/text.

Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008, Pub. L. 110-261 (codified in scattered sections of 50 U.S.C.), Retrieved June 17, 2019, from https://www.congress.gov/110/plaws/publ261/PLAW-110publ261.pdf.

The White House, Office of the Press Secretary (2014, January 17). Presidential Policy Directive -- Signals Intelligence Activities, Retrieved June 17, 2019, from https://obamawhitehouse.archives.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities.

Video Privacy Protection Act of 1988 (codified at 18 U.S.C. § 2710).

Fourth Amendment to the United States Constitution, Retrieved June 17, 2019, from https://www.govinfo.gov/content/pkg/GPO-CONAN-1992/pdf/GPO-CONAN-1992-10-5.pdf.

Online References

Artzt, Matthias / Delacruz, Walter (2019, January 29): How to comply with both the GDPR and the CLOUD Act, Retrieved June 17, 2019, from https://iapp.org/news/a/questions-to-ask-for-compliance-with-the-eu-gdpr-and-the-u-s-cloud-act/.

Amazon: Was ist Cloud Computing, AWS, Retrieved from https://aws.amazon.com/de/what-is-cloud-computing/.

Berengaut, Alexander / Goodloe, Katharine (2019, April 5): Reaching for the CLOUD, Retrieved June 17, 2019, from https://www.insideprivacy.com/surveillance-law-enforcement-access/reaching-for-the-cloud/.

Bühlmann, Lukas / Reinle, Michael (2019, March 24): Extraterritorial Reach of the CLOUD Act, Retrieved June 17, 2019, from https://www.mll-news.com/extraterritorial-reach-of-the-cloud-act/.

Carolan, Mary (2018, April 12): High Court sets out 11 questions for ECJ on EU-US data transfers, Retrieved June 17, 2019, from https://www.irishtimes.com/business/technology/high-court-sets-out-11-questions-for-ecj-on-eu-us-data-transfers-1.3459549.

Council of the European Union (2019, June 6): Council gives mandate to Commission to negotiate international agreements on e-evidence in criminal matters, Retrieved June 17, 2019, from https://www.consilium.europa.eu/en/press/press-releases/2019/06/06/council-

gives-mandate-to-commission-to-negotiate-international-agreements-on-e-evidence-in-criminal-matters/.

Daskal, Jennifer (2018, October 15): Setting the Record Straight: The CLOUD Act and the Reach of Wiretapping Authority Under US Law, Retrieved June 17, 2019, from https://www.crossborderdataforum.org/setting-the-record-straight-the-cloud-act-and-the-reach-of-wiretapping-authority-under-us-law/?cn-reloaded=1.

Der Standard.at (2018, December 13): Österreichs Unternehmen bei Cloud Computing unter EU-Schnitt, Retrieved June 17, 2019, from https://derstandard.at/2000093856112/Oesterreichs-Unternehmen-bei-Cloud-Computing-unter-EU-Schnitt.

Dignan, Larry (2019, May 12): Top cloud providers 2019: AWS, Microsoft Azure, Google Cloud; IBM makes hybrid move; Salesforce dominates SaaS, Retrieved June 17, 2019, from https://www.zdnet.com/article/top-cloud-providers-2019-aws-microsoft-azure-google-cloud-ibm-makes-hybrid-move-salesforce-dominates-saas/.

Edgar, Timothy (2015, October 19): Redress for NSA Surveillance: The Devil Is in the Details, Retrieved June 17, 2019, from https://www.lawfareblog.com/redress-nsa-surveillance-devil-details.

European Commission (a): Adequacy decisions, Retrieved June 17, 2019, from https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en.

European Commission (b): BCR overview until 25th May - List of companies for which the EU BCR cooperation procedure is closed, Retrieved June 17, 2019, from https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/binding-corporate-rules-bcr_en#approval-of-binding-corporate-rules.

European Commission (c): Binding Corporate Rules (BCR), Retrieved June 17, 2019, from https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/binding-corporate-rules-bcr_en#bindingcorporaterules.

European Commission (d): EU-US data transfers, Retrieved June 17, 2019, from https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/eu-us-data-transfers_en.

European Commission (e): Standard Contractual Clauses (SCC), Retrieved June 17, 2019, from https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/model-contracts-transfer-personal-data-third-countries_en.

European Commission (2016a): GUIDE TO THE EU-U.S. PRIVACY SHIELD, Retrieved June 17, 2019, from https://ec.europa.eu/info/sites/info/files/2016-08-01-ps-citizens-guide_en.pd_.pdf.

European Commission (2016b): Press release - Questions and Answers on the EU-U.S. Data Protection "Umbrella Agreement", Retrieved June 17, 2019, from, http://europa.eu/rapid/press-release_MEMO-16-4183_en.htm.

European Commission (2018, July): Rules on international data transfers, Retrieved June 17, 2019, from https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/rules-international-transfers-personal-data_en.

European Commission (2019, February 5): Press release - Questions and Answers: Mandate for the EU-U.S. cooperation on electronic evidence, Retrieved June 17, 2019, from http://europa.eu/rapid/press-release_MEMO-19-863_en.htm.

