The transnational reach of GDPR: a comprehensive framework that can regulate data privacy internationally, or is that unrealistic?

Alison Dowers

The transnational reach of GDPR: a comprehensive framework that can regulate data privacy internationally, or is that unrealistic?

Alison Dowers

UNIVERSITÉ GRENOBLE ALPES
Faculty of Law

DISSERTATION ADVISOR: Dr Fabien Girard

MASTER'S DISSERTATION

Master 2 Droit de l'entreprise, juristes-conseils d'affaires
2018/2019

Table of Contents

INTRODUCTION

"Privacy is not an option, and it shouldn't be the price we accept for just getting on the Internet."

– Gary Kovacs[1]

Privacy and Data Protection are not new concepts in terms of EU law. However, with fast changing technical developments and the widespread use of the internet, along with its borderless nature, it has become more complicated for the EU legislature to ensure a high level of data protection for individuals in the EU.

The European Union (hereafter referred to as the EU) considers data protection to be a fundamental right which is granted to those located within the EU. The right to protection of personal data is enshrined in both the EU Charter of Fundamental Rights[2] at Article 8 and the Treaty on the Functioning of the European Union[3] at Article 16. In 1995 the European Union enacted a Directive aimed at creating certain rules and regulations relating to data protection, this will be referred to throughout this Dissertation as the Data Protection Directive[4]. However, in 2011 the European Data Protection Supervisor (EDPS) published an opinion stating that the Data Protection Directive was outdated and didn't provide effective protection given the technical advancement that had occurred since 1995 and that were likely to occur in the future[5]. In 2012 the Article 29 Working party[6] (hereafter referred to as the WP29) and the European Council started working on a reform to the Data Protection Directive. This reform became the basis for the General Data Protection Regulation[7]

[1] G. Kovacs is Chief Executive Officer of AVG Technologies, he is based in San Francisco, US

[2] The Charter of Fundamental Rights of the European Union, 2012/C 326/02

[3] The Treaty on the Functioning of the European Union, Official Journal, C 326, 26/10/2012 P. 0001-0390

[4] Directive 95/46/EC of the European Parliament and the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal, L 281, 23/11/1995 P. 00031 – 0050 (hereafter referred to as the TFEU)

[5] Opinion of the European Data Protection Supervisor on the Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions, A comprehensive approach on personal data protection in the European Union, Brussels, 14 January 2011, https://edps.europa.eu/sites/edp/files/publication/11-01-14_personal_data_protection_en.pdf, last accessed 14 August 2019

[6] The Article 29 Working Party is a group of national data protection commissioners, it was created under article 29 of the Data Protection Directive. It is an independent European advisory body on data protection and privacy.

[7] EU General Data Protection Regulation (GDPR): Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 119/1. (hereafter referred to as GDPR),

(hereafter referred to as the GDPR). This began a long period of negotiation, finally the GDPR was adopted by the European Parliament on the 27 April 2016. Given that the GDPR is a regulation, it is applicable directly in states which are members of the EU (hereafter referred to as Member States) without having to be implemented by national legislation[8]. However, Member States were given a two-year grace period to prepare for the GDPR. The GDPR finally came into force the 25 May 2018.

The EU aimed for GDPR to provide a comprehensive approach to data protection. In order to achieve this aim, it was necessary to take into account the fact that society has changed in the last 30 years, and so has our use of technology. Today, most people use the internet in their daily lives and companies are increasingly reliant on technology to do business. Indeed, with globalisation of commerce it is also true to say that data is, more than ever, being transferred outwith the EU. With the rise in cross-border data transfer, the rise in commerce being conducted over the internet, the rise in people communicating through electronic means, the invention of social media and its prominence in today's society, it is clear that the internet poses a significant risk to the protection of data. Indeed, with technical developments, ways to generate, collect, store and analyse data have also developed allowing for data analyses on a much grander scale than ever could have been imagined in the past. The more data that can be collected, the more reliable any decisions that are based on that data will be. For entities, the more data that can be collected, the better they can find patterns and accurately make predictions using technology. This practice is generally known as "big data" and most companies that deal with big data are located in the United States of America.

Given these advancements, regulating data only within the boundaries of the territory the EU would not be sufficient to ensure a comprehensive system of data protection for individuals located in the EU. Therefore, the GDPR was drafted to have extraterritorial applicability and to regulate data transfer outwith the EU. To deal with the challenges to data protection posed by the internet, the GDPR aims to be a comprehensive system for regulating data protection not just in the EU, but internationally.

The focus on this dissertation will be to evaluate to what extent the GDPR could be considered to have achieved this ambitious aim through its extraterritorial application and the rules contained in the GDPR relating to cross-border data transfer.

[8] The TFEU, Article 228

DEFINITIONS

There are some important terms used in the GDPR that require to be defined:

Personal Data: The GDPR applies to the processing of Personal Data. Data is considered to be personal if it could lead to the identification of an individual either directly or indirectly. Personal data also includes information about the physical, psychological, genetic, mental, economic, cultural or social identity of that natural person[9]. Throughout this Dissertation the reference to "data" should be taken to mean "personal data".

Data Controller: The Data Controller is the body that determines the purpose and means of the processing of the personal data. This definition involves three different elements, the data controller must be a natural or legal person, public authority, agency or other body. They can act alone or jointly with others and they determine the purpose and means of the data processing[10].

Data Processor: The Data Processor is the body that processes data on behalf of the Data Controller. Again, the Data Processor can be a natural or legal person, public authority, agency or other body[11]. The Data Processor must be separate from the Data Controller and they must process the data on behalf of the later[12].

Data Subject: The Data Subject is the person to whom the data which is collected and process relates.

National Data Protection Authorities (DPAs): DPAs are appointed in Member States to enforce data protection laws and offer guidance to Data Subjects. DPAs have enforcement powers under GDPR which includes the power issue substantial fines.

[9] GDPR, Article 4(1)

[10] GDPR, Article 4(7)

[11] GDPR, Article 4(8)

[12] Article 29 Data Protection Working Party, Opinion 1/2010 on the concepts of "controller" and "processor", Adopted 16 February 2010, 00264/10/EN, WP169, page 25

1. EXTRATERRITORIAL APPLICATION OF GDPR

The territorial application of GDPR is dealt with in Article 3. The drafters of the GDPR sought to draft this Article in a way that would maximise the protection afforded to Data Subjects within the EU despite the borderless nature of the internet. As a result of this aim, Article 3 contains wording that results in the GDPR being applicable outwith the boundaries of Member States. This Chapter will examine the provisions of Article 3(1) which is focused on the establishment of the entity in the EU and Article 3(2) GDPR which focuses on the targeting of EU Data Subjects by entities not located in the EU.

This chapter will not focus on the possible basis for jurisdiction contained in Article 3(3) GDPR which states that GDPR will apply to the processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law, for example in Member State's overseas territories[13]. Therefore, if EU law applies in a country which is not a member of the EU, the GDPR will apply. As it is not believed that this basis of jurisdiction requires significant interpretation or analysis, it has not been examined in this dissertation.

1.1 Article 3(1): The Establishment principal

Article 3(1) GDPR states that GDPR will be applicable when there is "*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*"[14].

This article is using the *establishment principle* in order to justify the applicability of the GDPR[15]. Under this principle, the choice of laws in based on where the entity has its establishment, not where the activity (data processing) is actually being carried out.

This article targets entities that are not located within the territory of the EU, but which might undertake activities in one or more Member state, potentially though subsidiaries, international branches or potentially just the presence of one representative. For example, an international company which has its head office in the United States of America but also has subsidiaries located within one or more EU Member State. Even if the subsidiaries themselves do not undertake any processing activities, if they were considered to be "establishments" of the US head office, and the processing of

[13]GDPR, Article 3(3)

[14] GDPR, Article 3(1)

[15] Voigt, A. von dem Bussche, *The EU General Data Protection Regulation (GDPR), A Practical Guide*, Springer, 2017 (hereafter referred to as Voigt and von dem Bussche, GDPR, A Practical Guide), page 22

data undertaken by the US head office was considered to be processing "in the context of activities" of the subsidiaries, then the US head office would have to comply with the GDPR despite the fact that the processing does not take place within the EU and the entity's head office is located outwith the EU.

In order to understand the scope of this article, it is necessary to examine when a Data Controller or Data Processor will be considered to have an "Establishment" in a Member State. In addition, Article 3(1) requires that we define what is meant by the requirement that the data processing must be carried out "in the context of the activities" of the establishment located in the EU.

(a) Meaning of "Establishment"

For GDPR to be applicable under Article 3(1) GDPR, the Data Processor or Data Controller must have an "Establishment" located in the EU. Although the GDPR does not give us an exact definition of "Establishment", Recital 22 GDPR provides us with some guidance as to how it should be interpreted. The Recital states that "Establishment" should be interpreted as "the effective and real exercise of activity through stable arrangements"[16]. The Recital also makes it clear that the legal form of the body located in the EU is not important when determining if it is an Establishment, therefore, the body could be a subsidiary of a parent company or a branch[17].

The wording "effective and real exercise of activities through stable arrangements" is almost identical to that contained in Recital 19 of the Data Protection Directive. Therefore, existing case law of the European Court of Justice (hereafter referred to as the "ECJ") can serve as guidance as to the definition of Establishment despite being decided before the GDPR came into force.

In the case of Google Spain, Google Spain SL and Google Incorporated v Agencia Espanola de Proteccion de datos (AEPD) and Costeja Gonzalez (hereafter referred to as the Google Spain case) the ECJ held that "Establishment" cannot be defined restrictively[18].

The Weltimmo sro v Nemzeti adatvédelmi és informacriowabadsag hatosag (hereafter referred to as the Weltimmo case)[19] is another important case when interpreting what is meant by the "effective and

[16] GDPR, Recital 22

[17] Ibid

[18] Judgement of the Court of the European Union (Grand Chamber) of 13 May 2014, Google Spain, Google Spain SL and Google Incorporated v Agencia Espanola de Proteccion de datos (AEPD) and Costeja Gonzalez, Case C-31/12, EU:C:2014:317, (hereafter referred to as Google Spain), recital 53

real exercise of activities through stable arrangements" as detailed in Recital 22. It was held that when determining if the activity is undertaken through "stable arrangements", we must to consider the type of economic activity of the entity and the services which they offer[20]. This indicates that the circumstances of each individual case are important, and the context must be taken into account when considering if the activities are being undertaken through stable arrangements. For example, in the context of certain activities, even if only one person is present in a Member State, if this person provides services with a certain degree of stability, it could be sufficient to establish that that the Data Controller or Processor has an "Establishment" in the EU[21]. Consequently, GDPR would be applicable in the circumstances.

Traditionally, entities would only have one Establishment and it would be considered to be located in the state where it was registered, however, in the Weltimmo case the ECJ has already departed from this formalistic approach[22]. However, the place of registration of an entity could serve as an indication of its Establishment in that state, but it is not decisive.

There are some limits to what could be considered an Establishment, in the Verein für Konsumenteninformation v Amazon EU Sàrl case it was held that the mere accessibility of an entity's website in one or more Member State would not be considered sufficient to constitute an Establishment[23]. It is generally deemed necessary to have a stable presence and some human and technical resource[24].

(b) In the context of activities

In terms of Article 3(1), for GDPR to be applicable, the processing of the personal data needs to take place "in the context of activities" of the Establishment located in the EU. This indicates that the Establishment must be involved in the activities which result in the processing of the data[25]. We

[19] Judgement of the Court (Third Chamber) of 1 October 2015, Weltimmo sro v Nemzeti adatvédelmi és informacriowabadsag hatosag, Case 230/14, EU:C:2015:639) (hereafter referred to as Weltimmo)

[20] Ibid, Recital 29

[21] Ibid, paragraph 30

[22] Ibid, Recital 29

[23] Judgement of the Court (Third Chamber) of 28 July 2016, Verein für Konsumenteninformation v Amazon EU Sàrl, Case C-191/15, EU:C:2016:388, paragraph 76

[24] Article 29 Data Protection Working Party, Opinion 8/2010 on application law, Adopted on 16 December 2010, 0836-02/10/EN, WP 179

[25] Ibid

therefore need to determine what falls within "the context of activities" of the Establishment. The Google Spain case provides us with some guidance.

The Google Spain case related to a Spanish lawyer called Costeja Gonzalez who argued that his right to privacy and his right to be forgotten had been breached by the Spanish newspaper "*la Vanguardia*" and Google Spain and Google Incorporated. The newspaper had published an article relating to a court case involving Gonzalez and the forced sale of property for the recovery of debt. This article was available through the google search engine. These court proceedings had taken place 12 years before and there were no outstanding issues. Gonzalez wished to have the article either removed or made inaccessible when searched online.

The Spanish data protection agency (AEPD) held that the Newspaper was not in breach as they had lawfully published the article in accordance with government order. However, Google Spain and Google Inc. were requested to remove the article from their search results so the article would not be available when searched through Google. This case was appealed to the National High Court in Spain who referred several questions to the ECJ.

The ECJ famously ruled that a company that controls a search engine is a Data Controller regarding the processing of personal data though locating, indexing, storing and disseminating the information that can be searched through their engine. The ECJ had to consider whether EU Data Protection legislation was applicable to the processing of this data through the internet search engine of Google Inc. which is a non-EU located company but which has local entities in the EU (in this case Google Spain). One of important questions that the ECJ had to consider was whether the data processing undertaken through the search engine of Google Inc. could be considered as being undertaken "in the context of the activities" of its subsidiary Google Spain (the Establishment). The activities of the Google Spain were to represent Google locally and to sell advertising space.

Firstly, the ECJ confirmed that the processing only needs to occur "in the context of activities" of the Establishment, it is not necessary of the Establishment to carry out the processing themselves[26]. Therefore, it was not decisive that the data processing was undertaken by the entity which was not located in the EU. It was also held that the words cannot be interpreted restrictively[27]. Importantly, it was held that the activity of operating a search engine was clearly linked to the activity of selling advertising space which was the main activity of the subsidiary in Spain[28]. The reasoning was that the

[26] Google Spain, supra note 18, Recital 9

[27] Ibid, paragraph 53

[28] Ibid, paragraph 56

search engine was economically profitable due to the selling of advertising space and the success of the search engine (the processing of data) was necessary for the activity of selling the advertising space (the activity of Google Spain)[29].

What we can take from this decision is that there must be an economic activity that links the Establishment to the data processing[30]. In the Google Spain case, the selling of advertising space allows for the search engine to be profitable and the success of the search engine was necessary for the selling of advertising space. There is a clear economic link between the data processing and the activities of the Establishment.

(c) Summary

We can see that a broad interpretation should be given to the words "Establishment" and "in the context of activities" when considering if a non-EU entity has an Establishment in the EU and if the data processing is undertaken in the context of activities of this EU resident Establishment.

In order to be considered to have an Establishment in a Member State, it seems that it will be necessary to have a certain level of human and technical resource, but even one employee with a laptop could be enough to render GDPR applicable[31].

A link must exist between the processing of the data and the activities of the Establishment, but that link does not necessarily have to be an obvious and direct link. As we have seen in Google Spain, an activity that creates revenue which allows and results in the processing is sufficient[32].

1.2 Article 3(2): Lex loci solutionis

After having examined the potential basis for extra-territorial jurisdiction of GDPR under Article 3(1), it is important to examine the basis for jurisdiction contained in Article 3(2) GDPR.

