SCHOOL OF
ECONOMICS AND
MANAGEMENT

The Territorial Scope of GDPR: Conditions, Extraterritorial Application and Implications

Kehan Ruan

DEPARTMENT OF BUSINESS LAW

Master Thesis in European and International Trade Law

15 credits

HARN63

Spring 2024

Contents

Abstract

The General Data Protection Regulation (GDPR) has been called the strictest data protection law in history, and one of the key reasons for this is due to its vast territorial scope, which allows it to be applied to non-EU entities as long as the relevant conditions are met. Such a broad extraterritorial application has greatly improved the level of data protection, but it has also triggered some controversies and concerns.

This thesis takes the territorial scope of the GDPR as the subject of study, analyses the conditions for the application of Article 3 of the GDPR as well as evaluates it through the interpretation of the legislation and the case law. Then, the paper analyses the conflicts and shortcomings of the rule in practical application, involving the conflicts and interactions between the territorial scope and the data transfer rules, with the problems encountered in the practice of the representative regime. It proposes solutions such as merging the territorial scope and data transfer rules and guiding the commercialization of representative services. The last part of the thesis explores the implications of the extraterritorial application of the GDPR from an international trade perspective, where some of the GDPR's rules may potentially violate the national treatment and most favoured nation (MFN) requirements of the GATS, either de jure or de facto. In addition, it may create three types of trade barriers: social, regulatory, and technical. Finally, recommendations are provided to help eliminate trade barriers for third countries and the EU respectively. For third countries, it is possible to apply for adequacy decisions, upgrade the level of domestic data protection, and promote data protection standards that are in the national interest. For the EU, more interpretations and guidelines can be developed, and asymmetric enforcement can be implemented.

Keywords: GDPR, Territorial scope, Extraterritorial application, Data transfer, International trade, GATS, Trade barrier

Abbreviations

AEPD	Spanish data protection authority
CJEU	Court of Justice of the European Union
DPF	Data Privacy Framework
EDPB	European Data Protection Board
EU	European Union
GATS	General Agreement on Trade in Services
GATT	General Agreement on Tariffs and Trade
GDPR	General Data Protection Regulation
MFN	Most favoured nation
WTO	World Trade Organisation

1 Introduction

1.1 Background

The protection of personal data has always been an important issue under European Law. As a fundamental right, the right to protect personal data was granted by the Charter of Fundamental Rights of the European Union. To strengthen data protection on a legal level, the Data Protection Directive was enacted in 1995. After years of practice and cooperation between countries, the GDPR came into force on May 25, 2018, bringing the level of personal data protection in the EU to unprecedented heights, which is hailed as "the strictest data protection law in history".

Such praise is due not only to the GDPR's high level of personal data protection within the EU but also to its expansion of this protection beyond the EU. Article 3 of GDPR creates the establishment criterion and targeting criterion, which can regulate the processing of data by entities outside the EU under certain circumstances. In the establishment criterion, GDPR can be applied to processing activities by the establishment of a controller or processor in the EU. In targeting criterion, GDPR can be applied if an entity offers goods or services to individuals or monitors the behavior of individuals within the EU. It follows that the territorial scope of the GDPR is quite broad, and subsequent CJEU judgments have further broadly interpreted the provision, thereby expanding the application of the GDPR. For example, in C-230/14 Weltimmo, the CJEU extended the definition of establishment "to any real and effective activity - even a minimal one - exercised through stable arrangements"[1].

The extensive extraterritoriality has given rise to a series of controversies and concerns both within and outside the EU. Some criticize the territorial scope may have conflicts with relevant articles in GDPR.[2] Also, there are some controversies that the GDPR acts as a barrier to international trade by placing high compliance requirements on non-EU companies and hindering the cross-border data flow of services.[3]

1.2 Purpose and research questions

The purpose of the thesis is to clarify the application of the territorial scope of GDPR, explore the flaws and conflicts of its application, and also analyze its implications on international trade aspect.

[1] Case C-230/14 Weltimmo s.r.o. v Nemzeti Adatvédelmi és Információszabadság Hatóság [2015] ECR 639

[2] Kuner C, 'Protecting EU Data Outside EU Borders under the GDPR' (2023) 60 Common Market Law Review 77

[3] Meddin E, 'The Cost of Ensuring Privacy: How the General Data Protection Regulation Acts as a Barrier to Trade in Violation of Articles XVI and XVII of the General Agreement on Trade in Services' (2020) 35 American University International Law Review 997

The research questions are as follows: What are the conditions for the application of Article 3 and whether there are any uncertainties? What are the conflicts and shortcomings in the articles and application of territorial scope, and are there feasible solutions? What are the implications of the extraterritorial application on international trade?

1.3 Delimitations

This thesis has two types of delimitations as follows: First, this thesis interprets Article 3 of the GDPR in a way that does not include an interpretation of Article 3(3) of the GDPR. This is because the expression of Article 3 is very clear and the scope of application is small, so there is no necessity for further analysis. Secondly, the impact of the extraterritorial application of the GDPR in this paper mainly focuses on the impact on international trade, because it is significant and there are possibilities for in-depth analyses.

1.4 Method and materials

Based on the fact that the topic of this thesis is the application of the territorial scope of the GDPR, this thesis adopts a legal approach to research, using EU regulations and case law, academic articles, etc. as research materials. For example, regarding the process of interpreting regulations, this thesis uses EU regulations, the Guideline of EDPB, and case law for interpretation, supplemented by academic opinions for analysis and evaluation. It should be clarified that since the GDPR is a revised law based on Directive 95/46/EC, this thesis also uses cases from the period when the Directive is in force to illustrate the rules of the GDPR. In addition, this thesis also makes limited use of the comparative method by introducing other national or international regulations as research material to compare with the GDPR or other laws and to analyze the potential problems of the GDPR. Besides, for a part of the facts needed in the exposition, the data disclosed on the web is also analyzed as factual material.

1.5 Outline

The outline of this thesis is to first interpret Article 3 of GDPR through both text and case laws, in order to clarify the conditions for the application of the territorial scope of GDPR. Then, it will analyze conflicts and shortcomings in the application of territorial scope, as well as explore possible measures to solve them. Last, it will analyze the implications of the extraterritorial application of GDPR, focusing on the field of international trade.

2 Conditions for the application of Article 3

2.1 Introduction

Conditions for the application of territorial scope are determined by Article 3 of GDPR. To interpret it, EDPB has concluded two criteria for the application of Article 3(1) and Article 3(2) according to Guidelines 3/2018 on the territorial scope of the GDPR, which are the establishment criterion and targeting criterion. These two criteria had a lot of interpretation gaps at the beginning of the GDPR's entry into force, and after several judgments and the EDPB's Guideline, the conditions for their application have been further interpreted and expanded.

Therefore, this chapter will first interpret Article 3 of GDPR into establishment criterion and targeting criterion with relevant case law, explore the uncertainties in interpretation, followed with the conclusion and evaluation of conditions for the application of Article 3.

2.2 Controller and processor

Before analyzing the application of Article 3 of GDPR, it should first look at the definition of data controller and data processor. On the basis of Article 4(7) and 4(8) of GDPR, the controller and processor can both be 'the natural or legal person, public authority, agency or other body'. The controller is the party that 'determines the purposes and means of the processing of personal data', which means determining the data to be processed, length of storage, access, etc.[4] The processor is the party that 'processes personal data on behalf of the controller', and it can also determine the ways of processing from a technical or organizational perspective on the delegation of the controller.[5]

2.3 Establishment criterion

The establishment criterion is based on Article 3(1) of GDPR: 'This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.' To interpret it, it is important to clarify the two key points in Article 3(1), which are 'an establishment in the Union', and 'the processing of personal data in the context of the activities of an establishment in the Union'.

[4] Article 29 Data Protection Working Party, 'Opinion 1/2010 on the concepts of "controller" and "processor"' [2010]
[5] Ibid

2.3.1 'An establishment in the Union'

In regard to the definition of 'An establishment in the Union', the articles of GDPR do not provide a specific criterion. Instead, it was mentioned in the Recital 22 of GDPR[6] and Recital 19 of Directive 95/46/EC that an establishment can be defined if it has "the effective and real exercise of activity through stable arrangements", regardless of the legal from of the arrangements. The concept has been expanded and clarified through several judgments of CJEU, such as Google Spain SL, Google Inc. v AEPD, Mario Costeja González (C-131/12), and Weltimmo v NAIH (C230/14), which provide a feasible application reference for the identification of "an establishment" and has been kept using under GDPR.