European Commission (2019, April 3): Press release - Rule of Law: The Commission opens a debate to strengthen the rule of law in the EU, Retrieved June 17, 2019, from http://europa.eu/rapid/press-release_IP-19-1912_en.htm.

European Data Protection Supervisor (EDPS): Data Protection, Retrieved June 17, 2019, from https://edps.europa.eu/data-protection/data-protection_en.

Eurostat (2018, December): Cloud computing - statistics on the use by enterprises - Statistics Explained. Retrieved June 17, 2019, from https://ec.europa.eu/eurostat/statistics-explained/index.php/Cloud_computing_-_statistics_on_the_use_by_enterprises.

Gellman, Barton / Poitras, Laura (2013, June 7): U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program, Retrieved June 17, 2019, from https://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html?utm_term=.7a7af18c4f09.

Kuner, *Christopher* (2017, July 12): Third country law in the CJEU's data protection judgments. Retrieved June 17, 2019, from http://europeanlawblog.eu/2017/07/12/third-country-law-in-the-cjeus-data-protection-judgments/.

Lackey, Michael E. / Pottinger, Oral D. (2018): Stored Communications Act: Practical Considerations. Lexis Practice Advisor Journal, 3(3), 43–52, Retrieved from https://www.mayerbrown.com/-/media/files/news/2018/10/stored-communications-act-practical-considerations/files/stored-comm-with-checklist/fileattachment/stored-comm-with-checklist.pdf.

Macaskill, Ewen / Dance, Gabriel (2013, November 1): NSA files decoded: Edward Snowden's surveillance revelations explained, Retrieved June 17, 2019, from https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/5.

Matheson, Lee (2017, October 3): Understanding 'Schrems 2.0', Retrieved June 17, 2019, from https://iapp.org/news/a/understanding-schrems-2-0/.

Microsoft: Intelligente Geschäftsanwendungen - Microsoft Dynamics 365, Microsoft Deutschland, Retrieved June 17, 2019, from https://dynamics.microsoft.com/de-de/.

Office of Director of National Intelligence (2014, June): Statistical Transparency Report regarding use of National Security Authorities - Annual Statistics for Calendar Year 2013, Retrieved June 17, 2019, from https://www.dni.gov/files/tp/National_Security_Authorities_Transparency_Report_CY2013.pdf.

Office of Director of National Intelligence (2017, April): Statistical Transparency Report regarding use of National Security Authorities - Annual Statistics for Calendar Year 2016, Retrieved June 17, 2019, from https://icontherecord.tumblr.com/transparency/odni_transparencyreport_cy2016.

Office of the Director of National Intelligence, Retrieved June 17, 2019, from https://www.intel.gov/index.php/ic-on-the-record-database/results/780-joint-statement-by-the-office-of-the-director-of-national-intelligence-and-the-department-of-justice-on-the-declassification-of-the-renewal-of-collection-under-section-215-of-the-usa-patriot-act-50-u-s-c-sec-1861-,-as-amended-by-the-usa-freedom-ac.

Oracle: Infrastructure as a Service (IaaS) from Oracle, Retrieved June 17, 2019, from https://www.oracle.com/cloud/infrastructure.html#networking.

Privacy Shield List, Retrieved June 17, 2019, from https://www.privacyshield.gov/list.

International Association of Privacy Professional: Schrems 2.0: Expert Testimony, Retrieved June 17, 2019, from https://iapp.org/resources/article/schrems-2-0-expert-testimony/.

SalesForce: Was ist SaaS? Grundlegendes zu "Software as Service", SalesForce Deutschland, Retrieved June 17, 2019, from https://www.salesforce.com/de/learning-centre/tech/saas/.

SAP: SAP Business by Design, SAP Deutschland, Retrieved June 17, 2019, from https://www.sap.com/austria/products/business-bydesign.html.

Swire, Peter, / Daskal, Jennifer (2018, March 26): What the CLOUD Act means for privacy pros, Retrieved June 17, 2019, from https://iapp.org/news/a/what-the-cloud-act-means-for-privacy-pros/.

The Privacy and Civil Liberties Oversight Board: History and Mission, Retrieved June 17, 2019, from https://www.pclob.gov/about/.

The International Trade Administration (a), U.S. Department of Commerce: Privacy Shield Program Overview, Retrieved June 17, 2019, from https://www.privacyshield.gov/Program-Overview.

The International Trade Administration (b), U.S. Department of Commerce: The EU-U.S. and Swiss-U.S. Privacy Shield Frameworks, Retrieved June 17, 2019, from https://www.privacyshield.gov/servlet/servlet.FileDownload?file=015t0000000QJdg.

The International Trade Administration (c), U.S. Department of Commerce: How to Join Privacy Shield (part 1), Retrieved June 17, 2019, from https://www.privacyshield.gov/article?id=How-to-Join-Privacy-Shield-part-1.

United States Foreign Intelligence Surveillance Court (2018)*:* United States Foreign Intelligence Surveillance Court of Review, Retrieved June 17, 2019, from https://www.fisc.uscourts.gov/FISCR.