---

[29] Ibid

[30] Ibid, Recital 52

[31] B.Van Alsenoy, *Reconciling the (extra)territorial reach of the GDPR with Public International law*, Data Protection and Privacy Under Pressure, Transatlantic Tensions, EU surveillance, and big data, Gert Vermeulen and Eva Lievens (Eds), Maklu-Publishers, 2017, (hereafter referred to as Van Alsenoy, the extraterritorial reach of GDPR and Public international law) page 84

[32] Paul de Hert and Michal Czerniawski, *Expanding the European data protection scope beyond territory: Article 3 of the General Data Protection Regulation in its wider context*, (2016) 6 IDPL 230, page 237

Article 3(2) GDPR states:

> "This Regulation applies 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"

Therefore, GDPR can apply even if neither the data processor nor the data controller is established within a Member State.

The EU legislature are using the principle of *Lex loci solutionis* to justify the application of European Union law in this situation[33]. Under this principle, the applicable law is established based on where the relevant contractual performance is being offered or where the monitoring of personal behaviour of the Data Subject is taking place.

Article 3(2) provides two ways in which the GDPR will be applicable despite neither the Processor nor the Controller being located in the EU. Firstly, at Article 3(2)(a) it is provided that GDPR will apply if there is processing of personal data in relation to the offering of goods or services to data subjects in the EU. Secondly, at Article 3(b) GDPR will apply when processing of personal data is undertaken in relation to the monitoring of personal behavior of a data subject if this behavior occurs within the EU.

These two possible bases for extra-territorial jurisdiction will be examined in turn.

(a) Article 3(2)(a)

GDPR applies if a company undertakes data processing in relation to the offering of goods or services to Data Subjects in the EU, this applies even if the goods are services are offered for free. This is a clear example of GDPR trying to adapt to the modern age where international entities are able to offer their goods or services over the internet to customers despite not being physically present in the same country as said customers. The drafters of the GDPR clearly wanted to avoid the situation where a non-EU located entity could extend their business to customers in EU Member States but, in order to

[33] Voigt and von dem Bussche, GDPR, A Practical Guide, supra note 15, page 26

avoid the application of GDPR, they do not create any kind of presence within the Member State and simply offer their goods or services over the internet.

In order to understand the scope of this article it must be considered whether the Data Controller or Data Processor specifically targets clients that are located in the EU[34]. There must be an intention to attract customers in one or more EU country[35]. This means that there must be some kind of positive action on the part of the entity. The fact that a company's website is available to customers located in the EU, or the fact that they have used a language which is generally used in the country where the controller is established (for example an American company using English) will not, on its own, be sufficient to establish that the company was targeting customers in the EU[36].

However, recital 23 GDPR specifies some situations where it could be considered that an entity is targeting Data Subjects in the EU. For example, the use of a language which is generally spoken in one or more EU member state[37] or the acceptance of a currency used in Europe (especially if Euros are accepted)[38]. Other indications that a company is targeting people in the EU is the specific mentioning customers from Europe[39], or offering delivery to one or more member states[40].

By way of example of a situation where GDPR would apply by virtue of Article 3(2)(a), imagine an American company that sells clothes online. Their website is in English; however, they offer the possibility to pay for products in Euros or pounds and offer delivery of goods to various EU countries. In this scenario, GDPR would be applicable even though the company is not located in a Member state because it would be considered that the company is targeting customers located in the EU by allowing customers to pay in a currency used in Member States and by offering delivery in Member States. The US company could be considered to be targeting EU customers which is necessary for the GDPR to apply.

This article of GDPR is based on existing European case law[41] as the EJC has already been asked to clarify in what circumstances an entity "directs activity" towards customers in the EU in the context

[34] GDPR, recital 23

[35] Ibid

[36] Ibid

[37] Ibid

[38] Ibid

[39] Ibid

[40] Ibid

[41] Judgement of the Court (Grand Chamber) of 7 December 2010, Peter Pammer v Reederei Karl Schlüter GmBH & Co. KG, Case C-585/08, EU:C:2010:740 (hereafter referred to as the Pammer case)

of Article 15(1)(c) of the Council Regulation of 22 December 2000[42] which relates to jurisdiction regarding consumer contracts. However, the wording used by this Regulation is different to the GDPR. The Council Regulation refers to when a company "directs activity" to one or more Member State whereas Article 3(2)(a) refers to "the offering of goods or services". However, it is likely that these cases will help interpret the meaning of article 3(2)(a) as the general idea is similar.

These ECJ has provided guidance on when an entity could be considered to be targeting EU customers, for example, if they pay a search engine to prioritise advertising of their goods or services to individuals located in one or more Member State. Other examples include the provision of telephone numbers with international dialling codes, the detailing of the route from one Member State to the location that the services or goods are being offered from or the use of internet domains in the EU (eg .fr or .eu)[43].

In general, it does not take much for an entity to be considered to be offering goods or services to Data Subjects in the EU, however, there does seem to be a requirement of positive action in the targeting of EU customers by the non-EU located entity.

(b) Article 3(2)(b)

Article 3(2)(b) states that the GDPR will be applicable in relation to data processing which involves the monitoring of EU customers' behavior which takes place within the EU. The word "monitoring" could mean the tracking of individuals on the internet or using processing techniques like profiling[44]. When we talk about profiling, we are referring to the commonly used technique of using data in order to predict an individual's preferences, behaviors or attitudes[45]. This information can be very useful to companies and is very commonly used. For example, Facebook uses data collected from users to determine their likes and interests, they then use various algorithms in order to prioritise adverts they think will be of interest to that particular user. This makes their site more attractive to advertisers and Facebook becomes more profitable. There are arguments for and against these techniques, but there is no doubt that they can sometimes be abused. An example of the worrying aspects of these techniques can see from the Cambridge Analytica scandal in 2018 where Facebook users' data was processed without their consent in order to target political advertising. In order to provide an extensive level of

[42] Council Regulation (EC) no 44/2001 of 22 December 2000 on Jurisdiction and the recognition and enforcement of judgements in civil and commercial matters, Official Journal L012, 16/01/2001 P.0001-0023

[43] The Pammer case, supra note 41, paragraph 81 and 83

[44]GDPR, Recital 24

[45] Ibid

protection, GDPR aims to regulate all monitoring EU Data Subjects data even when the Data Controller or Data Processor is not located in the EU.

Article 3(2)(b) replaces article 4(1)(c) of the Data Protection Directive which provided that a Member State must apply their national data protection laws if a Data Controller uses equipment within the territory of said Member State[46]. The use of "equipment" has been given a wide interpretation by the WP29 who state that it extends beyond the normal interpretation of "equipment" which usually means a physical technical resource[47]. The WP29 has interpreted "equipment" to include "means"[48]. The result of this interpretation is that if a non-EU resident entity used means to process data within a Member State, applicability would have been established. This definition would include the use of Web tracking tools such as "cookies" or social media plug-ins[49]. These tools can be used by entities to analyse how users of their website have accessed their website (ie by search engine or online advertising), how long they stay on the website or how many times they have used the website.

Although the inclusion of the use of cookies within the scope of equipment was criticised, the drafting of Article 3(2)(b) appears to reinforce the position[50]. It appears that should a non-EU entity use cookies on the computer of a Data Subject located in a Member State, even if they had not specifically targeted customers within the EU, it could be considered that GDPR applies by virtue of Article 3(2)(b) as the cookies will monitor the behavior of the Data Subject within the EU[51]. Therefore, although it is stated that the mere accessibility of the website of a non-EU resident entity within one or more Member State is not sufficient to trigger the application of GDPR, in reality GDPR could apply due to Article 3(2)(b) as most websites use cookies. However, there could be an argument that often these tools identify devices and not natural persons and therefore should not fall within the definition of the GDPR. Another argument that cookies do not pose a large threat to data protection is that they are stored on the users' computers and can therefore be deleted by the user. However, given advancements in technology, new types of cookies have been developed such as supercookie, evercookies and zombie cookies which are designed to be difficult to find and delete or can even reactive after deletion.

[46] The Data Protection Directive, Article 4(1)(c)

[47] Article 29 Data Protection Working Party, Opinion 8/2010 on application law, Adopted on 16 December 2010, 0836-02/10/EN, WP 179

[48] Ibid, 21-22

[49] Voigt and von dem Bussche, GDPR, A Practical Guide, supra note 15, page 28

[50] Van Alsenoy, the extraterritorial reach of GDPR and Public international law, supra note 31, page 88

[51] Voigt and von dem Bussche, GDPR, A Practical Guide, supra note 15, page 28

(c) Data subjects within the EU

Article 3(2) GDPR makes reference to data subjects "in the EU" or behaviour "within the EU". We can see that the GDPR is moving away from the idea that nationality or residence is important when it comes to the jurisdictional scope of the regulation This is clearly done with the aim of increasing the scope of protection offered by the GDPR to apply to anyone who is located within the territory of an EU Member State.

However, this creates questions, for example when does the customer need to be present in the EU for GDPR to be applicable. It could be assumed that the Data Subject must be in the EU at the time of the data processing[52]. However, imagine a Data Subject that goes on holiday outwith the EU for two weeks, if an entity decides to process their data during these two weeks are they not bound by GDPR because the data subject is not located within a Member state at the point of processing? This is not in line with the clear aim of the GDPR to offer maximal data protection.

A more logical interpretation of Article 3(2) would be that GDPR is applicable if the data subject is located within the EU during the time of collection[53].

[52] Ibid, page 29

[53] Ibid

2. DATA TRANSFER TO THIRD COUNTRIES

After having discussed the possibility of extra-territorial application of GDPR under article 3 GDPR, this Dissertation now turns to examine how the GDPR regulates data transfer from an entity located in a Member State to entities which are located outwith the European Union (hereafter referred to as Third Countries).

Cross-border data transfer is very common. Sometimes entities which are located within the EU wish to send data to Third Countries. As the GDPR seeks to give Data Subjects a comprehensive level of protection, it would defeat the point if an entity which is bound by GDPR could simply transfer the data outwith the EU to entities located in Third Countries which perhaps provide for little to no data protection in their national law.

To better illustrate when data transfer might occur, imagine a French company that sells cheese throughout Europe. The French cheese company keeps a list of their clients' data and personal information and they have outsourced the storage of said data to an American company. There is little doubt that the GDPR applies to the French Cheese company, the Data Controller. Under Article 3(1), even if the data processing is not undertaken in the EU, the GDPR applies because the entity is established in the EU and the data is processed in the context of their activity of selling cheese.

However, the American company it is located outwith EU territory, it is therefore difficult to impose European Union law. Firstly, the GDPR could apply under Article 3(2)(a) if it was considered that the American company was targeting European customers with their services. If not, normally the European Regulation would not apply. However, the GDPR protects the European resident Data Subject by placing an obligation on the sending entity which is bound by the GDPR to ensure that the data transferred will be protected.

This chapter will first examine the rules relating to cross border data transfer to Third Countries and the different ways the sending entity can adhere to their obligation of ensuring that the data will receive an "adequate level of data protection". Thereafter the focus will turn to the specific situation of data transfer between EU based entities and entities located in the United States of America (hereafter referred to as the US). Transfer of data to the US will be specifically studied given that EU-US data transfer is very common but it also very difficult to regulate given the difference in approaches to data protection in the EU and in the US.

2.1. Rules

When it comes to transferring data from the EU to third countries, the sending entity is required to adhere to certain rules set out in the GDPR. This subchapter will concentrate firstly on the obligations placed on the sending entity. Thereafter, the concentration will turn to the how a Third Country can be considered safe for data transfer in terms of the GDPR. Finally, this subchapter will elaborate on various exceptions provided for by the GDPR that can allow for data transfer to third countries despite there being no assurance that the data will receive an adequate level of protection after transfer.

(a) Adequate Protection

Cross Border data transfer is dealt with in Article 44 GDPR. This article provides that any transfer of personal data that is undergoing processing or that is intended to undergo processing after transfer to a Third Country must comply with Chapter 5 GDPR[54].

In general, in order to determine if the cross-border transfer is legal, entities should apply a two-step approach[55]:

a) The data transfer must correspond to a legitimate basis for processing of data in the EU. In general, data processing of personal data is prohibited but can be allowed in certain circumstances, for example if the Data Subject has consented to the processing or if the processing is required to fulfil a contract or to protect a vital interest[56].
b) The transferring entity must adhere to the obligations detailed in Chapter 5 GDPR.

Both the obligations under points a) and b) need to be respected by the transferring entity for the transfer to be allowed. Under Chapter 5 GDPR, it is stated that transfer to Third Countries can occur in certain circumstances. Under Article 45 data transfer can occur if the receiving entity is in a country (or part thereof) which has obtained an Adequacy Decision granted by the European Commission. Article 46 provides that even if an Adequacy Decision cannot be relied on to justify the transfer, data transfer can occur if "appropriate safeguards" are put in place. Finally, Article 49 details various derogation which will allow for transfer despite there being no Adequacy Decision nor any appropriate safeguards put in place.

[54] GDPR, Chapter 5 contains Articles 44 to 50

[55] Voigt and von dem Bussche, GDPR, A Practical Guide, supra note 15, page 117

[56] GDPR, Article 6

(b) Article 45: Transfers based on an Adequacy Decision

There are some countries which the European Commission has granted Adequacy decisions, this means that they are considered to be "safe third countries" and are deemed to provide adequate levels of data protection under their national laws[57]. Data can be transferred to these safe third countries without the need to seek authorisation from the relevant Data Protection Authority[58].

Article 45 section 2 GDPR sets out the requirements a country must fulfil in order to receive an adequacy decision. Essentially the European Commission will undertake an overall assessment of the data protection offered by the third country when deciding if their data protection legislation is sufficient[59].

At the time of writing, the European Commission have awarded adequacy decisions to Andorra, Argentina, Canada, Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland, Uruguay and the United States of America (limited to the Privacy Shield framework which will be discussed in more detail in Chapter 2.2). Adequacy talks are also ongoing with South Korea[60].

(c) Article 46: Appropriate Safeguards and Article 49: permitted derogations

Under Article 46 GDPR, even if the transferring entity cannot rely on an Adequacy Decision, they can still transfer data to an entity located in the Third Country if "appropriate safeguards" are put in place to protect the data. The GDPR details the safeguards which are considered appropriate. For example, the sending entity can use the EU Standard Contractual Clauses (SCC)[61]. SCC are approved by the EU Commission and if an EU entity incorporates them into their contract with the receiving party located in a Third Country, the transfer is allowed. These contractual provisions will bind the receiving party and obligate them to protect the data in accordance with the SCCs.

Another appropriate safeguard relates to international companies which are present in both the EU and in Third Countries and that wish to transfer data from the EU located branches to the non-EU

[57] GDPR, Article 45

[58] GDPR, Article 45, Sec. 1 phrase 2 ; Recital 2013

[59] Voigt and von dem Bussche, GDPR, A Practical Guide, supra note 15, page 117

[60] The European Commission, Adequacy Decisions, how the EU determines if a non-EU country has an adequate level of data protection, https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en, last accessed 10 July 2019

[61] GDPR, Article 46(2)(c) and (d)

located branches. In these circumstances, an international company could adopt what is called "Binding Corporate Rules"[62] (hereafter referred to as BCR). The BCR will define the global data privacy policy for all the enterprises in the group. If the European Commission considers the BCR adopted by the group to provide sufficient data protection, then data can be transferred to Third Country located branches[63]. However, Article 3(1) would render GDPR directly applicable to the non-EU resident parts of multinational groups with subsidiaries and branches located in the EU so long as any data processing undertaken was undertaken in the context of activities of the EU resident parts. Therefore, it is a little unsure whether BCRs are still necessary given the scope of applicability of the GDPR.