Weltimmo, a Slovak-registered company that operated a Hungarian real estate trading website, failed to delete customers' advertisements upon request and charged advertisement fees. For this, it was fined by the Hungarian Data Protection Authority. However, Weltimmo argued that it was a company registered in Slovenia and that Hungarian law should not be applied to it by the Hungarian authorities. Thus, an important issue in this case is whether Weltimmo can be identified as an establishment in Hungary under Article 4(1)(a) of Directive 95/46.

The CJEU determined that, in view of the objectives pursued by the Directive, namely to ensure effective and comprehensive protection of the right to privacy and to avoid any circumvention of national rules, the notion of "establishment" under the Directive should be extended as "any real and effective activity — even a minimal one — exercised through stable arrangements."[7] The determination of the existence of stable arrangements and effective activities is based on an analysis of the economic activity and the delivery of services.[8] In some cases, the presence of only one representative may be sufficient to constitute a stable arrangement, provided that the representative acts with sufficient stability and possesses in the Member State the equipment necessary for the provision of the specific service.[9]

To judge by the facts, Weltimmo has a representative in Hungary who represents the company in administrative and judicial proceedings. It also has a bank account and a mailbox in Hungary.[10] Also, taking into account that Weltimmo's business is to operate a real estate website in Hungary, presenting it in Hungarian and charging for advertisements. Therefore, it can be recognized as a real and effective activity through stable arrangements.[11]

For the notion of "stable arrangements", the Guidelines 3/2018 on the territorial scope of the GDPR provides a further interpretation. It claims that when it comes to

[6] Recital 22 of GDPR: "Any processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union should be carried out in accordance with this Regulation, regardless of whether the processing itself takes place within the Union. Establishment implies the effective and real exercise of activity through stable arrangements. The legal form of such arrangements, whether through a branch or a subsidiary with a legal personality, is not the determining factor in that respect."

[7] Case C-230/14 Weltimmo s.r.o. v Nemzeti Adatvédelmi és Információszabadság Hatóság [2015] ECR 639, Para 31

[8] Ibid, Para 29

[9] Ibid, Para 30

[10] Ibid, Para 32

[11] Ibid, Para 33

online services, even one employee or agent may constitute “stable arrangements”, as long as that employee or agent “acts with a sufficient degree of stability.”[12]

In conclusion, to judge an entity is an establishment under the GDPR, it is necessary to determine whether it has a stable arrangement with real and effective activities, referring to case Weltimmo and Guidelines 3/2018. However, there is no suitable reference on what is a real and effective activity, which leaves a certain gap for application.

2.3.2 'In the context of the activities of an establishment'

To apply Article 3(1), the processing of personal data needs to be carried out in the context of the activities of an establishment, the interpretation of which was built by the case of Google Spain. In the case, Mr. Costeja sued Google Spain for seeking to remove his personal information from Google searches.[13] The first issue of the case is whether Google Spain can satisfy the establishment criteria, which goes to the question of whether its data-processing activities are carried out 'in the context of the activities of an establishment'.[14]

CJEU answered that, in light of the objectives of the Directive, the interpretation should not be restrictive.[15] Thus, although the data processing of the Google search engine is located at Google's headquarters in a third country, it has an establishment in Spanish territory with the purpose of marketing.[16] The operation and data processing of the search engine provides profitability for Google Spain and the activities of the Google headquarters are inextricably linked to Google Spain.[17] It is clear to see that the relevant data processing takes place in the context of the commercial activities of the establishment.[18]

In the wake of this case, an 'inextricable link' has been included in the application, which is a case-by-case judgment for the CJEU. An 'inextricable link' means the data processing is related to and inextricable from the establishment's activities in the EU[19], especially when data processing is associated with increased revenue for the establishment. [20]

In conclusion, when examining whether the data processing was conducted in the context of the activities of an establishment, the relations between data processing with the business or function of the establishment, such as marketing, publicity, or profiting. It’s crucial to check if these two have an 'inextricable link'. Also,

[12] Guidelines 3/2018 on the territorial scope of the GDPR (Article 3), European Data Protection Board, 2018, P7

[13] Case C-131/12 Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González [2014] ECR 317, Para 15

[14] Ibid, Para 32

[15] Ibid, Para 54

[16] Ibid, Para 55

[17] Ibid, Para 56

[18] Ibid, Para 57

[19] Article 29 Data Protection Working Party, ‘Update of Opinion 8/2010 on applicable law in light of the CJEU judgement in Google Spain’ [2016], P7

[20] Guidelines 3/2018 on the territorial scope of the GDPR (Article 3), European Data Protection Board, 2018, P8

considering the interpretation is still vague, the determination should be based on an analysis in concreto through specific facts of the case.[21]

2.4 Targeting criterion

The targeting criterion stems from Article 3(2) of GDPR, which applies to data processing falling into two categories, 'offering of goods or services, irrespective of whether a payment of the data subject is required, to data subjects in the Union' or 'the monitoring of their behavior as far as their behavior takes place within the Union.' Under the targeting criterion, the existence of an establishment in the Union is not taken into account.[22] Instead, it only applies to the data processing by a controller or processor that doesn't have an establishment in the Union. In addition, it is important to interpret the two categories of activities above based on case-by-case analysis.[23]

2.4.1 'Data subjects'

Before interpreting the criterion, it is necessary to define what is 'data subjects' under GDPR. It refers to Recital 14 of GDPR that the protections of the GDPR apply to the processing of personal data of natural persons, regardless of their nationality or place of residence.[24] It is further explained that data subjects mean natural persons in the EU, whether or not they are EU citizens. Moreover, the targeting criterion only applies in cases where the data processing is intentionally directed at natural persons in the EU and at the same time relates to one of the two activities under 3(2).[25]

2.4.2 'Offering of goods or services, irrespective of whether a payment of the data subject is required, to data subjects in the Union'

The first step in determining this category of activity requires clarification of the concept of goods and services. The GDPR does not provide a specific explanation of goods and services, but it can be found in other EU regulations. The Consumer Rights Directive (2011/83/EU) defines goods are any tangible movable items, including water and electricity under certain circumstances.[26] Regarding services, the information society services are also included, referring to Directive (EU)

[21] Guidelines 3/2018 on the territorial scope of the GDPR (Article 3), European Data Protection Board, 2018, P7

[22] Guidelines 3/2018 on the territorial scope of the GDPR (Article 3), European Data Protection Board, 2018, P13

[23] Ibid, P14.

[24] Recital 14 of GDPR: "The protection afforded by this Regulation should apply to natural persons, whatever their nationality or place of residence, in relation to the processing of their personal data."

[25] Guidelines 3/2018 on the territorial scope of the GDPR (Article 3), European Data Protection Board, 2018, P15

[26] Council Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament [2011] OJ L304/64, Article 2(3)

2015/1535 that "any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services".[27]

The next step is to examine whether the controller or processor obviously intends to offer goods or services to data subjects in one or more Member States within the EU, which is used to determine whether a controller or processor is offering goods or services to data subjects according to Recital 23.[28] The EDPB provides a number of factors to be checked, including delivery of goods in the EU, use of an EU web domain, having a dedicated address or phone number in an EU country, use of an EU language or currency, etc.[29] However, a single factor could not become decisive. The factors should be considered in conjunction with the facts of the case to determine whether they fall within the concept of offering goods or services.[30] On the contrary, some factors provided by Recital 23 can be used as exclusions. If the controller, processor, or intermediary displays a website, or e-mail address in the EU or uses a language commonly spoken in the third country where the controller is located, this is not sufficient as a basis for determining the intention.[31]

The guidance given by the EDPB appears to be easy to apply, but it has also attracted criticism. In the case of Pammer and Hotel Alpenhof, the court explained the "direction" of the activity by the fact that the enterprise was directed towards the goal and result of winning customers.[32] Such an interpretation may also be applied to the GDPR's interpretation of "intention". Svantesson, in his paper, expressed a negative view of the outcome of this judgment. He argues that, in practice, it is important to separate the objectives of an entity from its results, such as when an activity is not intended to win customers, but achieves such a result. If too much attention is paid to the objective, the actual effect of the result of the activity can be overlooked.[33]

Value can be seen in this argument and, as noted above, whilst the EDPB lists a number of factors that can be used to take into account the controller's or processor's "intention", the overall picture is too vague and there are gaps in practice. If the results of data activities were included in the determination of the criteria, it would clearly be possible to judge more objectively whether a controller or processor has fallen within the "Offering of goods or services" criterion.