The GDPR allows for data transfer despite there being no adequacy decision nor appropriate safeguards in place in certain circumstance. One example would be if the Data Subject has consented to the transfer[64].

The GDPR states that the consent to the data transfer can only occur if the Data Subject has "been informed of the possible risk of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards"[65]. This consent has to explicitly relate to the transfer of the personal data, implicit consent would not be sufficient[66]. The question remains as to what extent and how the Data Subject must be informed of the possible risks of the transfer. It is felt that the transferring entity should, as part of the consent declaration, state that they cannot guarantee a level of protection equivalent to the GDPR after transfer[67]. The transferring entity should also inform the Data Subject what data will be subject to transfer and the location to which it will be transferred. It is clear that there remains some questions as to how much information the Data Subject must be provided with in order to give their valid consent[68]. It is not clear if specific risks regarding the Third Country

[62] GDPR, Article 46(2)(b) and Article 47

[63] Intersoft Consulting, *GDPR Third Countries*, www.gdpr-info.eu/issues/third-countries/, last accessed 8 August 2019

[64] GDPR, Article 49(1)(a), however, this exception is not applicable to public authorities carrying out activities in the exercise of their public powers (GDPR, Article 49(3))

[65] GDPR, Article 49(1)(a)

[66]Voigt and von dem Bussche, GDPR, A Practical Guide, supra note 15, page 118

[67] Von dem Bussche, K. U. Plath, (ed) (2016) Arts. 2, 3 DSGVO.In: BDSG/DSGVO, 2nd edn. Verlag Dr Otto Schmidt, Cologne and Article 49 (2016), rec. 2.

[68] Voigt and von dem Bussche, GDPR, A Practical Guide, supra note 15, Page 118

must be communicated[69]. However, it is clear that Data Subjects can withdraw their consent to the transfer at any moment.

Data transfer to a Third Country is legal if it is required for the entity to exercise or defend a legal claim[70] or if the transfer is necessary for the performance of the contract between the Data Subject and the transferring entity[71]. Although there are some safeguards in place as it is necessary that there is a direct link between the performance of the contract and the transfer. In addition, if the contract can be fulfilled without the Third Country data transfer, then the transfer would be illegal. The transfer is only legal with regards to the data which must be sent for the performance. Transfer can also occur if it is necessary for the performance of a contract with a third party if that contract was made in the interest of the Data Subject[72].

Transfer can also occur for reasons of public interest[73]. The Public Interest will be interpreted in accordance with the national law of the Member State of the transferring entity. Transfer is also legal if it is for the protection of a vital interest of the Data Subject or other person but only where the Data Subject cannot lawfully give consent[74].

The GDPR created a new exception, transfer can take place if it corresponds with a legitimate interest of the Data Controller[75]. This exception can only be used if there is no other legal way the data could be transferred and if the controller adheres to certain conditions for example the transfer cannot be repetitive or relate to an indeterminate amount of Data Subjects. There is also a proportionality test, legitimate interest of the Data Processor must be balanced against the rights of the Data Subject. The Transferring entity still needs to ensure suitable safeguards are in place after the transfer and there is an obligation to inform the national Supervisory Authority about the transfer, inform the Data Subject of their legitimate interest and document the assessment that was undertaken and what safeguards were put in place to protect the data[76].

[69] Von dem Bussche, K. U. Plath, (ed) (2016) Arts. 2, 3 DSGVO.In: BDSG/DSGVO, 2nd edn. Verlag Dr Otto Schmidt, Cologne

[70] GDPR, Article 49(1)(d)

[71] GDPR, Article 49(1)(b)

[72] GDPR, Article 49(1)(c)

[73] GDPR, Article 49(1)(d)

[74] GDPR, Article 49(1)(f)

[75] GDPR, Article 49(1)(2)

[76] Voigt and von dem Bussche, GDPR, A Practical Guide, supra note 15, page 133

2.2. EU/US Privacy Shield

The attitude towards data protection in the EU is very different from the attitude in the US[77]. Where the legislators of the EU have tried to create a universal system of protection, the legislators in the US have taken a different approach. In the US there is no federal law regarding data protection. US legislation relating to data protection is often referred to as "piecemeal legislation" by data privacy experts[78]. The attitude of the government is that people are free to do what they wish with their data, and there is a concentration on the commercial benefits the come from data processing. There are also concerns that US legislation provides for unfettered access to personal data by US Intelligence services in the aim of national security. In the EU, data protection legislation is aimed to be global and protective of the rights of individuals.

This difference in culture and approach to data protection has created difficulty between the two jurisdictions regarding data transfer. While neither party either side of the Atlantic wishes to hinder data transfer between the EU and the US, it has not been an easy road to achieving a deal between the EU and the US regarding cross border data transfer that both parties could accept.

In the EU, the Data Protection Directive came into force in 1995 and introduced the requirement that data transferred to Third Countries required adequate protection after transfer. It was therefore necessary to evaluate if it could be considered that data transferred to the US would receive adequate data protection after transfer. In 1999, the WP29 evaluated data protection in the US and concluded that it did not provide adequate data protection due to their "patchwork of narrowly focused sectoral law" and the fact that in the US entities were left to self-regulate regarding data protection[79].

However, as mentioned, trade between the US and the European Union is very important to both sides. Therefore, the European Commission and the US Department of Commerce (DoC) started negotiations in order to agree to certain rules relating to the treatment of data which is transferred between the EU and the US. As a result, The *Safe Harbour* agreement was accepted by both sides in 2000. This subchapter of the Dissertation will examine the *Safe Harbour* agreement and its eventual

[77]P. M. Schwartz and K. Peifer, *Transatlantic Data Privacy*, 106 Georgetown Law Journal 115 (2017) UC Berkley Public Law Research Paper, page 115 (hereafter referred to as "P Schwartz et al, Transatlantic Data Privacy")

[78] James Q. Whitman, *The Two Western Cultures of Privacy: Dignity versus Liberty*, 113 YALE L.J. 1151, 1153 (2004): 1159

[79] Article 29 Data Protection Working Party, Working Document on determining the international application of EU data protection law to personal data processing on the Internet by non-EU based web sites, Adopted 30 May 2002, 5035/01/EN/Final, WP 56, at 2

downfall before going on to look at the agreement that replaced it, the US the EU/US Privacy Shield[80] (hereafter referred to as "Privacy Shield").

(a) Safe Harbour

When *Safe Harbour* was granted an adequacy decision in 2000, it did not provide the same level of data protection as the Data Protection Directive. This was always going to be the case, given the very different attitude to data protection in the US, the Department of Commerce were never going to accept a deal which provided the same level of protection as the Data Protection Directive. That being said, Safe Harbour was considered by the European Commission to provide "adequate data protection"[81]. As time passed, the EU became less happy with the protection offered by Safe Harbour as issues became more evident.

Eventually, the adequacy decision given to *Safe Harbour* was overturned 15 years after it was granted by a decision of the ECJ in the Maximillian Schrems case on 6 October 2015[82]. This case was brought before the ECJ after information was leaked by Edward Snowden regarding widespread global surveillance programmes run by the American intelligence services[83]. Schrems was an Austrian national and a user of the site Facebook. He started an action with the Irish Data Protection Commissioner arguing that Facebook Ireland had transferred his data to the United States and as a result they had breached the Data Protection Directive which provided that the sending entity required to provide for adequate data protection on transfer of the data[84]. The Irish Data Protection authority dismissed the case stating that adequate protection was provided as Facebook was registered under Safe Harbour[85]. The case was appealed to the Irish High Court and subsequently referred to the ECJ[86].

---

[80] The European Commission, 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-US Privacy Shield, Official Journal, L 207/1, p1

[81] P Schwartz et al, Transatlantic Data Privacy supra note 77, page 159

[82] Judgement of the Court (Grand Chamber) of 6 October 2015, Maximillian Schrems v Data Protection Commissioner, Case C-362/14, EU:C:2015:650, (hereafter referred to as Schrems)

[83] In 2013 Edward Snowden disclosed information regarding how the US National Intelligence Agency used global surveillance programmed using information provided by telecommunication companies (such as Microsoft, Google, Apple, Yahoo, Facebook and YouTube) and European governments.

[84] Court of Justice of the European Union Press Release, The Court of Justice declares that the Commission's US Safe Harbour Decision is invalid, Press Release No. 117/15, Luxembourg, 6 October 2015 (hereafter referred to as the ECJ press release No. 117/15)

[85] M. A. Weiss and K. Archick, *US-EU Data Privacy: From Safe Harbour to Privacy Shield*, Congressional Research Service, 19 May 2016

The ECJ ruled that Safe Harbour did not provide sufficient protection. It was held that in the granting of the adequacy decision the European Commission had failed to confirm that US domestic law provided protection to personal data which was essentially equivalent to that under the Data Protection Directive[87]. The ECJ therefore clarified that an "adequate level protection" when dealing with Third Country data transfer should be taken to mean "essentially equivalent" protection to that provided under EU law. The ECJ held that Safe Harbour did not provide an adequate level of protection given that the US public authorities were not bound by Safe Harbour, it related only to US owned undertakings[88]. The data could be accessed by the US intelligence services as soon as the personal data was transferred to the US. It was not clear if US law provided for limitations to this access[89]. This criticism was a clear result of the information leaked by Snowden regarding the access of the US intelligence agencies to EU citizen's data and the mass storage of said data[90]. The ECJ also condemned *Safe Harbour* because there was no real remedy provided for Data Subjects in case of breaches[91].

As a result of the demise of *Safe Harbour*, the European Commission and the US Department of Commerce began talks so that data could still be transferred between the EU and the US. This resulted in the negotiation and the acceptance by both sides of the new agreement, Privacy Shield, which was granted an adequacy decision on 12 July 2016[92].

(b) Privacy Shield Principles

Privacy Shield, like *Safe Harbour*, allows US based companies to self-certify their compliance with its provisions. Entities must register with the US Department of Commerce who is responsible for monitoring compliance. In order to register an US entity must have a privacy policy that is in line with the standards provided for under Privacy Shield. The idea is that once an entity is registered, they

---

[86] Thomas Clabum, *Safe Harbour Fails, European Court Rules*, InformationWeek, 19 May 2016

[87] Sidley, *Esentially equivalent, A comparison of the Legal Order for Privacy: From the European Union and the United States*, 25 January 2016, 9, 10

[88] ECJ press release No. 117/15, supra note 84

[89] M. A. Weiss and K. Archick, *US-EU Data Privacy: From Safe Harbour to Privacy Shield*, Congressional Research Service, 19 May 2016, 7

[90] Schrems, supra note 82 at 93

[91] Ibid, recital 88-89

[92] 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-US Privacy Shield, OJ L 207, 1.8.2016

are deemed safe under the GDPR and they can receive data transfers from entities that are bound by the GDPR. Privacy Shield registered entities must renew their registration on a yearly basis. Privacy Shield is also reviewed on a yearly basis by the US Department of Commerce and the European Commission[93].

Privacy Shield provides for seven privacy principles to which the US entity must adhere in order to self-certify under Privacy Shield. These principles existed under Safe Harbour but they have been adapted after the ECJ's decision in the Maximillian Schrems case.

In order to try and address the issues detailed a Schrems, Privacy Shield addresses the possible access to personal data of EU resident Data Subjects by US government. One of the changes brought by Privacy Shield was the creation of the position of a US Ombudsperson who is independent from the US national security services[94]. The role of this Ombudsperson is to hear complaints from EU data subjects with regards to the use of their personal data by US intelligence agencies for national security reasons.

[93]European Commission Press Release, European Commission launches EU-US Privacy Shield: Stronger Protection for transatlantic data flows, Brussels 12 July 2016

[94] Communication from the Commission to the European Parliament and the Council Transatlantic Data Flows: Restoring Trust Through Strong Safeguards, Brussels, 29 February 2016, COM (2016) 117 final

3. GDPR: THE COMPREHENSIVE FRAMEWORK REGULATING DATA PRIVACY INTERNATIONALLY

The legislature of the EU aimed to bring data protection into the 21st century by providing Data Subjects within the EU with the most complete protection possible for their data in a world where the internet is ubiquitous and borderless. The measures explained in the previous two Chapters of this Dissertation are some of the measures taken by the EU in order to try and guarantee a comprehensive framework to regulate data protection internationally. This Chapter will concentrate on the different ways that the GDPR could be considered to have made advancements regarding this aim.

The first part of this Chapter concentrates on the positive changes relating to the extra-territorial scope of the GDPR which could arise from Article 3 GDPR. The second part will focus on the improved protection offered by the GDPR regarding data transfer to third countries.

Before elaborating on the positive improvements specifically relating to the extra-territorial scope of the GDPR and data transfer to third countries, there is one important change that applies to both these areas. The GDPR has greatly increased the possible fines that can be levied by national Supervisory Authorities for data breaches in comparison to the Data Protection Directive.

Some breaches of the GDPR can lead to fines of up to 10 million euros or 2% of the total worldwide annual turnover of the preceding financial year[95]. These fines relate to various breaches including the non-respect of obligations relating to child consent[96] and breaches relating to organisational requirements[97].

The GDPR has also increased fines for breaches for non-respect of the rules relating to the transfer of data to third countries[98]. Entities could face fines of up 20 million euros or up to 4% of annual worldwide turnover[99].

This higher fine can also be applied to other breaches including breaches of basic principles for processing, including conditions for consent and processing of special categories of personal data[100].

[95] GDPR, Article 83(4)

[96] GDPR, Article 8

[97] GDPR, Articles 25 to 39

[98] GDPR, Articles 44-49

[99] GDPR, Article 83(5)

[100] GDPR, Articles 5, 6, 7, 9

The GDPR came into force slightly over one year ago at the time of writing and some enormous fines have already been levied against companies for data breaches. In July 2019, the UK's Information Commissioner's Office (ICO) fined British Airways £183.4 million for a data breach which resulted in around 500,000 customers details being diverted and collected by a different website between June and September 2018[101].

In addition, in July 2019 the Marriot hotel group was fined £99.2 million by the ICO. The hotel chain was fined due to a cyber-breach that originated in another hotel chain which was later purchased by Marriot. Around 339 million guests' personal details were leaked as a result[102].

These huge fines provide a strong incentive for companies to pay attention to their obligations and do their utmost to avoid possible data breaches.

[101] The Information Commissioners Office, *Intention to fine British Airways £183.39m under GDPR for data breach*, 08 July 2019 www.ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/07-announces-intention-to-fine-british-airways/

[102] The Information Commissioners Office, *Intention to fine Marriott International, Inc more than £99 million under GDPR for data breach*, 09 July 2019 www.ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/07/intention-to-fine-marriott -international-inc-more-than-99-million-under-gdpr-for-data-breach/

3.1 Extra-territorial scope

This Chapter will concentrate on how the GDPR could be seen to provide a harmonised mechanism for data protection internationally given the extra-territorial scope possible under Article 3 GDPR.

(a) An EU Regulation: Harmonising data protection law throughout the EU

The Data Protection Directive was that Directives of the European Union, meaning it was not directly applicable in Member States. It had to be implemented by legislation of the national legislature of the Member States before it was enforceable. This meant that not all Member States had exactly the same data protection laws as different Member States implemented the Data Protection Directive differently and provided varying levels of data protection.

As a result, entities could choose the location of their EU offices depending on which state had data protection regulations that aligned with their aims. Although the ECJ was already trying to limit this practice, this is no longer an issue as the GDPR is an EU regulation which means that it is directly applicable and enforceable in Member States without the need for national legislature to implement it. As a result, data protection is harmonised throughout the EU.

This can be seen as a positive advancement when it comes to the level of data protection offered. All the Member States of the EU are more powerful than one Member State. Now that the GDPR provides for a high level of data protection throughout the entire EU, this could put pressure on entities that are not located in the EU but wish to enter the EU market to adhere to the GDPR. Before, if one Member State provided for a higher level of protection, a non-EU entity could just avoid that Member State, it is objectively less convenient to avoid the entire EU now that data protection laws are harmonised.

(b) Article 3(1) GDPR: a reinforcement of the ECJ's decisions

The Data Protection Directive was enacted in 1995, it is hard to deny that society has changed in the past 25 years. The Data Protection Directive was created at a time where data processing was less complex, it mostly related to physical processing within the borders of a state.

The jurisdictional scope of the Data Protection Directive was essentially territorial. It was applicable to the processing of data when "the processing is carried out in the context of the activities of an

establishment of the controller on the territory of a Member State"[103]. This means that if the Data Controller was located outwith the EU, even if they had other establishments within the territory of the EU which were not involved in the processing of the data, the Data Protection Directive would not apply to their processing activities[104]. However, with technical developments, it became possible to process data at a distance and the Data Protection Directive was arguably out of date.

It fell to the ECJ to adapt the outdated Directive to fit with modern times. It has been mentioned that the *Google Spain* decision adapted the Data Protection Directive to apply even when the establishment which was located in the EU did not themselves carry out the processing activities but they were involved in activities which made the service profitable, the selling of advertising space[105]. Although the GDPR does not change the position, it reinforces the decision of the ECJ in Google Spain by clearly stating that the processing activity itself does not need to occur within the EU, the GDPR would be applicable if the Data Controller or the Data Processor has an establishment in the EU[106].

One positive advancement of this article in comparison to the Data Protection Directive is that it is expressly stated that the GDPR is applicable if the data processing is undertaken in the context of activities of an establishment of either the Data Controller or the Data Processor. Under the Data Protection Directive, there was only reference to the Establishment of the Data Controller[107]. As a result, even if only the Data Processor had an establishment in a Member State, and the processing was undertaken in the context of activities of that establishment, this would be considered enough for the GDPR to apply. This would be the case even if the Data Controller was located in a Third Country and has no presence in the EU. This is a clear extension of the possible application of the GDPR in comparison with the Data Protection Directive in response to the way data is processed in today's society.

(c) Article 3(2) GDPR: a borderless solution for a borderless internet

When it comes to the applicability of EU data protection laws, the biggest change brought by the GDPR is the extra-territorial application which is created by Article 3(2). Under Article 3(2) GDPR is

[103] The Data Proection Directive, Article 4(1)(a)

[104] Adèle Azzi, *The Challenges Faced by the Extraterritorial Scope of the General Data Protection Regulation*, 9 (2018) JIPITEC 126 para 17 (hereafter referred to as A. Azzi, the challenges faced by the extra-territorial scope)

[105] Google Spain, supra note 18, at 317

[106] GDPR, Article 3(1)

[107] Data Protection Directive, Article 4(1)(a)

applicable to any processing of data by a Data Controller or Data Processor which is not located with the EU but who (a) offers good or services to Data Subjects within the EU or (b) monitors their behaviour to the extent that their behaviour occurs in the EU.

The EU legislature wanted to give EU Data Subjects a comprehensive system of data protection. The issue they faced was how to respond to the situation where the Data Controller or Data Processor has no presence in the EU but taps into the EU market by offering goods or services to EU customers (likely over the internet) or by monitoring EU Data Subjects behaviour. The EU has tried to face this challenge head on by adopting Article 3(2) which extends the territorial scope of the GDPR to a greater extent than should have been possible using the wording of the Data Protection Directive.

When it came to the application of the Data Protection Directive, Article 4(1)(c) stated that it would apply even if the Data Controller was not located within the EU, but he makes use of equipment in the EU for processing the data. Under article 4(1)(c) the focus was on the location of the equipment used by the Data Processor. Under article 3(2) the focus is now on the location of the Data Subject. It could be argued that the switch in focus is a positive step forward with regards to the level of protection it offers EU Data Subjects as there was a level of ambiguity regarding what constituted "equipment"[108].

When the Data Protection Directive was drafted, "equipment" was probably in reference to physical equipment such as a main-frame computer and servers[109]. However, with advancements in technology, the WP29 amended the definition by stating that a Data Controller that is not located within the EU would be considered to have used equipment in the EU if he places cookies on a personal computer located in the EU[110]. In addition, the use of JavaScript, banners and spyware in the EU was also considered the use of "equipment"[111]. However, the WP29 stated this interpretation should only be used to establish extraterritorial applicability when it was reasonable and necessary[112].

[108] S. Bu-Pasha, *Cross Border Issues Under EU data protection law with regards to personal data protection*, Information and Communications Technology Law 2017, Vol. 26, No. 3, 213-228, 24 May 2017, page 218

[109] A. Azzi, the challenges faced by the extra-territorial scope, supra note 104, paragraph 18

[110] Article 29 Data Protection Working Party, Working Document on determining the international application of EU data protection law to personal data processing on the Internet by non-EU based web sites, Adopted 30 May 2002, 5035/01/EN/Final, WP 56

[111] A. Azzi, the challenges faced by the extra-territorial scope, supra note 104, paragraph 18

[112] Article 29 Data Protection Working Party, Working Document on determining the international application of EU data protection law to personal data processing on the Internet by non-EU based web sites, Adopted 30 May 2002, 5035/01/EN/Final, WP 56, 9

Although the Data Protection Directive was already being inventively interpreted to have an extra-territorial scope, the emphasis on Data Subject under Article 3(2) could be argued to give the EU a more legitimate claim to applicability of EU law. This is because the European Union has more of a connection and more of a legitimate interest in applying their laws to a situation that affects people located on EU territory than if they just concentrate on the location of the equipment[113].

In general, Article 3(2) GDPR is essentially the solution of the EU to protect EU Data Subjects while taking into account the fact that risk to said protection is not limited to what happens within the boundaries of the EU. Issues the EU could face with regard to this ambitious solution will be examined in Chapter 4.1.

3.2 Cross Border data transfer

It has already been stated that cross border data transfer is essential for business. Therefore, the GDPR provides for EU entities to transfer data outwith the borders of the EU in certain cases.

This sub-chapter will focus on the protection provided for by the GDPR when it comes to Third Country data transfer. Then there will be a specific analysis of the changes brought by Privacy Shield.

(a) GDPR: additional safeguards

Third Country data transfer was already regulated under the Data Protection Directive. It is interesting to analyses if the GDPR brought any new provisions which could be seen as an enhancement to the level of data protection offered to EU Data Subjects.

It is considered that the GDPR provides for improved mechanisms for data transfer to Third Countries[114]. The GDPR expressly allows for transfer if BCRs are put in place, this is an update as under the Data Protection Directive as some Member States' law did not recognise the validity of BCRs[115]. The GDPR also simplifies the use of SCC as entities no longer require authorisation from

[113] Misteale Taylor, *Permissions and prohibition in data protection jurisprudence* (2016) 2 brussels privacy hub working paper 3, 18) and M. Czerniawski, *Do we need to use of equipment as a factor for territorial applicability of the EU data protection regime*, in Dan Jerker B. Svantesson and Dariusz Kloza (eds), trans-atlantic data privacy as a challenge for democracy (Intersentia 2017) 221, 232

[114] S. Bu-Pasha, *Cross Border Issues Under EU data protection law with regards to personal data protection*, Information and Communications Technology Law 2017, Vol. 26, No. 3, 213-228, 24 May 2017, page 222

[115] A. Myers, *Top 10 operational impacts of the GDPR: Part 4 – Cross-border data transfers*, 19 January 2016, https://iapp.org/news/a/top-10-operational-impacts-of-the-gdpr-part-4-cross-border-data-transfers/, last accessed 11 August 2019 (hereafter referred to as "Myers, 10 operational impacts of the GDPR"

the relevant Data Protection Authority in order to use SCCs as was required under the Data Protection Directive. It could be argued that simplifying the use of these techniques of ensuring data protection after transfer to a Third Country will encourage entities to use them and thereby ensure for a greater level of data protection.

In the Schrems case, the ECJ stated that when transferring data to Third Countries, the principle that the Third Country must provide for an "adequate level of data protection" should be taken to mean an "essentially equivalent" level of protection as provided under EU law. The GDPR has now codified this principle at Recital 104 of the GDPR.

The GDPR also introduces a new provision relating to requests for data transfer from a court, tribunal or administrative body of a Third Country. The GDPR requires that the transfer can only occur if an international agreement exists between Third Country and the Member State in question[116]. This transfer cannot prejudice the other provisions in the GDPR relating to data transfer. This is generally viewed as being an enhancement of the protection for Data Subjects in the EU as it limits data transfer to an extent. However, given that this is a new provision, how it will work in practice is still to be seen[117].

Under the GDPR the mechanism for obtaining an adequacy decision remains the same, however, the requirements are broader and more detailed. When deciding whether to grant an adequacy decision, the European Commission will take into account the legal system of the location in question, whether there is sufficient access to justice, international law, human rights, public security legislation, defence and national security, public order and criminal law[118]. Adequacy decisions are also subject to periodic review[119] which means that the European Commission can reassess the adequacy decision in light of changes that might have occurred since it was granted.

Under GDPR there are obligation on the transferring entity to provide notice to the Data Subject when they are transferring their data to a Third Country. They require to state what safeguards are in place after transfer (pursuant to an adequacy decision or other appropriate safeguard)[120]. This information

[116] GDPR, Article 48 and Recital 115

[117] D. J. Kessler, J. Nowak and S. Khan, *The Potential Impact of Article 48 of the General Data Protection Regulation on Cross Border Discovery from the United States*, (2016) 17(2) The Sedona Conference Journal 577

[118] Myers, 10 operational impacts of the GDPR, supra note 115

[119] GDPR, recital 107

[120] GDPR, Article 13

must be provided in a very clear and transparent way so that Data Subjects can understand the information[121].

There are some exceptions to the necessity to ensure "adequate protection" after transfer, one of these exceptions is if the Data Subject provides their consent to the transfer. Under the Data Protection Directive the Data Subject required to give "unambiguous consent" to the transfer[122]. Under the GDPR there is a requirement to obtain "explicit consent"[123]. This is a higher burden for companies to obtain consent under the GDPR as the Data Subject will have to actively respond to the question and give their consent.

The GDPR has introduced some elements that did not exist, or were not codified, under the Data Protection Directive. The GDPR has clarified some matters relating to Third Country transfer such as the use of SCCs and BCRs. The GDPR has also reinforced protections by providing broader and more detailed requirements to obtain an adequacy decision.

(b) The aftermath of Schrems: Privacy Shield in comparison to Safe Harbour

As mentioned, the Safe Harbour agreement which allowed data transfer between the US and the EU was ended by the ECJ in the Schrems case[124] on 6 October 2015. The ECJ took issue with the fact that under US law, US intelligence agencies such as the NSA and the FBI could access the personal data of EU Data Subjects which was transferred under Safe Harbour and undertake indiscriminate surveillance on a large scale[125]. Should there be a conflict between Safe Harbour and the US laws relating to intelligence services powers of surveillance, the later would take precedence[126]. There is no denying that sometimes national security interests can trump the right to privacy of an individual. However, under EU law, any invasion of the right to privacy or data protection must be proportional and necessary to meet a general interest recognised by the European Union or to protect the rights and freedoms of others[127]. Therefore, there is no blanket exception to data protection rules for national

[121] GDPR, Article 12

[122] The Data Protection Directive, Article 26(1)(a)

[123] GDPR, Article 49(1)(a)

[124] Schrems, supra note 82

[125] S. Bu-Pasha, *Cross Border Issues Under EU data protection law with regards to personal data protection*, Information and Communications Technology Law 2017, Vol. 26, No. 3, 213-228, 24 May 2017, page 221

[126] Ibid

[127] Article 7 (the right to respect for private life, family, home and communications) of the European Charter of Fundamental Rights and Article 8 (the right to protection of personal data) of the TFEU can be limited in certain circumstances under Article 52(1) of the Charter.

intelligence agencies. Under US law, on the other hand, it seems that there are very few limitations on the intelligence agencies powers to access data.

The ECJ also noted that a number of Safe Harbour registered companies did not comply with the Safe Harbour principles and there was a lack of oversight[128]. In addition, EU Data Subjects did not have remedies available under Safe Harbour to access or correct their data[129].

Privacy Shield is generally seen as an improvement over Safe Harbour in terms of the assurances of data protection for EU Data Subjects. One aspect of Privacy Shield that can be commended is that fact that it is subject to annual review. This means that the European Commission and the WP29 (which was replaced by the EDPB after GDPR came into force) can meet with the US authorities and state any concerns that they might have and seek assurances regarding compliance. This keeps the pressure on the US authorities to ensure that Privacy Shield is being properly implemented and forces them to be more transparent about what is being done in order to adhere to their commitments under Privacy Shield.

The report of the first annual review by the European Commission was published on 18 October 2017. The review stated that Privacy Shield continued to offer a sufficient level of protection for data transfer[130]. The Commission highlighted the improvements over Safe Harbour including increased monitoring of registered companies by the DoC and strengthened remedies for EU Data Subjects to obtain redress[131]. The Commission also stated that there were assurances provided by the US government that access to data transferred under Privacy Shield by public authorities for national security, law enforcement or other public interest reason was not without limits or safeguards[132].

[128] Schrems, supra note 82, paragraph 21

[129] DLA Piper, *Schrems 2.0 – The Demise of Standard Contractual Clauses and Privacy Shield*, 1 July 2019, https://blogs.dlapiper.com/privacymatters/schrems-2-0-the-demise-of-standard-contractual-clauses-and-privacy-shield/, last accessed 10 August 2019

[130] European Commission, "EU-US Privacy Shield: First review shows it works but implementation can be improved", Brussels, 18 October 2017 https://europa.eu/rapid/press-release_IP-17-3966_en.htm, last accessed 10 August 2019 (hereafter referred to as the "European Commission First annual review press release"),

[131] The European Commission, 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(2017) 344 final}, 18 October 2017 Page 2

[132] Ibid

The WP29 also issued a report on the first annual joint review, the WP29 also praised the efforts made the US authorities to support the operation of Privacy Shield[133]. In this respect they praised the procedural checks that are now undertaken by the DoC on the self-certification of registered companies[134].

Regarding the US authorities' access to EU Data Subjects' personal data, the US authorities have been more transparent about the use of their surveillance powers. In this regard they have published some important documents such as decisions from the Foreign Intelligence Surveillance Court (FISA Court). This allows for a better understanding of how the surveillance powers are used and what safeguards are in place to avoid use of these powers in excess of what is necessary[135].