[27] Council Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services [2015] OJ L241/1

[28] Recital 23 of GDPR: "in order to determine whether such a controller or processor is offering goods or services to data subjects who are in the Union, it should be ascertained whether it is apparent that the controller or processor envisages offering services to data subjects in one or more Member States in the Union."

[29] Guidelines 3/2018 on the territorial scope of the GDPR (Article 3), European Data Protection Board, 2018, P17

[30] Ibid, P18.

[31] Recital 23 of GDPR: "Whereas the mere accessibility of the controller's, processor's or an intermediary's website in the Union, of an email address or of other contact details, or the use of a language generally used in the third country where the controller is established, is insufficient to ascertain such intention."

[32] Case C-585/08 Peter Pammer v Reederei Karl Schlüter GmbH & Co. KG [2010] ECR 273

[33] Svantesson DJB, 'Extraterritoriality and Targeting in EU Data Privacy Law: The Weak Spot Undermining the Regulation' (2015) 5 International Data Privacy Law 226

2.4.3 'The monitoring of their behavior as far as their behavior takes place within the Union'

In order to define this activity, primary reference should be made to the statements the Guideline. It states that the key to judging "monitoring the behavior of data subjects" is to identify whether natural persons are being tracked on the Internet. The next step is to identify the techniques that may be used for data processing and the purposes to be achieved, for example, for the analysis or prediction of the characteristics, personal preferences, behaviors, attitudes, etc. of natural persons.[34] It follows from the text that not all online collection of personal data falls under "monitoring" under the GDPR, the more important factor is to analyze the purpose of data processing. The EDPB also helps define several obvious types of monitoring activities, including behavioral advertising, geo-targeting, personal health and diet analysis, online tracking using technologies such as cookies or fingerprinting, personal behavioral profiling, etc.[35]

Generally speaking, the targeting criterion is complementary to the establishment criterion. It regulates the cases in which data controllers and processors do not have an establishment within the EU in order to circumvent EU controls. The targeting criterion places more emphasis on the actual effect or intent of data processing, thus enabling the determination of those who are targeting personal data within the EU.

2.5 Conclusion and evaluation

Through the above interpretation, it can be seen that the application conditions of the GDPR territorial scope include the establishment criterion and the targeting criterion. For data processing, it is necessary to determine firstly whether its controller or the processor has an establishment in the EU. This requires an effective and genuine activity through a stable arrangement. Also, the data processing needs to be in the context of the activities of an establishment and the determination needs to be based on an examination of the responsibilities of the organization or individual in the EU and the purpose of the data processing. With reference to previous cases, the requirements to meet the standards for organizations may be very low.

If the establishment criterion is not applicable, a judgment should be made as to whether it falls within the targeting criterion, which requires the data processing related to offering goods and services to the data subjects in the Union or monitoring the behavior of the data subjects as far as their behavior takes place within the Union. There are not many cases to refer to regarding these two types of activities, so judgment can be made by referring to EDPB's Guideline, which lists many realistic factors that can be used as a basis for evaluation. Case-by-case judgment should be made in conjunction with the nature and purpose of the specific data processing.

[34] Recital 24 of GDPR: "In order to determine whether a processing activity can be considered to monitor the behaviour of data subjects, it should be ascertained whether natural persons are tracked on the internet including potential subsequent use of personal data processing techniques which consist of profiling a natural person, particularly in order to take decisions concerning her or him or for analysing or predicting her or his personal preferences, behaviours and attitudes."

[35] Guidelines 3/2018 on the territorial scope of the GDPR (Article 3), European Data Protection Board, 2018, P20

Evaluating the territorial scope, it is undeniable that it strengthens the protection of GDPR, because it creates a very broad extra-territorial scope of application of the GDPR, making it possible for controllers and processors in third countries to be regulated by the GDPR.

Also, it helps reduce the circumvention of the GDPR. Since international enterprises often collect data for processing in third countries or entrust it to other processors, it is often difficult to decide which country's law should regulate such behavior, e.g., the law of the place where the data are processed or the law of the place where the data subjects are located. Such confusion can create inconveniences for transnational legal practice. Article 3 directly applies the GDPR to more data processing involving personal data within the EU, which solves the problem of legal application to cross-border online data processing.

However, as can be seen from the EDPB Guidelines for Article 3, many of the criteria elements do not have very clear definitions, exhaustive lists, or sufficient case references, instead, they are more likely to be analyzed by the courts based on the individual facts of each case. It leaves uncertainty about the application of the law, which is certainly favorable for improving the degree of protection and expanding the scope of protection, but it will also correspondingly increase the compliance burden of enterprises and increase the difficulty of practicing the GDPR.

3 Conflicts and shortcomings in the application of territorial scope

3.1 Introduction

Since the introduction of the GDPR, various types of criticism of its extraterritorial application have never ceased. Non-EU processors and controllers have faced a lot of confusion or difficulties regarding the interpretation of the rules, the specifics of the application, and the compliance requirements in practice. The next section will focus on two types of conflicts and shortcomings that have surfaced in the extraterritorial application of the GDPR.

3.2 The conflicts and interplay between territorial scope and data transfer rules of GDPR

The GDPR's territorial scope and data transfer rules have been a source of concern in practice for data processors, controllers, and scholars. This is because these two rules share similar rationales but there is not enough clarification on how they interact with each other, which leads to inconsistency and confusion in their application.[36] To explore this topic, the rules for the application of territorial scope have been explained in the previous section. Therefore, this section will describe the data transfer rules next, as well as the conflicts and interactions between the two rules, and will conclude with the measures and potential concerns at last.

3.2.1 Data transfer rules of GDPR

The data transfer rules are the rules applicable to the transfer of personal data from the EU to third countries. As a result of such transfers to third countries, whose laws do not necessarily have the same level of protection as the GDPR, and in order to guarantee that the protection of natural persons' data is not undermined, Chapter V of the GDPR sets out the necessary measures that should be taken in the case of international data transfers, including adequacy decision, Binding corporate rules, Standard Data Protection Clauses, etc.[37] These measures enable the same level of protection as the GDPR for personal data within the EU transferred to third countries. In addition, Article 49 provides exemptions for data transfers to third countries under several specific situations.

3.2.2 Conflicts and interplay

Comparing data transfer rules and territorial scope regarding their objectives, similar ones can be found in Recital 23 "In order to ensure that natural persons are not deprived of the protection to which they are entitled under this Regulation" and

[36] See supra note 2

[37] See Article 44 of GDPR

Article 44 “In order to ensure that the level of protection of natural persons guaranteed by this Regulation is not undermined”. Meanwhile, they apply measures from different angles to reach the goals. The data transfer rules use additional measures on the data transferred to third countries to ensure the protection level same as GDPR, while the territorial scope intends to apply GDPR directly to the data processing outside EU borders.[38]

When these two sets of rules apply in practical situations, both of them can occur in relation to the same data processing, i.e. where personal data within the EU are transferred to a third country for processing, and that processing also falls into a situation under Article 3(2). In terms of Facebook Inc., which is based in the United States, when EU users use the platform, their personal data are transferred to servers located in the United States for processing,[39] which can be defined as data transfers to a third country. However, as the Spanish data protection authority (AEPD) pointed out in its decision to fine Facebook $1.2 million in 2017, Facebook processes user information for advertising targeting purposes. Such data processing can either make the GDPR directly applicable to it following the rules of territorial scope, or it can be subject to measures corresponding to the level of protection of the GDPR in accordance with the rules of data transfer. Therefore, in this case, the business side is confusing what approach to take in order to avoid violating the GDPR, which would undoubtedly be burdensome for the business if both sets of rules were to be applied. Moreover, there is a gap in the guidance on what measures should be taken to better protect personal data.

Besides, the protection from territorial scope could be harmed by the different legal frameworks of a third country. As stated in the Guidelines, when the data processing falls under Article 3(2) due to approaches by the data importer, the GDPR will apply directly to that processing. Since third countries have their legal frameworks, which may conflict with the GDPR, this will undermine the protection level of the GDPR.[40] The scenario can be found in the case of Schrems II that the U.S. Foreign Intelligence Surveillance Act allows U.S. government executives to obtain foreign intelligence information to spy on non-U.S. citizens, potentially located outside the United States.[41] While the law consists of proportionality and minimization procedures similar to the GDPR, it does not apply to non-U.S. persons located outside the United States.[42] This means if protection is based on applying the GDPR to data processing, i.e., in accordance with the territorial scope, then the protection is likely to be struck down by US law and be monitored by the US government.