The US authorities have also been more transparent about the mechanism of oversight of intelligence agencies when undertaking their surveillance activities. They stated the oversight was undertaken by a number of entities that were independent from the surveillance community[136]. An important entity in this regard is the Privacy and Civil Liberty Oversights Board (PCLOB) which is an independent entity which publishes reports on privacy matters and has made recommendations which have led to reform of US law. The Department of Justice and the Inspector General also have an oversight role.

Another element of Privacy Shield that did not exist under Safe Harbour is the Ombudsperson mechanism which aims to give EU Data Subject a right of recourse and enforcement against the US authorities who use their surveillance powers in excess of what is necessary. The Ombudsperson hears complaints from Data Subjects and investigates possible breaches. The creation of this mechanism is generally considered as a significant improvement with regards to EU Data Subjects being able to enforce their rights[137].

It seems that Privacy Shield is a significant improvement over Safe Harbour. It has addressed concerns about self-certification by introducing compliance checks and monitoring processes. With regards to the concerns relating to US intelligence services' access to the data transferred under Privacy Shield, the Commission and the WP29 seem to be happy with the greater transparency given

[133] The Data Protection Working Party, EU/US Privacy Shield, first annual joint review, 28 November 2017, Article 29 Data Protection Working Party, 17/EN WP 255 (hereafter referred to as "the WP29 first annual joint review")

[134] Ibid, page 7

[135] Ibid, page 14

[136] Ibid, page 17

[137] Ibid, page 18

by the US authorities relating to the exercise of these powers and how they are monitored. The introduction of the Ombudsperson is also an important change as Schrems criticised the lack of possibility for EU Data Subjects to challenge the US intelligence agencies' disproportionate use of their surveillance powers.

4. THE TRANSNATIONAL REACH OF GDPR: THE REALITY OF THE CHALLENGING AIM OF REGULATING DATA PROTECTION OUTWITH EU TERRITORY

The EU hopes that the GDPR will be a comprehensive framework that can regulate data privacy internationally through use of extra-territorial applicability and rules relating to Third Country data transfer. However, the cross-border reach of GDPR could be difficult to exercise in practice.

The first part of this chapter will look at the challenges which are specific to the extra-territorial application of GDPR and the issues the EU could face when trying to enforce GDPR on entities which are not present within an EU Member State. The second part of this chapter will focus on the problems related to the provisions in the GDPR which relate to cross-border data transfer.

4.1. Extra-territorial application

As detailed in Chapter 1.2 of this dissertation Article 3(2) leads to the applicability of GDPR if an entity which is not located within the EU territory (a) offers goods or services to an EU Data Subject (b) or monitors their activity to the extent that said activity takes place within the EU. As a result, the jurisdictional scope of the GDPR has the potential to very large.

However, it needs to be established whether this extensive application of EU law is justified under principles of international law. In addition, it must be considered what authority the EU DPAs and Courts have to exercise jurisdiction in international cases which relate to the internet. This also leads to the question of enforceability of judgements. This subchapter will concentrate on the legitimacy of the EU when it comes to this extra-territorial application of GDPR and the exercise of jurisdiction and then move on to potential enforcement issues.

(a) Extra-territorial application: conflict with international law

The extra-territorial application of GDPR was created to provide the most comprehensive protection for EU Data Subjects possible. However, it must be examined if this extra-territorial application is permitted in terms of international law and the rules on the conflict of laws. There EU might find the application of EU law outwith EU territory challenging in reality especially given the fact that the EU unilaterally declared their law applicable despite the situation being international in context.

The applicability of EU law under Article 3(2) GDPR is based on the concept of *Lex Loci Solutionis*. The applicable law is not based on the location of the establishment of the Data Controller or the Data Processor but on the location of where the contractual performance is being offered.

Given the previous decisions of the ECJ, it seems likely that the wording of offering of goods and services to EU Data Subjects or the monitoring of their activities will be given a broad interpretation[138]. Take the example used by authors De Hert and Michal Czerniawski of an EU Data Subject who books a trip to the US using a US travel agency's website which has options to be read in English, French and Spanish and offers the possibility to pay in Euros[139]. Taking Article 3(2) and recital 23 GDPR the mere use of French and Spanish and the option to pay in Euros would be sufficient to establish that the US travel agency was selling goods or services to EU Data Subjects and, therefore, GDPR would be applicable. However, it could be argued that there is a weak link between the European Union and the contract that was created between the US travel agency and the EU Data Subject. Both the payment and the service will occur in the US[140]. Therefore, the performance of the contract is in the US, not the EU.

This extensive claim to extra-territorial applicability could result in a conflict of laws between the EU law and American law. US laws treat data protection very differently from the EU specifically with regards to the potential powers of US intelligence services' access to data. Using the example above, the travel agency could be obligated under US law to transfer the data to the US authorities in a way that would not be consistent with EU law[141]. The law the US entity is more likely to follow is the one that has the biggest threat of repercussions if not followed. Therefore, it is necessary to question if the EU could actually enforce their decisions taken under GDPR on entities which have no presence in the EU. This question will be dealt with in the third part of this subchapter.

When it comes to the monitoring to EU Data Subjects' behaviour which occurs with the EU, this too could lead to the extra-territorial application of GDPR. It could be argued that this provision is aiming its sights on the big players in the data privacy battle like Google and Facebook[142]. Recital 24 GDPR states Data Subjects are monitored in terms of article 3(2)(b) if they are tracked or if there is the use of personal data processing techniques or profiling. Google and Facebook often use tools such as "cookies" to determine users' interests and target advertisements. The GDPR brings these activities within the scope of the GDPR even if the Data Processor and Data Controller are located outwith the

[138] A. Kloth, Volkerrechtsblog, *International Law and International Thought, One law to rule them all, on extraterritorial applicability of the new EU General Data Protection Regulation*, 5 February 2018, https://voelkerrechtsblog.org/one-law-to-rule-them-all/ last accessed 12 August 2019 (hereafter referred to as "Kloth, One law to rule them all")

[139] This example is taken from De Hert and M. Czerniawski, IDPL 2016, 230, 339

[140] Kloth, One law to rule them all, supra note 138

[141] Ibid

[142] Ibid

EU. Although, the big actors such as Facebook and Google are undoubtedly established within the EU and already obligated to respect the GDPR by virtue of article 3(1).

In addition to these large targets, the applicability of GDPR when an entity monitors the behaviour of an EU Data Subject could potentially renders GDPR application for all Third Country entities which have websites which are accessed by EU Data Subjects as almost all websites use cookies[143].

(b) Jurisdiction of European DPAs and Courts: reliance on the controversial Effects Principle

In addition to having to establish that the GDPR is applicable in an international context where there is a potential conflict of laws, the EU will also have to establish that the DPAs, National Courts and the ECJ have jurisdiction when it comes to actions against entities located in Third Countries.

There are recognised basis of jurisdiction which are established in international law. There is the territorial principle which provides that a state will have jurisdiction over an event that happens on their territory[144]. There is also the effects principle which states that a state can exert jurisdiction over events that occur outwith their jurisdiction if they have a substantial effect within said state[145].

No matter which basis of jurisdiction is chosen, a state, or regional organisation, is required to establish that it is reasonable that they exercise jurisdiction in the situation[146]. There requires to be a "sufficient connection" between the state seeking to exercise jurisdiction and the event in question in order to justify the exercise of jurisdiction[147].

It is often viewed that the territorial principle is the strongest basis for jurisdiction[148]. Under Article 3(1) GDPR the GDPR is applicable if the Data Controller or Data Processor is established in the EU, so it could be argued that the EU could exercise territorial jurisdiction in this case. However, the GDPR makes it clear that the actual processing does not require to be undertaken in the EU.

---

[143] Ibid

[144] R. Jennings, *Oppenheim's International Law*, Vol. 1, Peace (Essex, 1992), 458

[145] *Restatement (Third) of foreign relations Law*, (Am. Law inst. 1987), 402(1)(c)

[146] Ibid, 403(1)

[147] Christopher Kuner, *Data protection law and international jurisdiction on the internet (Part 1)*, (2010) 18 IJLT 176

[148] U. Kohl, *Jurisdiction and the internet – Regulatory competence of the online activity*, Cambridge university press, 2007, 20 and C. Ryngaert, *Jurisdiction in International Law*, Oxford University Press 2008, 27

In order to exercise jurisdiction, the EU will have to rely on the effective doctrine as the ECJ did in the Google Spain ruling[149]. However, this remains controversial in the context of jurisdiction for online activity or content[150]. A balance must be struck by the EU between requirement for effectiveness and the principle of non-intervention[151].

Although the GDPR seeks to regulate data protection internationally through extra-territorial application, this could prove difficult to justify in reality. Article 3(2) has the potential to make GDPR applicable to an enormous extent. This could cause conflicts with other jurisdictions who might not have the same approach towards data protection as the EU. The effectiveness of these provisions also needs to be considered in concurrence with the EU's actual ability to enforce the GDPR outwith the territory of the EU.

(c) Fine issued under the GDPR: the difficulty with enforcement in Third Countries

Under the GDPR the DPAs have enormous powers when it comes to the level of fines they can issue if companies do not comply with the GDPR. The GDPR provides for detailed guidance for Member States on how to monitor entities, deal with complaints, investigate issues and impose warnings or fines[152].

Although there have been some fines that have been issued under the new provisions of the GDPR[153] it seems that the Data Protection Authorities have been more keen to use their powers to issue warnings compelling entities to comply with GDPR or risk being exposed to an enormous fine[154]. The EU approach to regulation is to encourage compliance and use fines only as a punitive measure[155].

As argued, the mere threat of such enormous fines is a good method to encourage entities to respect the provisions of the GDPR. When it comes to entities which are located or established in the EU, the fines are a clear deterrent.

---

[149] Google Spain, supra note 18, paragraph 58 and Van Alsenoy, the extraterritorial reach of GDPR and Public international law, supra note 31, page 93

[150] Jonathan Zittrain, *Be careful what you ask for: Reconciling a Global Internet and Local Law*, Harvard Law School Public Law Research Paper No. 03/2003

[151] *Restatement (Third) of foreign relations Law*, (Am. Law inst. 1987)

[152] Jan Philipp Albrecht, *How the GDPR Will Change the World*, 2 Eur. Data Prot. L. Rev. 287 (2016).

[153] The fines issued against Marriot hotel and British Airways detailed in Chapter 3(1)

[154] M. Al Khonaizi, *Fines under EU GDPR in non-EU jurisdictions: Enforceable or Mere Reputation Risk?*, MJIL (hereafter referred to as "Khonaizi, Fines under EU GDPR in non-EU jurisdictions")

[155] Ibid

However, it is less clear how fines will be enforced against entities that are bound by GDPR by virtue of Article 3(2) GDPR despite having no presence within EU territory.

In these circumstances, the EU will have to rely on the authorities of the jurisdiction where the entity is located in order to enforce the fines. This could be extremely difficult given not all jurisdictions share the same views on data protection as the EU[156]. A clear example of a jurisdiction that has a different approach to data protection is the US. If an entity is located in a Safe Third Country, enforcement is less complicated as there is already an agreement between the EU and the Third Country relating to data protection. With regard to the US, if the entity is registered under Privacy Shield, they voluntarily submit themselves to enforcement actions under GDPR which could include the fines[157]. If the US entity is not registered under Privacy Shield, the fine would have to be enforced by the US Courts. Under US law, the court will only enforce the foreign judgement if the judgement does not violate a constitutional right, rights established under federal or state laws or any public policy considerations[158]. It could be difficult for the EU Data Protection Authority to effectively enforce a judgement in the US if the company is not registered under Privacy Shield. The US company could argue that the judgement would violates their First Amendment rights[159].

Although the example of the US has been given, this issue could apply to enforcement in any non-EU jurisdiction where there is no agreement between the European Commission and the relevant authorities in the Third Country. The Data Protection Authorities would have to rely on the national courts in the entities jurisdiction to enforce their judgements or fines and given the issues relating to possible jurisdictional matters are conflicts of laws, this could be challenging.

It should be noted that under the GDPR an entity must appoint a representative in the EU if it is not established in the EU but it is subject to the scope of application of the GDPR under article 3(2) GDPR[160]. This representative's role is to act as a contact point for Data Subjects and the Supervisory

[156] Ibid

[157] U.S. Dep't of Com., *EU– U.S. Privacy Shield Framework Principles* 7 (2016), https://www.privacyshield.gov/EU-US-Framework.

[158] *See* Matusevitch v. Telnikoff, 877 F.Supp. 1, 2 (D.D.C. 1995), Mata v. Am. Life Ins. Co., 771 F. Supp. 1375, 1384 (D. Del. 1991), Abdullah v. Sheridan Square Press, Inc., No. 93CIV.2515 (LLS), 1994 WL 419847, at *1 (S.D.N.Y. May 4, 1994)

[159] Khonaizi, Fines under EU GDPR in non-EU jurisdictions, supra note 154

[160] GDPR, Article 27, however, there are exceptions to this rule if the non-EU entity only undertakes occasional processing that does not have a large scale impact on special categories of personal data or personal data relating

Authorities in the EU. They can be addressed directly when it comes to issues relating to compliance with GDPR.

However, it is not clear what role this representative will play in the enforcement proceedings. Some authors question whether the representative could be considered jointly and severally liable with the non-EU resident entity or if their role is simply to accept documents and communicate with the data protection authorities[161]. Recital 80 of the GDPR does state that the presence of the representative does not affect the responsibility or liability of the controller[162]. However, Article 80 also states that the representative should be subject to enforcement proceedings in the case of non-compliance of the entity with GDPR. It is not clear at this point what role the representative would play in enforcement proceedings or, indeed, how a judgement rendered in the EU will be enforced against an entity located abroad.

It has been argued that the EU is unlikely to try and enforce fines against non-EU entities which are not represented in the EU[163]. It would potentially be very difficult for the EU to enforce and they would be better to focus on the large actors who are without doubt present in the EU such as Google and Facebook[164]. This clearly undermines the objective of the GDPR to be a comprehensive framework which regulates data privacy internationally. Article 3(2) is not hugely effective if entities risk nothing by ignoring it. However, the GDPR is still considered to be an international standard for data protection, the refusal of an entity to comply could risk the reputation of that entity[165]. In this sense, the GDPR could have an impact outwith the territory of the EU but perhaps not in the concrete way that was hoped by the legislators.

4.2 Cross border data transfer

When it comes to cross border data transfer, the GDPR has tried to reinforce obligations on sending entities in order to ensure a high level of protection for the personal data of EU residents. This does not mean that the provisions of the GDPR relating to data transfer are without criticism. This part of

---

to criminal convictions and offences and that it is not likely the result in any risk to the rights and freedoms of Data Subjects.

[161] P. Zeni, F. Gilbert and M. Calehuff, *GDPR and Privacy Shield: Difference Tools for Different Goals*, 36 ACC Docket 78, 36 No. 7 Acc Docket 78, September 2018, page 5 (hereafter referred to as R. Zeni et al., Different Tools for Different Goals), page 6

[162] Voigt and von dem Bussche, GDPR, A Practical Guide, supra note 15, page 133

[163] Khonaizi, Fines under EU GDPR in non-EU jurisdictions, supra note 154

[164] Ibid

[165] Ibid

the dissertation will focus firstly on general criticisms of the protection offered by the GDPR when it comes to Third Country data transfer in general. Thereafter, it will elaborate on specific issues relating to data transfer to the US and Privacy Shield.

(a) Data Transfer to Third Countries: an adequate level of protection?