3.2.3 Measurements by EDPB

In order to clarify the conditions for the application of the data transfer rules and to illustrate their interplay with the territorial scope rules, the EDPB has issued a

[38] See supra note 2

[39] Case C-311/18 Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems [2020] ECR 559

[40] Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR, European Data Protection Board, 2021, Para 4.

[41] See supra note 39

[42] See supra note 37

Guideline on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR.

The guideline defines the concept of "transfer of personal data to a third country or to an international organization", and Chapter V of the GDPR applies if three cumulative criteria are met:

> *1) A controller or a processor ("exporter") is subject to the GDPR for the given processing. 2) The exporter discloses by transmission or otherwise makes personal data, subject to this processing, available to another controller, joint controller or processor ("importer"). 3) The importer is in a third country, irrespective of whether or not this importer is subject to the GDPR for the given processing in accordance with Article 3, or is an international organization."*[43]

It can be seen that the EDPB considers that data processing can be applied to both Article 3 and Chapter V of the GDPR.

The EDPB also describes the interrelationship between the territorial scope and the data transfer rules. As mentioned above, the EDPB has emphasized the risk that making the GDPR directly applicable to data processing on the basis of Article 3 alone may result in less effective protection. For example, data processing in third countries may be subject to legal frameworks that conflict with the GDPR, reducing the level of protection, or it may be more difficult to obtain remedies outside the EEA. Therefore, the measures in the Data Transfer Rules should be complementary to Article 3.[44]

In addition, the EDPB provides guidance on what to do when both sets of rules apply at the same time. It states that Article 3 should be considered when the processor or controller is already subject to the GDPR, and to avoid duplicating the safeguards provided by the GDPR in the instrument of transfer. Instead, the protection should be improved by adding specific clauses in the instrument of transfer, taking into account the actual situation in the place where the data is received and the potential for particular risks.[45] This is a response to the EDPB's view that Chapter V is complementary to Article 3 and the direct application of the GDPR.

3.2.4 Concerns and potential solutions

The Guideline explains a number of previously unresolved matters, but it also raises a number of concerns on that basis.

A) Possibility of circumventing the application of Chapter V

It has been argued that the Guideline's interpretation of data transfer could provide a way to circumvent the application of the data transfer rules.[46] This is because the

[43] See supra note 39, Para 9

[44] See supra note 39, Para 4 & 23.

[45] See supra note 39, Para 29.

[46] Svetlana Yakovleva, 'GDPR Transfer Rules vs Rules on Territorial Scope: A Critical Reflection on Recent EDPB Guidelines from both EU and International Trade Law Perspectives' (2021)

EDPB considers that a data transfer requires an exporter and an importer of data, and if the exporter does not exist, then it cannot be considered a data transfer. Such a situation would occur when a data subject within the EU discloses personal data directly to a processor or controller outside the EU, which is a process without an exporter. Therefore, it does not constitute a data transfer and Chapter V cannot apply to such a situation.

The interpretation may seem reasonable theoretically, however, it creates a flaw in practice where companies may change their data processing strategies in response. For some multinational companies, the original data flow may have been to have branches in the EU collecting EU user data and then transferring it to data processing centers located outside the EU for processing. However, following the issuance of the Guideline, these companies may have made the data provided by EU users no longer collected and stored by organizations within the EU but instead flowed directly to data processing centers outside the EU.[47] In this way, they can avoid being recognized as data transfers and, more importantly, avoid being obliged to carry out data protection in accordance with the measures under Chapter V. Since data protection measures under Chapter V often increase a company's compliance costs, it is foreseeable that more and more companies will try to circumvent the application of Chapter V by changing the flow of data. The consequences are clear: the data protection measures under Chapter V will not be utilized as they should be and the level of data protection will be significantly reduced.

To solve this problem, it may be necessary to adopt a new definition of data transfer. The definition of data transfer should not be based on the existence of an importer and an exporter as a mandatory condition but should focus on whether the personal data has actually been transferred from within the Union to outside the Union. As long as it goes through a process from inside the EU to outside the EU, it should be recognized as a data transfer. Such modification could broaden the scope of application of Chapter V and avoid circumvention, further enhancing the level of data protection.

B) The remaining unresolved double burden of non-EU controllers and processors

The Guideline explains the interaction of the territorial scope and data transfer rules to some extent, for example, that a data processing that falls under Article 3(2) may also be a data transfer. However, such an explanation does not fundamentally address the difficulty of businesses applying two sets of rules since the Guideline does not indicate which legal obligations apply in such cases.[48] The underlying problem is that businesses are confused about carrying out their compliance measures and they are forced to comply with the obligations of two sets of rules because of one category of processing. The result is an increased compliance burden on businesses and a reduced incentive to comply with the GDPR.

---

https://europeanlawblog.eu/2021/12/09/gdpr-transfer-rules-vs-rules-on-territorial-scope-a-critical-reflection-on-recent-edpb-guidelines-from-both-eu-and-international-trade-law-perspectives/, accessed 30 April 2024

[47] Ibid

[48] Christopher Kuner, 'Exploring the Awkward Secret of Data Transfer Regulation: the EDPB Guidelines on Article 3 and Chapter V GDPR' (2021) https://europeanlawblog.eu/2021/12/13/exploring-the-awkward-secret-of-data-transfer-regulation-the-edpb-guidelines-on-article-3-and-chapter-v-gdpr/, accessed 30 April 2024

The fundamental solution to this problem is to merge the two sets of rules, territorial scope, and data transfer, into a more complete set of rules. The new rules would have a wider scope of application and could be applied to all cases of data processing and data transfers by non-EU entities.

3.3 The representative regime under GDPR and its problems encountered in practice

The GDPR's representation regime is based on Article 27, which applies in situations under Article 3(2), where the data controller or processor does not have an establishment in the EU and their data processing activities relate to the offering of goods or services to the data subject in the EU or the monitoring of the data subject's behavior in the EU. Eligible processors or controllers should have a representative in one of the EU Member States where the data subject is located. The function of the representative is to be authorized by the controller or processor to deal with relevant problems on their behalf with data subjects and supervisory authorities in the EU, in order to ensure compliance with the GDPR.[49]

3.3.1 The positive impact of the Representative regime

The representative regime has positive implications for the enforcement of the extraterritorial effects of the GDPR and helps controllers and processors outside the EU to comply with the GDPR. As the controllers or processors targeted by this regime do not have an establishment in the EU, EU supervisory authorities and EU data subjects have obvious difficulties in communicating their views or enforcing the law against them. For example, if an EU data protection authority needs to investigate whether a data controller is in breach of the GDPR but does not have an establishment in the EU, it will be difficult for the data protection authority to obtain the information needed for the investigation. For example, it may be difficult to get in touch with the controller, or the controller may deliberately not respond to the data protection authority. With a representative within the EU, the problem of difficult supervision and enforcement can be mitigated to some extent. In accordance with Articles 30 and 31 of the GDPR, the representative of the controller or processor shall keep records of the relevant processing, make them available to the supervisory authority on request, and cooperate with the supervisory authority in the performance of its tasks on request. This shows that the representative regime can help the regulator in its investigations, enforcement, and other actions.

In addition, the representative system complements the data protection officer regime, which was established under GDPR Articles 37, 38, and 39. The role of the data protection officer lies in being responsible for guiding compliance and preventing risks in data processing, which is more geared towards the prevention of issues within the organization.[50] The representative regime, as a bridge between the controller or processor and the data subjects and data protection authorities in the

[49] See Article 27 of GDPR
[50] See Article 38 of GDPR

EU, is well positioned to assist the controller or processor in communicating with the outside world, by virtue of its functional and geographic location.

3.3.2 Concerns and potential measures on the Representative regime

A) A low level of representative responsibility poses a risk to GDPR implementation

The establishment of the system of representatives has not only brought about positive effects but also some concerns and criticisms. Representatives have the function of communicating, conveying, keeping records of processing, and assisting the regulator, and failure to keep records of data processing or to assist the regulator in communicating with its clients can undermine the effectiveness of the representation system in practice. Therefore, it is important to monitor the due diligence of the representative and the liability for failure to do so. For this issue, the EDPB also states in the Guideline that representatives are only responsible for the direct obligations set out in Article 30 and Article 58(1).[51]

Relevant judgments are reflected in the case Sanso Rondon v LexisNexis. LexisNexis is the representative of World Compliance Inc. within the EU. Sanso Rondon brought a claim against LexisNexis, on the basis that World Compliance had infringed his rights. The primary focus of this case is therefore whether, in relation to a dispute between a data subject and a controller outside the EU, the data subject can bring a claim against the controller's representative within the EU. The England and Wales High Court ruled that the claim did not stand because a representative has a limited role that supports EU enforcement but cannot be enforced in place of a controller or processor.[52]

However, after clarifying the responsibilities of the representative, an important concern emerges. In the case of a GDPR violation by a data controller or processor, the representative's liability seems too narrow. Since the representative cannot be the subject of a data subject's claim, the claim can only be brought against the controller or processor behind it. However, because they are outside the EU, the jurisdictional limitations of the GDPR make it much more difficult to claim compensation, negatively impacting the data subject's access to remedies.

Instead, an expanded interpretation of the liability of the representative seems to be the more sensible option. Inconsistent with the Guideline, Recital 80 takes an affirmative position on this point. If the controller or processor fails to comply, the designated representative should be subject to enforcement proceedings.[53] The Spanish data protection law is also a proponent of this perspective. Article 30 of the law provides the possibility for the Spanish Data Protection Authority to influence the representative and take appropriate measures. In addition, in the event of a liability claim, the representative may also be jointly and severally liable to compensate for the damage together with the person liable for the claim. Of course, the power of enforcement against the representative does not imply a reduction of

[51] See Supra note 12, para 89

[52] See Sanso Rondon v LexisNexis Risk Solutions UK Ltd [2021] EWHC 1427 QB-2020-002788

[53] See Recital 80 of GDPR

the controller's or processor's liability, and the representative also has the right of recourse against the person responsible.[54]

The advantage of such a provision is that it increases the liability of the representative so that the representative will be more diligent in assisting the data protection authority and will also motivate the controller or processor behind to take the instructions of the data protection authority more seriously. After all, even if the EU cannot take enforcement measures directly against controllers and processors outside its borders, it can enforce them against representatives within its borders, which will have a deterrent effect. Moreover, enforcing against representatives will also provide partial remedies to the data subjects concerned and enhance the protection of the data subjects.[55]

It is clear that the current interpretation of the liability of representatives can pose a hidden problem for the implementation of the GDPR, and adjustments should be made to the interpretation of the liability of representatives.

In order to solve this problem, the representative's accountability can be strengthened by means of an agreement between the representative and its principal. When a controller or processor violates the GDPR, it is clearly contrary to the original design of the representative regime to have its representatives assume liability instead. However, at the same time, increasing the representative's accountability is essential for strengthening the effectiveness of the GDPR's extraterritorial enforcement. Therefore, it is possible to refer to the idea of the Spanish data protection law, which requires the representative to partially bear the liability for remedies and preserves the representative's right of recourse to the person who is really liable. The EDPB can provide a template for a liability share agreement. It requires the controller or processor to designate a representative with a co-signature by both parties to agree on the representative's share of the liability and to grant the representative a right of recourse afterward.[56] Such an agreement would not violate the design of the representative regime and would give EU data protection authorities a point of focus for enforcement against entities outside the EU. Data subjects would have more efficient access to remedies, and non-EU controllers and processors would place greater emphasis on GDPR compliance.

B) Ineffective implementation of representative regime

Another concern with the representative regime is its poor level of implementation. Kuner noted in his 2021 book that the representative regime appears to be ineffective. Although the representative regime requires businesses without an establishment in the EU to have a representative, in practice, "very few organizations or individuals provide services as representatives, and their reliability, experience, and solvency are often unclear."[57]

[54] See Organic Law 3/2018, of December 5, on Personal Data Protection and guarantee of digital rights, Art. 30

[55] See Kuner C and others, 'The EU General Data Protection Regulation (GDPR): A Commentary' (2020)

[56] Vander Maelen C, 'GDPR Codes of Conduct and Their (Extra)Territorial Features: A Tale of Two Systems' (2022) 12 International Data Privacy Law 297

[57] See Kuner C, 'Territorial Scope and Data Transfer Rules in the GDPR: Realising the EU's Ambition of Borderless Data Protection' [2021] SSRN Electronic Journal <https://www.ssrn.com/abstract=3827850> accessed 3 May 2024, P27

The implementation dilemma of the representation regime is justified. First, the cost of establishing a representative can be prohibitive for the entities concerned. Since the representative regime only applies to non-EU controllers and processors that do not have an establishment within the EU, the eligible entities tend to be under-sized multinational internet companies. This is due to the fact that large companies have usually set up establishments such as offices in EU member states long ago, referring to Google Inc. in the Case of Google Spain. Thanks to today's Internet developments, small and medium-sized multinational Internet companies are able to conduct business and make profits in the EU solely through online means. They do not need a natural person or organization to conduct business for them in the EU. If they were to set up a representative as required, that would certainly increase financial and labor costs, which are normally beyond their capacity.

Second, doubts about the effectiveness of the GDPR's extraterritorial enforcement also worsen the implementation dilemma of the representation regime. As analyzed above, due to the jurisdictional limitations of the GDPR, it is difficult for EU and Member State courts to ensure the effectiveness of enforcement against non-EU entities. In the absence of representation within the EU, it is also difficult for EU data protection authorities to access information about relevant controllers and processors, and even more difficult to build a liaison with them to enforce measures such as fines. As a result, even if the obligation to have a representative is not fulfilled, most non-EU entities are exempted from substantive penalties by reference to the reality of enforcement difficulties, which aggravates non-compliance with the representative regime.

This problem should be addressed by helping to reduce the cost of appointing representatives for non-EU companies, which could be done, for example, by guiding the commercialization of representative services and helping with representative training, thereby enhancing the professionalism of representatives and reducing the cost of appointing them.[58] As a result, the willingness of firms to appoint representatives would be strengthened. Furthermore, non-EU companies can also be forced to make representative designations by increasing penalties. EU data protection authorities could focus on investigating the presence of representatives of some of the larger international Internet companies in the EU and issue warnings and fines to those that do not. This would show non-EU processors and controllers that the EU takes the GDPR seriously and is committed to enforcing it, which would increase their awareness to designate representatives.

3.4 Conclusion

This chapter explores the conflicts and shortcomings of the GDPR's territorial scope, encompassing two aspects. The first one is the conflicts between the territorial scope and the data transfer rules. The GDPR's territorial scope and data transfer rules have raised concerns in practice, leading to confusion in their application due to their similar objectives and unclear interaction. The two sets of rules achieve their

[58] vantesson DJB, 'Extraterritoriality and Targeting in EU Data Privacy Law: The Weak Spot Undermining the Regulation' (2015) 5 International Data Privacy Law 226

objectives in different ways: the data transfer rules protect the transferred data through additional measures, and the territorial scope directly applies the GDPR to data processing outside of the EU, which confuses and burdens businesses with compliance process. The European Data Protection Board (EDPB) has issued guidance clarifying the conditions for the application of the two sets of rules and their interaction, and suggesting specific clauses to be added to data transfer tools to enhance protection. However, the guidance also raises new concerns, such as the possibility that companies may adjust their strategies to circumvent Chapter V provisions, resulting in a lower level of protection. To address these concerns, it is recommended that data transfers be redefined to broaden the scope of application and that the territorial scope and data transfer rules be merged to create a more complete body of rules.

The second one is the implementation dilemma of the representation regime. The GDPR's representation regime is based on Article 27 and applies to data controllers or processors that do not have an establishment in the EU but are involved in the provision of goods or services to, or the monitoring of the behavior of, EU data subjects. These entities should have a representative in the EU to deal with issues relating to data subjects and supervisory authorities and to ensure compliance. The representative system helps to strengthen the extraterritoriality of the GDPR and facilitates investigations and enforcement by supervisory authorities. However, the narrow scope of responsibility of the representatives makes it difficult for data subjects to obtain redress in case of a GDPR breach. It is recommended that the scope of responsibility of representatives be broadened to enhance their due diligence and compliance motivation. In addition, the implementation of the representative system has been ineffective, mainly due to the high cost of setting up representatives and the lack of effective representative services. This can be addressed by directing the commercialization of representation services, providing training and increasing penalties to motivate non-EU companies to pay more attention to representation set-up and GDPR compliance.