Chapter 5 of the GDPR states that if an EU entity wishes to transfer data to a Third Country, they have to ensure that the transfer is either pursuant to an Adequacy Decision or that appropriate safeguards are in place to protect the data after transfer. Under the Data Protection Directive and the GDPR, in order for an Adequacy Decision to be granted, the country national legislation (or the international agreement in the case of Privacy Shield) must provide for an adequate level of protection[166]. Schrems and Recital 104 of the GDPR make it clear that an "adequate level of protection" means a level of protection which is essentially equivalent to that provided for in the EU[167].

There are specific ways that an entity can ensure that adequate safeguards are in place after transfer, one way is to place SCCs in the contract with the receiving entity[168]. However, the SCCs are not without criticism. Under the Data Protection Directive, some Member States required further safeguards to just using the SCCs such as requiring authorisation from the Supervisory Authorities[169]. This is no longer the case under GDPR as article 46(2) clearly states that if the transferring entity uses SCCs then they do not require any further authorisation from a Supervisory Authority.

However, the future of the SCCs is uncertain as the legality of transfer under them is subject to an ECJ court case which was lodged by Schrems in 2016[170] (often referred to as "Schrems II"). Schrems' arguments mainly relate to transfer to the US and the unlimited surveillance operations that US intelligence services can undertake under US law. However, if the decision leads to the termination of the SCCs, it will have an effect on transfers to other Third Countries as well.

In addition to the issues relating to the USA, there are also arguments that the SCCs are outdated given that they have not been modified since before GDPR came into force and therefore do not reflect the additional obligations placed on Data Controllers and Data Processors provided for under

[166] GDPR, Article 45

[167] Sidley, *Esentially equivalent, A comparison of the Legal Order for Privacy: From the European Union and the United States,* 25 January 2016, 9, 10

[168] GDPR, Article 46(2)(c)(d)

[169] Voigt and von dem Bussche, GDPR, A Practical Guide, supra note 15, page 120

[170] Case before the European Court of Justice, Facebook Ireland and Schrems, Case C-311/18

the GDPR. This specifically relates to the SCCs to be inserted in a contract between an EU Data Controller and a Third Country Data Processor (otherwise known as "controller to processor (C2P) SCCs"). The GDPR created additional obligations on Data Processors that were not provided for under the Data Protection Directive. These additional obligations are not reflected in the current drafting of the C2P SCCs[171].

Another potential issue with the SCCs is that they are adopted by each National Supervisory Authority[172]. Although they must thereafter be approved by the European Commission, this could result in different Member States adopting SCCs which do not provide for exactly the same protection. This undermines the aim of the GDPR which was to harmonise data protection throughout the EU.

In addition to potential issues with the SCCs, another issue with the protection offered by the GDPR relating to cross border data transfer relates to the consent exception. Despite there being no guarantee to the protection of the data transferred, an EU located entity can transfer data if a Data Subject consents to the transfer[173]. Although it is specified that the Data Subject must explicitly consent to the specific transfer that is proposed[174] and the Data Subject must be informed of the possible risks, it is not exactly clear how much information about the transfer the transferring entity is required to give the Data Subject[175]. It is not clear if specific risks relating to the particular receiving country need to be communicated or if a generalised disclaimer would be sufficient[176]. Although the Data Subject has the right to withdraw their consent to the transfer at any time, it could be argued that there are still issues with the consent exception to the adequate protection rule. The EU legislators, when creating GDPR, took the position that there should be a collective approach to consent and contract doctrines[177]. The authors Paul Schwartz and Karl-Nikolaus Peifer talk of the concept of information privacy inalienability[178]. This is the idea that individuals might not be free to do as they wish with their data, there are some things that the individual cannot consent to. The GDPR creates some rights

[171] BDK Advokati, *Standard Contractual Clauses challenged by GDPR and scrutinized by the CJEU*, Lexology, https://www.lexology.com/library/detail.aspx?g=d4a4a515-4868-4445-8b1c-0d358feab8fe, last accessed 23 August 2019

[172] GDPR Article 46(2)(c) and Article 93(2)

[173] GDPR, Article 49 sec. 1 lit. a, however, this exception is not applicable to public authorities carrying out activities in the exercise of their public powers (GDPR, Article 49, Sec. 3)

[174] GDPR, Article 49

[175] Voigt and von dem Bussche, GDPR, A Practical Guide, supra note 15, page 118

[176] Ibig, page 119

[177] P Schwartz et al, Transatlantic Data Privacy supra note 77, page 139

[178] Ibid

that the Data Subject cannot waive or trade[179]. The Court of Justice has stated that there must be rules for data processing that set out a minimum level of data protection[180]. It is stated:

"a data subject cannot through consent 'sell' fundamental rights protection by the Charter, including the fundamental interest in privacy and data protection."[181].

It therefore seems odd that a data subject can simply consent to the transfer of their personal data to an entity located in a Third Country that might provide for little to no data protection. There is clearly an information obligation in place but it seemed the EU was trying to avoid a situation where a Data Subject could waive fundamental rights relating to data protection. The idea was that Data Subjects often do not read privacy notices, or they do not understand them[182]. Since the GDPR aimed to protect people from this, why then can an individual consent to a transfer which might result in their data having little to no protection after transfer.

There are other loopholes that could undermine the intention of the legislature to create a comprehensive system of protection when it comes to Third Country data transfer. EU entities can transfer data to countries that do not have adequacy decisions through countries that do. One example would be transferring data through Canada. Canada has been awarded an adequacy decision by the European Commission therefore the transferring entity can transfer the data without concern. Once the data arrives in Canada, it is subject to the Canadian data protection rules. Under Canadian law, entities can transfer data outside of Canada, for example to the US, if they ensure that the data will be given as much protection as required under Canadian law.

This could be seen as posing no issue given Canadian law has been deemed sufficient and therefore if the entity in the US receives the data, they have to adhere to a law that is deemed sufficient. However, there are some issues given that the Canadian adequacy is being questioned. It is due to be reviewed in 2020 and there are suggestions that the Canadian governments surveillance powers are going to cause a problem for the re-issuing of the adequacy decision[183]. Not only is it of concern that Canadian laws might not actually provide for adequate protection despite having an adequacy ruling, but it is

[179] J. P. Albrecht and F. Jorzo, DAS NEUE DATENSCHUTZRECHT DER EU 126–29 (2017)., page 72

[180] Schrems, supra note 82, paragraph 91

[181] J. P. Albrecht and F. Jorzo, DAS NEUE DATENSCHUTZRECHT DER EU 126–29 (2017)., page 72

[182] P Schwartz et al, Transatlantic Data Privacy supra note 77, page 171

[183] S. Grynwajc, *GDPR: Surviving the likely demise of the Privacy Shield*, Law Office of S. Grynwajc, Transatlantic Legal Services, 8 July 2018

also of concern that it could result in data being transferred to other countries which do no themselves have adequacy rulings.

The GDPR has tried to reinforce their objective of providing for complete protection for EU Data Subjects even when data is transferred outwith their territory. However, it is clear that there are still some possible ways to undermine this protection. Companies can make transfers using outdated SCC which might not completely protect data subjects from Third Country extensive government surveillance activities. In addition, EU entities can rely on Data Subjects' consent to the transfer which might undermine the concept of information privacy inalienability which the GDPR has tried to reinforce in order to provide the most comprehensive protection possible. Finally, there are questions about the accuracy of adequacy decisions awarded by the European Commission. There is a question as to whether some adequacy decisions are out of date and whether the legal systems of the countries or areas which have been deemed safe actually provide sufficient data protection.

This leads into the next topic of analysis of the actual protection offered by Privacy Shield which has been awarded an adequacy decision. There are still prevalent issues with this agreement which could possibly reduce the protection of data which is transferred under Privacy Shield.

(b) Privacy Shield: a level of data protection "essentially equivalent" to that in the EU?

Although Privacy Shield is considered to be an improvement on Safe Harbour, it is not free from criticism. Since its creation, there have been debates about whether the protection offered by Privacy Shield meets the test established by Schrems and provides for a level of data protection which is essentially equivalent to that in the EU.

European Commission detailed a number of criticisms of Privacy Shield in its first annual joint review. The Commission made several recommendations including more proactive monitoring of registered companies[184].

The WP29 also had several concerns relating to Privacy Shield which it highlighted in its report on the first annual joint review[185]. The important concerns highlighted in the WP29's first annual report will be examined in this subchapter and to what extend said concerns were resolved by the time of the

[184] European Commission First annual review press release and The European Commission, 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(2017) 344 final, (hereafter referred to as "The European Commission, First Annual Review"), page 5

[185] The WP29 first annual joint review, supra note 133

second annual review undertaken by the European Data Protection Board[186] (hereafter referred to as the EDPB) in its report on the second annual review published on the 22 January 2019[187].

Like Safe Harbour, under Privacy Shield, entities self-certify their compliance with Privacy Shield in order to register. Some entities seek outside companies to undertake this evaluation and others undertake an internal evaluation. The lack of verification undertaken by the US authorities as to the validity of the self-certification and the absence of ongoing monitoring of compliance was of concern to the WP29[188]. Although Privacy Shield allows the DoC to undertake periodic review of compliance[189], by the time of the first annual joint review, no reviews had been undertaken. The DoC stated they would only use this power if they had reason to believe an entity had been failing to comply[190]. It was argued that in order to ensure that the self-certification process works, the DoC is required to perform random periodic review of compliance.

By the EDPB's second annual review, there were some improvements in this area. It was stated that the DoC checks first time applications to ensure that there are no inconsistencies between their privacy policies and their certification[191]. However, the checks conducted by the DoC were largely to ensure the companies met the procedural requirements for registration. There remains a lack of oversight in terms of ensuring that registered companies adhere to the substantial principles of Privacy Shield[192].

In terms of ongoing oversight of registered companies, the EDPB saw an improvement in this area as well. It was noted that the DoC and the Federal Trade Commission (hereafter referred to as the FTC) conducted random investigations in order to check the compliance of registered companies[193].

[186] The WP29 was created under the Data Protection Directive, it was replaced by the European Data Protection Board when GDPR came into force on 25 May 2018

[187] The European Data Protection Board, "EU-US Privacy Shield – Second Annual Joint Review", 22 January 2019, (hereafter referred to as "the EDPB second annual joint review".)

[188] The WP29 first annual joint review, supra note 133, page 10

[189] ANNEXES to the Commission Implementing Decision 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, C(2016) 4176 final, Brussels 12 July 2016, Annex I/Annex 1 (Letter from acting Under Secretary for the International Trade Ken Haytt) to Commission decisions (EU) 1250/2016

[190] WP29 First Annual Joint Review, page 10

[191] The EDPB second annual joint review, supra note 187, page 11, paragraph 49

[192] Ibid, page 11, paragraph 51

[193] Ibid, page 12, paragraph 56

However, again these checks focused mainly on formalities and did not check the compliance of registered companies with the substantive Privacy Shield principles[194].

There is also concern relating to the lack of guidance given to registered companies relating to how to implement the Privacy Shield principles in practice. The WP29 felt companies should be given clearer guidance regarding certain aspects of the Privacy Shield and how to apply them in practice, for example how Data Subjects should be given the option to opt out from processing their personal data for a new purpose and clearer guidance on when registered companies should provide Data Subjects with notice relating to the processing[195].

Of significant concern was how onward-transfer provisions were applied and monitored. Under Privacy Shield onward transfer of data transferred under Privacy Shield is possible so long as the receiving entity is bound by contract to comply with the Privacy Shield Principles[196]. However, there is a lack of guidance provided by the US authorities as to how companies can adhere to their obligations regarding onward transfer[197]. In addition, there seems to be no verification by US authorities that registered companies are actually adhering to this obligation[198].

By the EDPB's second annual joint review, this matter had also been partly dealt with. The DoC has published guidance regarding onward transfer and obligations of the processor on their website[199]. However, it was noted that further guidance was required for example regarding the Choice Principle, the Notice Principle and clarification relating to Data Subjects' right of access to the personal data collected about them[200].

The WP29 raised the issue of the difference of interpretation of "HR data" which receives a higher level of protection under Privacy Shield. However, the US interpreted "HR data" to only include data on employees of an EU located branch of an entity which is transferred to a non-EU located branch of that same entity. This interpretation does not include data about employees that is transferred from and EU company to an external US Data Processors[201]. From the WP29's perspective, this would

[194] Ibid, page 13, paragraph 58

[195] The WP29 first annual joint review, supra note 133, page 8

[196] S. Bu-Pasha, *Cross-Border issues under EU data protection law with regards to personal data protection*, Information and Communications Technology Law, 2017, VOL. No. 3, 213-228, page 225

[197] The WP29 first annual joint review, supra note 133, page 8

[198] Ibid

[199] The EDPB second annual joint review supra note 187, page 9, paragraph 40

[200] Ibid, page 10, paragraph 43

[201] The WP29 first annual joint review, supra note 133, page 9

clearly be HR data and should benefit from the added protection. By the second annual review, the EDPB stated that there was an impasse regarding the interpretation of "HR data" and an agreement had not been reached between the EU and US authorities. The EDPB stated that the European Commission should investigate what impact this difference of interpretation could have on the protection of personal data of Data Subjects in the EU[202].

The WP29 also highlighted concerns relating to automated decision making and profiling. The GDPR provides protection for individuals and states that they will not be subject to decision which will have a legal effect on them when said decision is made solely by automated processing[203]. There were concerns that Data Subjects whose data is transferred to the US under Privacy Shield will not be granted these protections provided for under the GDPR. During the first annual review it was stated by the US authorities that no data that was transferred under Privacy Shield was subjected to automated decision-making systems, in addition they stated that US law provides for some protections in this area. However, it is not clear if these rules apply to all possible uses of decision-making systems[204].

By the time of the EDPB's report on the second annual review, an investigation has been conducted in order to determine if automated decision-making software was used on data transferred under the Privacy Shield[205]. It was felt that automated decisions were more likely to take place when a US company targets EU customer directly. In this situation, GDPR should directly apply to the US company in terms of Article 3(2) GDPR. The FTC has investigated some companies relating to the effects automatic decision-making systems have had on Data Subjects in the US[206]. The EDPB called for the European Commission to monitor this area[207].

In addition to these commercial concerns relating to Privacy Shield, there are also still very real concerns about the US intelligence services' access to the EU Data Subject's personal data. After

[202] The EDPB second annual joint review, supra note 187, page 14, paragraph 67

[203] GDPR, Article 22

[204] The WP29 first annual joint review, supra note 133, page 10

[205] European Commission, "Automated decision-making on the basis of personal data that has been transferred from the EU to companies certified under the EU-U.S. Privacy Shield: *Fact-finding and assessment of safeguards provided by U.S. law", October 2018* https://ec.europa.eu/info/sites/info/files/independent_study_on_automated_decision-making.pdf, last accessed 10 August 2019

[206] The EDPB second annual joint review, supra note 187, page 15, paragraph 73-75, reference to the Equifax data breach case and the Realpage company case

[207] The EDPB second annual joint review, supra note 187, page 15, paragraph 77

Schrems, Privacy Shield had to address this issue clearly. However, there are still concerns in the EU that the US Intelligence services have unlimited and unmonitored access EU Data Subjects' data under US law.

Schrems held that any derogations from data protection principles should only occur so far as necessary[208] and any legislation allowing general access for public authorities to personal communications which are sent on by electronic means would be considered to be a breach of Article 7 of the European Charter of Fundamental Rights[209].

The WP29 stated in their report that there were still concerns that the US intelligence services use the powers granted under US law to undertake massive indiscriminate surveillance on EU Data Subjects.[210]. There are two specific acts of US law which are of concern in the EU. Firstly, the is section 702 of the Foreign Intelligence Surveillance Act (hereafter referred to as FISA) which was added by the 2008 amendments to the FISA 1978. Section 702 FISA allows the US intelligence services to search foreign communications of non-US citizens located outside the US. The second US act in question is the Executive Order 12333 which gives powers to the US intelligence services to conduct foreign intelligence surveillance outside the US.

With regard to section 702 FISA, the US authorities made assurances that the surveillance is not indiscriminate and that internet service providers are only required to provide intelligence services with data relating to a specific phone number, email address, IP address or other identifier after it has been specifically brought to the relevant authorities attention[211]. For the second annual review the US Government published some documents such as decisions from the Foreign Intelligence Surveillance Court to try and prove this assertion[212].

The US authorities argue that the EO 12333 falls outwith the scope of Privacy Shield as it relates to US surveillance operations outside the borders of the US. The WP29 on the other hand state that the adequacy decision of a country must also consider their legislation relating to how its national law allows it to conduct surveillance outside its territory

[208] Schrems, supra note 82, recital 92

[209] Ibid, recital 94

[210] The WP29 first annual joint review, supra note 133, page 16

[211] The WP29 first annual joint review, supra note 133, page 15

[212] The EDPB second annual joint review, supra note 187, page 16, paragraph 78

Both the WP29 and the EDPA stated that they do not have sufficient information to establish whether the US authorities access to personal data of EU Data Subjects is undertaken only to the extent that it is necessary or whether it can still be considered massive and indiscriminate surveillance. Despite the publishing of some FISA decisions, there is still a significant lack of information relating to FISA court rulings.

There are also concerns that there is no oversight of these intelligence agencies when exercising their powers relating to foreign surveillance. The WP29 and the EDPB identified that there was a complex system of oversight to ensure that the US intelligence services did not abuse their powers. However, it is not really clear how effective this complex system actually is[213].

It is also important to note that the second annual joint review came after the misuse of personal data by Facebook and Cambridge Analytica was already public knowledge. This scandal obviously heightened concerns relating to Privacy Shield given that Facebook is a registered company. The European Parliament seriously questioned whether Privacy Shield could be trusted. As a result, on 11 June 2018, the Committee on Civil Liberties, Justices and Home Affairs at the European Parliament passed a motion recommending that the European Commission suspend Privacy Shield unless the American authorities meet their obligations. On 5 July 2018, the European Parliament passed a non-binding resolution calling for the suspension of Privacy Shield if certain conditions were not met before the 1 September 2018[214]. The European Parliament called for Privacy Shield to be made fully compliant with the GDPR. It was also stated that Privacy Shield must be changed address all the issues highlighted in the first joint annual review of Privacy Shield made by the WP29 as detailed above.

1 September 2018 came and went without Privacy Shield being suspended. It is clear that the issues highlighted by the WP29 in their report on the first annual review were not met by the 1 September 2018 given they were still not met by the Second annual joint review. Therefore, it seems that the suspension was an empty threat.

In addition to the issues raised during the annual reviews, Privacy Shield has also been challenged before the ECJ. In fact, history seems to be repeating itself as Schrems has also lodged a challenged

[213] The WP29 first annual joint review, supra note 133, page 17 and The EDPB second annual joint review, supra note 187, page 18, paragraph 93

[214] European Parliament, resolution of 5 July 2018 on the adequacy of the protection afforded by the EU-US Privacy Shield (2018/2645(RSP)).

against Privacy Shield[215]. The court heard arguments in July 2019 and their decision is expected in early 2020[216]. Schrems arguments this time are broadly the same as he successfully argued before the ECJ which resulted in the termination of Safe Harbour. The argument is that the US authorities still have too much access to European Data Subjects data after it is transferred under Privacy Shield[217]. However, this time Schrems does not just attack the Privacy Shield mechanism but also the Standard Contractual Clauses. Therefore, this case could have an impact for Third Country data transfer in general[218]. Schrems argues that transfer under the SCC does not provide sufficient protection given the US authorities still have indiscriminate access to the data that is transferred[219]. The general view is that the SCCs could be invalidated but the outcome for Privacy Shield is less certain[220].

Privacy Shield was also challenged by the French Digital Rights Group, La Quadrature du Net[221] who argue that Privacy Shield can never give adequate protection of data given the US governments surveillance activities[222]. The court is awaiting the decision is Schrems to make a decision in La Quadrature du Net[223].

It is clear that there are still issues relating to the protection offered by Privacy Shield and questions as to whether it provides for an essentially equivalent protection as the protection afforded under EU law. It seems that there are still a lot of issues which need to be addressed relating to Privacy Shield such as providing further guidance for registered companies, verification of companies' compliance on registration and ongoing supervision of compliance, differences relating to interpretations and differences regarding protection from automated decision making. There are still considerable concerns about US intelligence agencies surveillance activities of EU Data Subjects and concerns relating to whether these activities are exercised proportionally and only where necessary. Although the European Commission ignored the call from the European Parliament to suspend Privacy Shield

[215] Case before the European Court of Justice, Facebook Ireland and Schrems, Case C-311/18

[216] [216] J. Baker, "EU Court Hearings to determine the future of Privacy Shield, 25 June 2019, https://iapp.org/news/a/eu-high-court-hearings-to-determine-future-of-privacy-shield-standard-contractual-clauses/, last accessed 10 August 2019 (hereafter referred to as "Baker, The future of Privacy Shield")

[217] Ibid

[218] DLA Piper, "Schrems 2.0 – The Demise of Standard Contractual Clauses and Privacy Shield, 1 July 2019, https://blogs.dlapiper.com/privacymatters/schrems-2-0-the-demise-of-standard-contractual-clauses-and-privacy-shield/, last accessed 10 August 2019

[219] Ibid

[220] Ibid

[221] Case before the European Court of Justice, La Quadrature du Net and Others v Commission, case T-738/16

[222] N. Lomas, "EU-US Privacy Shield compliant to be heard by Europe's top court in July, June 2019

[223] Baker, The future of Privacy Shield

after Cambridge Analytica scandal, they may not be able to ignore these issues for much longer after the European Court of Justice makes their decision in Schrems II and la Quadrature du Net cases next year.

(c) Enforcement: an effective remedy before a tribunal?

When considering the level of protection offered by Privacy Shield it is essential to consider if EU Data Subjects can enforce the rights granted to them. Under Schrems it was held that EU individuals should have recourse before an independent tribunal in order to ensure their rights[224]. Privacy Shield and GDPR requires that Data Subjects have a mechanism in place in order to ensure compliance with their rules. These mechanisms must be available to Data Subjects at no extra cost to them[225].

Under GDPR Data Subjects have significant remedies to enforce compliance with the GDPR, Data Subjects can lodge complaints with their Supervisory Authority[226] but they can also seek judicial remedy before their national courts[227]. Data Subjects can be granted damages[228] but as detailed in Chapter 3.1, companies that are found to be non-compliant can face extremely large fines[229].

Under Privacy Shield, there are two mechanisms for enforcement, one for general enforcement of Privacy Shield and the second is specific to US intelligence agencies access to data.

Regarding general enforcement, the FTC and the DoC are charged with enforcing Privacy Shield compliance for registered companies[230]. In the second annual review the EDPB mentioned that the FTC had dealt with around 100 referrals from Data Subjects but only 8 of them were public[231]. This means it is hard to assess how effective the FTC is as a method of recourse. It seems that the only real recourse mechanism available to Data Subjects is if the registered entity provides an Independent Recourse Mechanism (IRM)[232]? An IRM is when the dispute is resolved by an independent company under alternative dispute resolution. However, there are concerns that the companies that offer IRMs

[224] Schrems, supra note 82, paragraph 95

[225] R. Zeni et al., Different Tools for Different Goals, supra note 161

[226] GDPR, Article 77

[227] GDPR, Article 79

[228] GDPR, Article 82

[229] GDPR, Article 83

[230] EU-US Department of commerce, EU-US Privacy Shield Framework Principles 4 (216), https://www.privacyshield.gov/EU-US-Framework https://perma.cc/V2NJ-T6BZ, 25-26

[231] EDPB, second annual joint review, page 13, paragraph 63

[232] The WP29 first annual joint review, supra note 133, page 10

are also the companies that provide Privacy Shield compliance reviews. This could give rise to a clear conflict of interest because if the company verified the compliance of a registered company with Privacy Shield, they might not be objective when then asked to review said compliance by a Data Subject[233]. It is not clear if there are any safeguards in place to avoid these conflicts of interest.

Another concern is the lack of clear information and guidance available to EU Data Subjects advising them of their rights under Privacy Shield and how they can enforce them[234]. The DoC has now published a document on their website for EU citizens relating to their rights and how to enforce them. However, this document is only one page long and more information should be provided[235].

We have seen that under the GDPR entities can suffer enormous fines for non-compliance. These fines do not apply to breaches of Privacy Shield by registered companies. If the FTC find non-compliance with Privacy Shield, they can impose on the condemned company certain obligations such as record keeping for a specific period[236]. They can also issue fines of up to $40 000 per violation or $40 000 per day of continued violations[237]. This is not as significant a deterrent as a €20 million fine which is possible for breach of the GDPR.

Companies can also have their Privacy Shield registration removed if they are found to be in persistent failure to comply with Privacy Shield. The DoC will remove the company if they receive notice from a government body, the company itself, the self-regulatory body or an IRM body. The removal will happen after 30 days' notice where the party can resolve their failure[238].

The Privacy Shield has also created a specific recourse and enforcement mechanism relating to US Intelligence services access to personal data. Schrems made clear that even with regard to state surveillance matters, Data Subjects should have possible recourse before an independent tribunal in order to ensure their rights[239].

---

[233] The WP29 first annual joint review, supra note 133, page 10,

[234] The WP29 first annual joint review, supra note 133, pages 8 and 9

[235] The EDPB second annual joint review, supra note 187, page 10, paragraph 45 and The Department of Commerce, "The EU-U.S. and Swiss-U.S. Privacy Shield Frameworks Information for EU and Swiss Individuals", www.privacyshield.gov/servlet/servlet.FileDownload?file=015t0000000QJdq, last accessed 10 August 2019

[236] R. Zeni et al., Different Tools for Different Goals, supra note 161, page 5

[237] The Privacy Shield Framework, "Enforcement of Privacy Shield", http://www.privacyshield.gov/article?id=Enforcement-of-privacy-shield, last accessed 11 August 2019

[238] Ibid

[239] Schrems, supra note 82, paragraph 95

In the first annual joint review, it was questioned whether EU Data Subjects could seek to enforce their rights relating to surveillance matters before the US Courts under either the Administrative Procedure Act (APA) or under FISA. The main hurdle for EU Data Subjects in this regard relates to how the US courts have applied the "standing" principle in relation to privacy and surveillance cases[240]. In surveillance cases, the plaintiff needs to prove that they have suffered or will suffer direct injury or harm or that harm is foreseeable[241]. In the US, it is a developing area, but it seems that the US courts are limiting the possibility of recourse for breach of privacy. It has even been suggested that judicial recourse for a privacy violation could be limited to the situation where the victim has suffered economic harm[242]. However, in the EU, if an individual's data is illegally processed, it is considered that that person has suffered harm[243] and the Data Subject can seek reparation for material and not material damages they suffered as a result of the breach[244].

As a result, there are concerns that few EU Data Subjects, who have had their privacy breached, would be able to fulfil the requirement of standing in order to seek judicial remedy in terms of use of the powers of section 702 FISA or EO 12333[245].

Given the difficulties relating to the seeking judicial remedy before the US courts, Privacy Shield created the new position of the Privacy Shield Ombudsperson. Under this Ombudsperson mechanism, EU Data Subjects can refer issues relating to the US authorities' access to their data. The Ombudsperson can refer the questions to the competent General Inspector to make a review. However, there are questions about the powers of the Ombudsperson with regards to access to information which might be necessary in order to undertake their assessment. There were also questions about their power to remedy non-compliance as it seems their powers are limited to confirming the compliance towards the petitioner[246]. In addition, the decision of the Ombudsperson is not subject to judicial review. The first and second annual joint reviews both concluded that they could not assess whether the Ombudsperson mechanism was an effective remedy before the court

[240] The First Amendment of the Constitution of the United Stated

[241] Clapper v Amnesty International, 568 U.S. 398 (2013)

[242] C. J. Hoofnagle, *Federal Trade Commission Privacy Law and Policy*, 286 (2016) page 345

[243]P Schwartz et al, Transatlantic Data Privacy supra note 77, page 170

[244] GDPR, Article 82(1)

[245] The WP29 first annual joint review, supra note 133, page 18 et The EDPB second annual joint review, supra note 187, page 18, paragraph 97

[246] The WP29 first annual joint review, supra note 133, page 19 and The EDPB second annual joint review, supra note 187, page 19, paragraph 102

because it is not shown that they have sufficient power to access information or remedy non-compliance[247].

At the time of the first and second annual joint review the permanent Ombudsperson had not yet been appointed. In fact, the first permanent Ombudsperson was not appointed until 20 June 2019 when former CEO Keith Krach was appointed by the Senate[248]. Krach is also the Under Secretary of State for Economic Growth, Energy and the Environment. The WP29 and the EDPB both raised concerns that the appointment of a high-ranking government official as the Ombudsperson might raise questions about his independence[249]. It will be interesting to see their opinion of the new Ombudsperson at the third annual joint review.

In terms of effective recourse and enforcement mechanisms, it seems that Privacy Shield still has a long way to go. For general enforcement, not only do EU Data Subjects have a lack of available information about how they can enforce their rights, but their enforcement options seem largely limited to whether or not the US company offers IRM or not. Given the questions about the possible conflict of interest of companies offering IRM, this does not seem to be an effective remedy before an independent tribunal.

Regarding possible recourse against US intelligence organisation surveillance activities, it seems that seeking a remedy before the US courts would be difficult given the hurdle of standing as the US court have interpreted it relating to surveillance cases. As a result, there is the new Ombudsperson mechanism, but it is not clear if the Ombudsperson can actually remedy a potential misuse of powers by the intelligence organisations. Therefore, it is difficult to say whether this would be considered an effective remedy before an independent tribunal.

[247] The WP29 first annual joint review, supra note 133, page 19 and The EDPB second annual joint review, supra note 187, page 12, paragraph 103

[248] M. Young and S. Jungyun Choi, "Privacy Shield Ombudsperson Confirmed by the Senate" 25 June 2019, https://www.insiderprivacy.com/cross-border-transfers/privacy -shield-ombudsperson-confirmed-by-the-senate/, last accessed 10 August 2019

[249] The WP29 first annual joint review, supra note 133, page 19 and The EDPB second annual joint review, supra note 187, page 19, paragraph 100

CONCLUSION

There is no doubt that the GDPR has extensive ambitions. The aim of creating a comprehensive system of data protection which is enforceable around the world is not an easy task. In order to fight against the borderless nature of the internet, the GDPR created a Regulation that also seemingly has no borders. However, unilaterally deciding that EU law as applicable outwith EU territory could lead to a number of challenges. The EU could have difficulty establishing the applicability of EU law in a situation where there is a conflict of laws and the link to the EU is minimal. In addition, there could be difficulty establishing the jurisdiction of EU DPAs, Courts and the ECJ in these international situations. Finally, the most difficult challenge could be enforcing judgements against entities in Third Countries who may not share the same views on data protection as the EU.