4 Implications of the extraterritorial application of GDPR on international trade

4.1 Introduction

As an EU regulation with vast extraterritorial application, the GDPR's international impact is enormous. Within this, its impact on international trade cannot be ignored. For third countries, the GDPR intends to bring data protection measures, while imposing non-negligible data protection obligations on non-EU businesses at the same time, creating trade barriers to a certain extent. US Commerce Secretary Wilbur Ross has made public statements that the implementation of the GDPR seriously interferes with transatlantic cooperation and creates unnecessary trade barriers that will affect every non-EU country.[59]

For the analysis of the impact of the extraterritorial application of GDPR on international trade, the General Agreement on Trade in Services (GATS) should be used as the basis for examination. Relying on the influence of the WTO, GAT is at present the most influential international agreement in the field of international trade in services. It applies in principle to all service sectors, including services related to data processing, [60] and is committed to ensuring that all participants receive fair and equitable treatment.

As a member of the WTO, the EU and all its member states are bound by GATS. Not only should they comply with the general obligations of GATS, but the EU has also made specific commitments in relation to the protection of personal data in relation to services such as Data Processing Services, Data Base Services, Other Computer Services, Communication Services, etc. For most of these services, the EU has committed no limitations on market access and national treatment for all modes of supply, except for the presence of natural persons.[61] In response to the EU's obligations and commitments in GATS, the EU is obliged to keep its trade measures from conflicting with GATS.

Thus, this chapter starts by analyzing whether the GDPR potentially violates the GATS, including the core obligations of the GATS such as Most Favored Nation treatment, and National Treatment, followed by an analysis of whether the GDPR constitutes a barrier to trade. Afterward, the chapter explores solutions from the perspective of both third countries and the EU.

[59] Wilbur Ross, 'EU data privacy laws are likely to create barriers to trade' *Financial Times* (30 May 2018)

[60] General Agreement on Trade in Services (GATS) 1869 U.N.T.S. 183; 33 I.L.M. 1167 (1994)

[61] See EU Schedule of Specific Commitments WTO doc GATS/SC/31 of 15 April 1994, s 1.II. B c), d) and e))

4.2 Does the GDPR potentially violate the GATS?

4.2.1 Analysis of the GDPR compliance with National Treatment of GATS

According to Article XVII, National Treatment requires Member to 'accord to services and service suppliers of any other Member, in respect of all measures affecting the supply of services, treatment no less favorable than that it accords to its own like services and service suppliers in the sectors inscribed in its Schedule.' This provision means that for relevant data services under the GDPR, the EU should not give less favorable treatment to services and service suppliers of other non-EU WTO members compared to the like services and service suppliers of the EU with respect to measures related. If a judgment is to be made on whether National Treatment is satisfied, the core elements are the likeness of services and service providers and less favorable treatment. Therefore, these two constitutive elements will be interpreted next and applied to analyze whether the GDPR and the regulations under it violate the National Treatment requirement.

A) Likeness

For the definition of 'like' under GATS, the text and case laws do not have a fixed interpretation, which at present can only be inferred from existing judgments. Reference could be made to the Panel report in the China Electronic Payments case. The Panel stated that 'like' should be interpreted in a dictionary sense, as "having the same characteristics or qualities as some other person or thing; of approximately identical shape, size, etc., with something else; similar". "Like" services are services that "are not necessarily identical and are essentially or substantially the same." The Panel also concluded from a contextual analysis of Article 17 that since Article 17 was intended to ensure equal opportunities for competition for like services of other members, "like services" could be inferred to be services in a competitive relationship.[62]

Moreover, in China - Publications and Audiovisual Products (WT/DS363/R), the Panel identified a specific criterion for determining "like services". The service can be considered "like services" if the origin of the service is the only factor in the differential treatment of domestic and foreign service suppliers by trade measures.[63]

B) No less favourable treatment

Article XVII.3 of GATS provides that if a member introduces treatment that alters the conditions of competition in favor of the member's supplier of services or services. Such treatment then constitutes less favorable treatment for suppliers of like services or services of other members.[64] This is a broad definition, which implies that any measure capable of changing the conditions of competition may be recognized as less favorable treatment. A more precise interpretation is clearly needed.

[62] China — Certain Measures Affecting Electronic Payment Services (DS413), Report of the Panel, 16 July 2012

[63] China — Measures Affecting Trading Rights and Distribution Services for Certain Publications and Audiovisual Entertainment Products (DS363), Report of the Panel, 12 August 2009, para. 7.975

[64] See GATS Article XVII.3

In Case Argentina — Financial Services (DS453), the Panel found that Argentina had complied with the disputed measure on the grounds that those measures were aimed at reaching the regulatory objective of " creating a fair competitive environment". However, the Appellate Body did not consider that a member's regulatory objectives could be used to justify the disputed measures. The Appellate Body held that the legal standard of 'no less favorable treatment' required ensuring equal conditions of competition, that is, equal opportunities for domestic and foreign services to compete in the market, rather than making domestic and foreign services 'equally competitive' through Argentine measures. The Appellate Body also reiterated that the National Treatment obligation requires Member States to refrain from disrupting or distorting existing market conditions and opportunities in favor of domestic services and service providers.[65]

To summarize, the key to defining less favorable treatment is that a member cannot adopt measures that make the competitive conditions of the market favorable for domestic services and service suppliers and that cannot be justified on the grounds that the member is trying to achieve its regulatory objectives. Next, it will be analyzed whether the representative regime of GDPR has the potential to give less favorable treatment to services and service suppliers from non-EU members, thus potentially violating GATS.

C) Analysis of Representative Regime

As discussed in the previous chapter, the representative regime applies to controllers and processors that do not have an establishment in the EU. They are required to designate representatives to perform functions such as keeping records of data processing, liaising, and assisting EU supervisory authorities within the EU.[66]

a) likeness

A likeness analysis of the representative regime reveals that the entities to which it applies may constitute like service suppliers with respect to the relevant service suppliers in the EU. Firstly, it needs to be determined whether the service suppliers in the EU and outside the EU are of a similar nature, meaning that they are essentially and generally the same. Although there is no way to identify a specific class of service suppliers in the absence of a corresponding WTO dispute, it is certain that many types of service suppliers exist both within and outside the EU. They are essentially and generally the same in terms of the types of services they provide and the way they provide them. Taking online music service providers as an example, there are online music platform companies that exist both inside and outside the EU and do business in the EU. The basic functions of these music platforms are similar, including providing online music streaming, searching, and other functions to users. They can be described as sharing essential and general likenesses.

Second, it needs to be determined whether the differential treatment given by the Representative regime to service suppliers in the EU versus those outside the EU is

[65] Argentina – Measures Relating to Trade in Goods and Services (DS453), Report of the Appellate Body, 14 April 2016, paras 6.138–6.147

[66] See Article 27 of GDPR

due solely to the different origins of the two. Given that controllers and processors within the EU have an establishment as defined under the GDPR, the representative regime applies only to non-EU controllers and processors, namely only to service providers from other members under GATS. It can be seen that the reason for applying the representative regime is due to the fact that these service suppliers are non-EU members, which means that they have different origins.

As a result of the above argumentation, it can be concluded that the non-EU service suppliers to which the representative regime applies have the like service suppliers within the EU.

b) Less favorable treatment

When it comes to the analysis of less favorable treatment under a representative system, the EU may indeed have given non-EU service providers less favorable treatment. This is because the competitive condition of the market has been changed to be more favorable for the like suppliers within the EU. The implementation of the representative regime requires non-EU service suppliers to spend additional financial and labor costs to establish a representative in the EU and to maintain this position for a sustained period of time. The costs for non-EU service suppliers to conduct business in the EU are therefore higher than before, which may lead to higher prices for their services and ultimately to a competitive disadvantage in the market. On the contrary, EU-based service suppliers do not need to add the cost of a representative, and the price of their services can remain unchanged, ultimately resulting in favorable conditions for competition in the market.

The above analysis leads to the conclusion that the representative system has the potential to violate the national treatment clause.