In conclusion, the GDPR has stated that it is applicable over some situations where, in reality, it would be difficult to enforce. However, another solution is difficult to imagine given that the threat to EU Data Subjects personal data is clearly not limited to the boundaries of the EU. The EU are not going to ban entities which are located in Third Countries from making their products, services and, essentially, their websites available to EU citizens.

However, it could be argued that there is a changing tide with the attitudes of individuals who are becoming increasingly aware of the importance of their data security. Given the scandals which came to light with Snowden's revelations about the powers and practices of the NSA and the Cambridge Analytical scandal, people are demanding higher standards of protection for their data. In addition, entities are aware of the bad press they could receive in case of data breach. GDPR could be respected outside the EU by entities for reputational reasons and not through fear of the huge fines. It is to be seen how effective this indirect applicability internationally actually will be.

When it comes to data transfer, the GDPR has brought some changes in comparison to the Data Protection Directive. It is the opinion of this Dissertation that the continued exception of consent to the rules about ensuring an adequate level of data protection after transfer undermines the purpose of the GDPR which is to provide Data Subjects with data protection rights which are inalienable, that cannot be waived or sold. In addition, there are serious questions about the effectiveness of the SCCs which can be used for transfer.

In addition, it is questionable how much confidence can be placed in the adequacy decisions of the European Commission. There are still serious questions about the Privacy Shield despite the European Commission's decision that it provides for a level of protection which is essentially equivalent to that in the EU. Given the comments by the WP29 and the EDPB on the first two annual joint review, it is

difficult to see if Privacy Shield is actually an improvement on Safe Harbour. It will be interesting to see the decision taken by the ECJ in Schrems II and La Quadrature du Net cases.

In conclusion, the GDPR seems to have fallen short of their ambitious aim of providing a comprehensive framework that can regulate data privacy internationally, however, this is not through lack of trying. It will have to be seen how the ECJ faces the challenges relating to the cross-border reach of the GDPR.

BIBLIOGRAPHY

BOOKS

- J. P. Albrecht and F. Jorzo, *Das neue Datenschutzrecht der EU*, Nomos, 2017
- J. P. Albrecht, *How the GDPR Will Change the World*, 2 Eur. Data Prot. L. Rev. 287 (2016)
- C. J. Hoofnagle, *Federal Trade Commission Privacy Law and Policy*, Cambridge University Press, 2016
- R. Jennings and A. Watts, *Oppenheim's International Law, Vol. 1, Peace*, Oxford University Press, 1992
- U. Kohl, *jurisdiction and the internet – Regulatory competence of the online activity*, Cambridge University press 2007, 20
- *Restatement (Third) of foreign relations Law of the United States*, The American Law institute, 1987
- C. Ryngaert, *Jurisdiction in International Law*, Oxford University Press 2008, 27
- Voigt, A. von dem Bussche, *The EU General Data Protection Regulation (GDPR), A Practical Guide*, Springer, 2017

ARTICLES

- M. Al Khonaizi, *Fines under EU GDPR in non-EU jurisdictions: Enforceable or Mere Reputation Risk*, Michigan Journal of International law Online, www.mjilonline.org/fines-under-eu-gdpr-in-non-eu-jurisdictions-enforceable-or-mere-reputation-risk/, Last accessed 9 August 2019
- A. Azzi, *The Challenges Faced by the Extraterritorial Scope of the General Data Protection Regulation*, 9 (2018) JIPITEC 126
- J. Baker, *EU Court Hearings to determine the future of Privacy Shield*, 25 June 2019, https://iapp.org/news/a/eu-high-court-hearings-to-determine-future-of-privacy-shield-standard-contractual-clauses/, last accessed 10 August 2019
- BDK Advokati, *Standard Contractual Clauses challenged by GDPR and scrutinized by the CJEU*, Lexology, https://www.lexology.com/library/detail.aspx?g=d4a4a515-4868-4445-8b1c-0d358feab8fe, last accessed 23 August 2019
- S. Bu-Pasha, *Cross Border Issues Under EU data protection law with regards to personal data protection*, Information and Communications Technology Law 2017, Vol. 26, No. 3, 213-228, 24 May 2017
- T. Clabum, *Safe Harbour Fails, European Court Rules*, InformationWeek, 19 May 2016
- M. Czerniawski, *Do we need to use of equipment as a factor for territorial applicability of the EU data protection regime?* in Dan Jerker B. Svantesson and Dariusz Kloza (eds), Trans-Atlantic data privacy as a challenge for democracy (Intersentia 2017) 221
- DLA Piper, *Schrems 2.0 – The Demise of Standard Contractual Clauses and Privacy Shield*, 1 July 2019, https://blogs.dlapiper.com/privacymatters/schrems-2-0-the-demise-of-standard-contractual-clauses-and-privacy-shield/, last accessed 10 August 2019
- S. Grynwajc, *GDPR: Surviving the likely demise of the Privacy Shield*, Law Office of S. Grynwajc, Transatlantic Legal Services, 8 July 2018

- P. de Hert and M. Czerniawski, *Expanding the European data protection scope beyond territory: Article 3 of the General Data Protection Regulation in its wider context*, 6 IDPL 230, 2016
- D. J. Kessler, J. Nowak and S. Khan, *The Potential Impact of Article 48 of the General Data Protection Regulation on Cross Border Discovery from the United States*, (2016) 17(2) The Sedona Conference Journal 577
- A. Kloth, Volkerrechtsblog, *International Law and International Thought, "One law to rule them all, on extraterritorial applicability of the new EU General Data Protection Regulation*, 5 February 2018, https://voelkerrechtsblog.org/one-law-to-rule-them-all/, last accessed 12 August 2019
- Christopher Kuner, *Data protection law and international jurisdiction on the internet (Part 1)*, (2010) 18 IJLT 176
- N. Lomas, *EU-US Privacy Shield compliant to be heard by Europe's top court in July, Tech Crunch*, 28 May 2019, www.techcrunch.com/2019/05/28/eu-us-privacy-shield-complaint-to-be-heard-by-europes-top-court-in-july/
- A. Myers, *Top 10 operational impacts of the GDPR: Part 4 – Cross-border data transfers*, 19 January 2016, https://iapp.org/news/a/top-10-operational-impacts-of-the-gdpr-part-4-cross-border-data-transfers/, last accessed 11 August 2019
- P. M. Schwartz and K. Peifer, *Transatlantic Data Privacy*, 106 Georgetown Law Journal 115 (2017)
- M. Taylor, *Permissions and prohibition in data protection jurisprudence*, (2016) 2 Brussels Privacy Hub working paper 3
- B.Van Alsenoy, *Reconciling the (extra)territorial reach of the GDPR with Public International law*, in Data Protection and Privacy Under Pressure, Transatlantic Tensions, EU surveillance, and big data, Gert Vermeulen and Eva Lievens (Eds), Maklu-Publishers, 2017
- M. A. Weiss and K. Archick, *US-EU Data Privacy: From Safe Harbour to Privacy Shield*, Congressional Research Service, 19 May 2016
- M. Young and S. Jungyun Choi, *Privacy Shield Ombudsperson Confirmed by the Senate*, 25 June 2019, https://www.insiderprivacy.com/cross-border-transfers/privacy -shield-ombudsperson-confirmed-by-the-senate/, last accessed 10 August 2019
- P. Zeni, F. Gilbert and M. Calehuff, *GDPR and Privacy Shield: Difference Tools for Different Goals*, 36 ACC Docket 78, 36 No. 7 Acc Docket 78, September 2018
- J. Zittrain, *Be careful what you ask for: Reconciling a Global Internet and Local Law*, Harvard Law School Public Law Research Paper No. 03/2003

REPORTS

- Sidley, *Esentially equivalent, A comparison of the Legal Order for Privacy: From the European Union and the United States*, Sildey, 25 January 2016

LEGISLATION AND TREATIES

European Union

- The Charter of Fundamental Rights of the European Union, 2012/C 326/02

- The Treaty on the Functioning of the European Union, Official Journal, C 326, 26/10/2012 P. 0001-0390
- Directive 95/46/EC of the European Parliament and the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal, L 281, 23/11/1995 P. 00031 – 0050
- Council Regulation (EC) no 44/2001 of 22 December 2000 on Jurisdiction and the recognition and enforcement of judgements in civil and commercial matters, Official Journal L012, 16/01/2001 P.0001-0023
- *EU General Data Protection Regulation (GDPR):* Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), Official Journal 2016 L 119/1.

United States of America

- Executive Order 12333
- The First Amendment of the Constitution of the United Stated
- Foreign Intelligence Surveillance Act

REPORTS AND PRESS RELEASES FROM EUROPEAN UNION BODIES

Article 29 Working Party and European Data Protection Board

- Working Party on the Protection of Individuals with Regard to the Processing of Personal Data, Opinion 1/99, Adopted on 26 January 1999, 2 DG MARKT Doc. 5092/98, WP 15
- Article 29 Data Protection Working Party, Working Document on determining the international application of EU data protection law to personal data processing on the Internet by non-EU based web sites, Adopted 30 May 2002, 5035/01/EN/Final, WP 56
- Article 29 Working Party, Working Document on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995, Adopted 25 November 2005, 2093/05/EN, WP 114
- Article 29 Data Protection Working Party, Opinion 1/2010 on the concepts of "controller" and "processor", Adopted 16 February 2010, 00264/10/EN, WP169
- Article 29 Data Protection Working Party, Opinion 8/2010 on application law, Adopted on 16 December 2010, 0836-02/10/EN, WP 179
- European Data Protection Bored, Guideline 3/2018 on the Territorial scope of the GDPR (Article 3) – Version for public consultation, Adopted on 16 November 2018

The European Commission

- Communication from the Commission to the European Parliament and the Council Transatlantic Data Flows: Restoring Trust Through Strong Safeguards, Brussels, 29 February 2016, COM (2016) 117 final

- The European Commission, 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-US Privacy Shield, Official Journal, L 207/1
- ANNEXES to the Commission Implementing Decision 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, C(2016) 4176 final, Brussels 12 July 2016, Annex I/Annex 1 (Letter from acting Under Secretary for the International Trade Ken Haytt) to Commission decisions (EU) 1250/2016
- The European Commission, 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, 18 October 2017, SWD(2017) 344 final
- European Commission, "Automated decision-making on the basis of personal data that has been transferred from the EU to companies certified under the EU-U.S. Privacy Shield: *Fact-finding and assessment of safeguards provided by U.S. law", October 2018*
- Opinion of the European Data Protection Supervisor on the Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions, A comprehensive approach on personal data protection in the European Union, Brussels, 14 January 2011, https://edps.europa.eu/sites/edp/files/publication/11-01-14_personal_data_protection_en.pdf, last accessed 14 August 2019

The European Parliament

- European Parliament, Resolution of 5 July 2018 on the adequacy of the protection afforded by the EU-US Privacy Shield, 2018/2645(RSP)

Press Releases

- Court of Justice of the European Union Press Release, The Court of Justice declares that the Commission's US Safe Harbour Decision is invalid, Press Release No. 117/15, Luxembourg, 6 October 2015
- European Commission Press Release, European Commission launches EU-US Privacy Shield: Stronger Protection for transatlantic data flows, Brussels 12 July 2016
- European Commission Press Release, EU-US Privacy Shield: First review shows it works but implementation can be improved, Brussels, 18 October 2017, IP/17/3966

Privacy Shield Annual Joint Reviews

- Article 29 Data Protection Working Party, EU/US Privacy Shield, first annual joint review, Adopted 28 November 2017, 17/EN WP 255
- The European Commission, 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(2017) 344 final
- The European Data Protection Board, EU-US Privacy Shield – Second Annual Joint Review, 22 January 2019

CASE LAW

The European Court of Justice

- Judgement of the Court of the European Union (Grand Chamber) of 13 May 2014, Google Spain, Google Spain SL and Google Incorporated v Agencia Espanola de Proteccion de datos (AEPD) and Costeja Gonzalez, Case C-31/12, EU:C:2014:317
- Judgement of the Court (Grand Chamber) of 7 December 2010, Hotel Alphenhof GesmbH v Oliver Heller, Case C-144:09, EU:C:2010:740
- Judgement of the Court (Grand Chamber) of 6 October 2015, Maximillian Schrems v Data Protection Commissioner, Case C-362/14, EU:C:2015:650
- Judgement of the Court (Grand Chamber) of 7 December 2010, Peter Pammer v Reederei Karl Schlüter GmBH & Co. KG, Case C-585/08, EU:C:2010:740
- Judgement of the Court (Third Chamber) of 28 July 2016, Verein für Konsumenteninformation v Amazon EU Sàrl, Case C-191/15, EU:C:2016:388
- Judgement of the Court (Third Chamber) of 1 October 2015, Weltimmo sro v Nemzeti adatvédelmi és informacriowabadsag hatosag, Case 230/14, EU:C:2015:639

Pending Cases before the The European Court of Justice

- Case before the European Court of Justice, Facebook Ireland and Schrems, Case C-311/18
- Case before the European Court of Justice, La Quadrature du Net and Others v Commission, case T-738/16

The United States of America

- Abdullah v. Sheridan Square Press, Inc., No. 93CIV.2515 (LLS), 1994 WL 419847, at *1 (S.D.N.Y. May 4, 1994)
- Clapper v Amnesty International, 568 U.S. 398 (2013)
- Matusevitch v. Telnikoff, 877 F.Supp. 1, 2 (D.D.C. 1995), Mata v. Am. Life Ins. Co., 771 F. Supp. 1375, 1384 (D. Del. 1991),

INTERNET SOURCES

- Department of Commerce of the United State of America, EU-US Privacy Shield Framework Principles 4 (2016), https://www.privacyshield.gov/EU-US-Framework https://perma.cc/V2NJ-T6BZ, Last accessed 8 August 2019
- Department of Commerce of the United State of America, EU– U.S. Privacy Shield Framework Principles 7 (2016), https://www.privacyshield.gov/EU-US-Framework, Last accessed 8 August 2019
- Department of Commerce of the United State of America, "The EU-U.S. and Swiss-U.S. Privacy Shield Frameworks Information for EU and Swiss Individuals", www.privacyshield.gov/servlet/servlet.FileDownload?file=015t0000000QJdq, last accessed 10 August 2019

- The European Commission, « Adequacy Decisions, how the EU determines if a non-EU country has an adequate level of data protection, https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en, last accessed 8 August 2019
- The Information Commissioners Office, "Intention to fine British Airways £183.39m under GDPR for data breach", 08 July 2019 www.ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/07-announces-intention-to-fine-british-airways/
- The Information Commissioners Office, "Intention to fine Marriott International, Inc more than £99 million under GDPR for data breach", 09 July 2019 www.ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/07/intention-to-fine-marriott -international-inc-more-than-99-million-under-gdpr-for-data-breach/
- Intersoft Consulting, "GDPR Third Countries", www.gdpr-info.eu/issues/third-countries/, last accessed 8 August 2019
- The Privacy Shield Framework, "Enforcement of Privacy Shield", http://www.privacyshield.gov/article?id=Enforcement-of-privacy-shield, last accessed 11 August 2019