4.2.2 Analysis of the GDPR compliance with the Most Favored Nation treatment of GATS

As a general obligation, MFN treatment, unlike national treatment, is mandatory for members. Article II of GATS states the Most Favored Nation treatment, which regulates the Member to ‘accord immediately and unconditionally to services and service suppliers of any other Member treatment no less favorable than that it accords to like services and service suppliers of any other country’[67]. MFN focuses on whether the treatment is at the same level of favoritism as that received by different other members. MFN treatment is likewise a principle that operates in the context of like services and service providers. For the analysis of " likeness", it is possible to refer directly to the analysis of " likeness" in the context of national treatment above. MFN treatment also involves another interpretative factor "no less favorable treatment" for which reference should be made to the famous EC - Bananas III case. The Panel reported that "no less favorable treatment" should be interpreted as "no less favorable conditions of the competition"[68]. The Appellate Body report added

[67] See Article II of GATS

[68] European Communities — Regime for the Importation, Sale and Distribution of Bananas (DS27), Report of the Appellate Body, 9 September 1997

that "no less favorable treatment" should be interpreted as encompassing de facto and de jure discrimination.[69]

The analysis of whether the extraterritorial application of the GDPR may violate MFN can be exemplified by the adequacy decision. The adequacy decision originates from Article 45 of the GDPR, which applies to EU decisions on data transfers to non-EU countries. The European Commission assesses whether the third country or international organization provides an adequate level of data protection, which involves the consideration of a number of factors. This includes, for example, consideration of the third country's domestic legislation, i.e. how the third country reflects the rule of law, respect for human rights and fundamental freedoms in its domestic legislation, such as personal data protection rules. The EU expects third countries to have laws that give data subjects remedies for personal data protection and to establish independent supervisory authorities to ensure compliance with data protection regulations.[70]

While on a theoretical level, the GDPR sets the same standard for assessing adequacy to third countries or international organizations, in practice, adequacy decisions may imply discriminatory treatment. Both South Korea and the United States received adequacy decisions, but the processes they went through were very different. South Korea's adequacy decision began in 2015 and was followed by two rounds of adequacy decision negotiations with the EU, which failed due to the lack of independence of the South Korean data protection authority and the narrow scope of application of the Act on the Promotion of Information and Communication Network Utilization and Information Protection.[71] Although the EU determined South Korea did not have an adequate level of data protection, in fact, its domestic data protection law is said to be the strictest in the world. It has well-established rules with a wide scope of application and severe penalty rules. Those who break the law may be subject to criminal penalties, which may even include imprisonment.[72] In order to meet the EU's adequacy protection requirements, South Korea has put in a rather protracted effort to amend the relevant domestic laws. Eventually, after six years of effort, the European Commission adopted Korea's adequacy decision in 2021.

For the United States, the process may be much simpler. The beginning of EU's adequacy decision for the United States began in 1998, two years after the European Commission adopted the U.S. Safe Harbor framework. After the Safe Harbor agreement came into force, it was subject to numerous allegations that self-certified companies were not strictly adhering to the privacy protection principles and that the US government was not providing the oversight it should have, leaving the protection of EU data subjects compromised.[73] In 2015, the CJEU ruled that Safe Harbor was unable to satisfy the EU's data protection standards because of its inability to organize companies' leakage of personal data files to unauthorized

[69] See supra note 63

[70] See Article 45 of GDPR

[71] Dlight Law, 'Data Protection Law in South Korea'https://dlightlaw.com/en/data-protection-law-in-south-korea/ accessed 18 May 2024

[72] Ko H and others, 'Structure and Enforcement of Data Privacy Law in South Korea' (2017) 7 International Data Privacy Law

[73] Long WJ and Quek MP, 'Personal Data Privacy Protection in an Age of Globalization: The US-EU Safe Harbor Compromise' (2002) 9 Journal of European Public Policy 325

government agencies, making the Safe Harbor Agreement was ruled invalid. This happened all over again with the US-EU Privacy Shield agreement launched a year later. Just three years after the Privacy Shield was invalidated, the U.S. received a new adequacy decision for the EU-U.S. Data Privacy Framework (DPF). It is noteworthy that the European Parliament's consideration of the DPF in May 2021 found that it did not achieve "essential equivalence" in terms of the level of protection, and called on the Commission "not to adopt a new adequacy decision in relation to the United States unless meaningful reforms were introduced, in particular for national security and intelligence purposes"[74]. However, the adequacy decision was adopted by the European Commission only two months later.

Comparing Korea's process of obtaining a sufficiency determination with that of the United States, Korea appears to have been treated less favorably, both in terms of the length of time and data protection requirements, which potentially violates MFN treatment. The reasons for this differential treatment can also be clearly explained on an economic level. The United States is the EU's largest trading partner and has maintained an active and deep cooperative relationship for many years.[75]

4.3 The potential for extraterritorial application of the GDPR causing trade barriers

While the implementation of the GDPR has raised the standard of data protection for EU data subjects, it also comes with complex data protection rules and a high level of protective measures. For many non-EU countries, it has created new types of trade barriers in practice. This section will analyze separately the social, regulatory, and technical barriers to trade that the application of the GDPR will bring to non-EU countries.

4.3.1 Social barrier to trade

Social barriers to trade usually refer to trade protection measures on the grounds of protecting workers' rights and interests, such as the most famous SA8000 standard. Similar international conventions contain provisions that require workers to be provided with appropriate labor protection, labor environment, etc. While their intentions are positive, such standards are usually initiated by more developed countries and are based on their higher standards of domestic human rights protection. For developing countries, where human rights protection is not yet well developed, it undoubtedly sets an obstacle for market access and international trade development, weakening the advantage of developing countries that originally developed foreign trade through low labor prices.

Similar social barriers to trade can be seen in the GDPR. Unlike many developing countries, the EU has established the right to data protection as a constitutional right.

[74] Council pursuant to Regulation (EU) 2016/679 o on the adequate level of protection of personal data under the EU-US Data Privacy Framework [2023]

[75] European Union, 'EU trade relations with the United States' (2023) https://policy.trade.ec.europa.eu/eu-trade-relationships-country-and-region/countries-and-regions/united-states_en#:~:text=Although%20overtaken%20by%20China%20in,artery%20of%20the%20world%20economy accessed 6 May 2024

Through Article 8 of the Charter of Fundamental Rights of the European Union, the protection of personal data was established. After the entry into force of the Lisbon Treaty, the right to personal data protection is recognized as a constitutional right in the EU. It is further reflected in the practical aspects of the GDPR, which grants individuals the right to access, consent, revocation of consent, deletion, and correction of their data. Data subjects also have the right to bring a case to court when they believe their rights have been violated. In this way, the GDPR demonstrates a high standard of protection of the rights of individuals with regard to personal data protection.

However, for developing countries, their societies originally have a lower level of awareness of personal data protection, and their data protection measures are relatively imperfect. Trying to apply high standards of data protection measures, like the GDPR, to such a level of social awareness is an obstacle in itself. Relevant companies in developing countries need to pay more private costs to protect personal data, offsetting the gap in personal data protection between different national levels of social development. Furthermore, the EU can also recognize some such companies as unsuitable for data transfer through the relevant provisions of the GDPR, or penalize them, which will adversely affect the development of relevant companies from developing countries in the EU and act as a trade barrier.

An article from an Indian academic demonstrates the existence of social barriers to trade. Since India just passed the Digital Personal Data Protection Act in 2023, its level of data protection is overall low and most Indian companies are unfamiliar with data protection requirements. Their knowledge has a greater gap with the strict protection level of GDPR and therefore requires higher costs than European countries to meet GDPR compliance requirements. Due to the GDPR's requirement to have a data protection officer, some Indian companies may spend more than €10 million on hiring a data protection officer and purchasing legal consulting services.[76]

4.3.2 Regulatory barrier to trade

Regulatory barriers to trade mean impeding international trade through the imposition of strict regulatory measures. The consequences of regulatory barriers to trade can be explored through the OECD's Restrictions to Trade in Digital Services Index. The index presents “cross-cutting barriers that impede or completely prohibit the ability of businesses to use electronic networks to provide services”[77]. In the 2020 data for EU countries, the number one measure causing restrictions on trade in data is restrictions on cross-border transfers of data, which shows how restrictive the GDPR's strict data transfer rules are for trade in data services.[78]

Not only the data transfer rules but also other rules of the GDPR can cause potential regulatory barriers to trade. The GDPR has ten chapters, which contain a wide range

[76] Omkar Sathe, ‘EU-India FTA: GDPR’s trade barrier needs to be dealt with’ (2024) https://www.orfonline.org/expert-speak/eu-india-fta-gdpr-s-trade-barrier-needs-to-be-dealt-with accessed 20 May 2024

[77] OECD, ‘OECD Digital Services Trade Restrictiveness Index’ (2022) https://goingdigital.oecd.org/en/indicator/73 accessed 20 May 2024

[78] Ibid

of rules, including principal rules, enforcement rules, and penalty rules. Many of the rules are the world's foremost in the degree of protection and have a strong degree of innovation. After the entry into force of the GDPR, the EDPB has issued more than twenty Guidelines to further illustrate the application of the relevant rules. For some ambiguous rules, it is even necessary to determine how to apply them through the judgment of the Court of Justice of the European Union (CJEU). These rules are complex and require in-depth study and understanding. For example, the GDPR sets out six different conditions for the legal processing of personal data alone. Such a large number of legal documents makes it necessary for processors and controllers to learn precisely how to apply them in order to make data processing lawful, thus increasing compliance and administrative burdens for enterprises. There are also some conflicting and confusing points in the GDPR, such as the conflict between territorial scope and data transfer rules mentioned in Chapter 2, which makes enterprises feel confused and need to spend more human resources to learn and change the internal structure of the company to apply them. In addition, after absorbing the GDPR, some EU countries have introduced new data protection acts that differ from the GDPR and may impose stricter controls, which further increases the compliance burden on businesses. A survey of small and medium-sized businesses by International Data Corporation in 2016 revealed that 78 percent of more than 700 companies were either unaware of the GDPR's impact on their company or completely unaware of it.[79]

4.3.3 Technical barrier to trade

Technical barriers to trade (TBT) usually refer to technical requirements through regulations, such as technical standards, tests, qualification procedures, etc., that create unnecessary obstacles to international trade. Looking at the GDPR, it can be seen that it contains technical requirements that could also be potential technical barriers to trade. For example, the GDPR has detailed technical codes of practice and standards for the storage of personal data. According to Articles 7 and 30, after acquiring personal data, data controllers are required to create records containing the personal information of the controller and related persons; the purpose of data processing provided to the data subject; the classification of the data subject and their data; the information about the recipients that may be disclosed to the data, including recipients in third countries; the expected timeframes for deletion of the data; technical and organizational security measures; and data processing records that contain detailed information about the data subjects. [80]

To meet such compliance requirements, companies not only need to allocate more human resources to the relevant operations but also need to enhance the technical level of data protection, such as establishing compliant databases and developing technical tools for compliance operations. As a result, technical barriers to trade are created. While this may not be a big deal for large companies that already have a high level of compliance technology, small and medium-sized companies will have

[79] ESET, 'IDC Survey for ESET: Businesses Confused about EU's Data Privacy Regulation; Encryption Desired by Over One Third of the Companies'(2016) https://www.eset.com/za/about/newsroom/press-releases-za/products/idc-survey-for-eset-businesses-confused-about-eus-data-privacy-regulation-encryption-desired-by-o/ accessed 18 May 2024

[80] See Articles 7 and 30 of GDPR

to pay a high cost of technical development and application in order to meet the GDPR compliance requirements. For example, a U.S.-based company Uber Entertainment completely shut down one of its most popular games because it could not afford the high cost of upgrading the platform to GDPR compliance requirements.[81]

4.4 Possible measures to be taken by third countries to reduce trade barrier

4.4.1 Applying for Adequacy decision

Third countries that want to minimize the trade barriers resulting from the extraterritorial application of the GDPR, can take the measure of applying to the EU to obtain an adequacy decision. Although the previous paragraphs have already described the possibility that an adequacy decision can take a long time for a country, it is still the most effective way to help non-EU countries get rid of data transfer restrictions under the current GDPR framework. If an adequacy decision is passed, personal data within the EEA can flow directly to third countries without any further constraints or authorizations, such as Standard Contractual Clauses or Binding Corporate Rules.[82] It will significantly help abroad businesses in that country to reduce their compliance burden and compliance risks, thus helping them to expand and flourish in the EU.

On July 10, 2023, the Adequacy Decision on the EU-U.S. Data Privacy Framework (DPF) was approved for adoption by the European Commission. This means that after the successive failures of the U.S.-EU Safe Harbor Framework and the EU-US Privacy Shield, which were invalidated by the CJEU, the U.S. has been given a new opportunity to help EU-US data transfers. Building on the foundation of the EU-US Privacy Shield, many of the U.S. organizations that have participated in the program can participate in the DPF more simply by updating references to the EU-U.S. Data Privacy Framework Principles in their privacy policies within three months and re-certifying annually in order to remain in the framework.[83] For certified organizations, data transfers to and from the EU will become easier and compliance costs will be reduced.[84]

Within the contents of the DPF, there are several provisions that contribute well to the level of protection of EU data in the United States, which are highly worthwhile for other countries that have not yet received adequacy decisions to refer to. One of the highlights is the strengthened oversight of surveillance of data by U.S. intelligence services. Since Schrems II, the EU has been particularly concerned about the surveillance of EU personal data by third-country government agencies, based

[81] Layton R, 'The 10 Problems of the GDPR' (2019)

[82] Council pursuant to Regulation (EU) 2016/679 on the adequate level of protection of personal data under the EU-US Data Privacy Framework [2023]

[83] Ibid

[84] Data Privacy Framework Program, 'Benefits of the Data Privacy Framework (DPF) Program' (2023) https://www.dataprivacyframework.gov/program-articles/Benefits-of-the-Data-Privacy-Framework-(DPF)-Program accessed 20May 2024

on the national laws of that country. To reach the aim, the United States adopted an Executive Order on "Enhancing Safeguards for United States Signals Intelligence Activities", which keeps the data surveillance activities of the U.S. intelligence services within necessary and proportionate boundaries. It also provides oversight and remedies, which creates a whole new remedial mechanism providing individual access to complaints with a fair and impartial review.[85]

4.4.2 Enhancing domestic data protection level

The fundamental reason why the adequacy decision of the United States can be reached is that the country itself has a comparatively good level of data protection and measures. Therefore, for those third countries that are not yet able to meet the requirements of the adequacy decision, they can strengthen their own data protection level in the following aspects to increase the possibility of meeting the requirements. Firstly, in terms of domestic legislation, the laws can be revised with reference to the relevant elements of Directive 95/46/EC and GDPR, such as adding provisions on data deletion, granting the data subject the right to access and correct the data, and requiring enterprises to set up a data protection officer, etc. Through the improvement of the domestic data protection law, the data protection level of legislation will gradually approach GDPR, as strong proof of having an adequate level of data protection.

Secondly, an independent data protection authority can be established to enhance the remedy of personal data. Each country in the EU has an independent data protection authority responsible for guaranteeing the enforcement of data protection laws. Data subjects can also make direct complaints through these agencies to get remedies in a convenient way. In addition, Japan, as a country that has received an EU adequacy decision, has also established a Personal Data Protection Commission that can independently exercise the functions of supervising law enforcement, handling complaints, and formulating regulations.[86] It can be seen that having an independent data protection authority is very highly valued by the EU.

4.4.3 Promoting data protection standards consistent with national interests

Some third countries do not recognize the level of data protection in the EU, which they consider to be too excessive and to be an obstacle to business development. Instead, they prefer to implement data protection levels and rules that are favorable to their national interests, through regional agreements and free trade agreements. Take the United States as an example, unlike the EU, the United States has a more relaxed protection of personal data, it has not established the right to personal data as a basic human right, and it does not have an independent data protection agency. Such a model is more conducive to the free development of U.S. Internet enterprises, which is more in line with the economic interests of the United States. In order to promote a data protection framework that meets U.S. interests, the U.S. promoted

[85] See Supra note 77

[86] DLA Piper Intelligence, 'National Data Protection Authority' (2024) <https://www.dlapiperdataprotection.com/index.html?t=authority&c=JP> accessed 18 May 2024

APEC's adoption of the APEC Privacy Framework, which is less restrictive of data protection than the EU's data protection laws. Instead of restricting cross-border data flows with measures, it promotes cross-border flows of data through harmonized rules with the intention of promoting e-commerce in the Asia-Pacific region. APEC has also introduced cross-border privacy rules to help companies become certified, which allows them to transfer data unhindered with other certified companies. This institutional design has helped the United States to enforce its data protection will within APEC member countries and to expand the reach of the U.S. data protection regime.

The same purpose is reflected in the U.S. Free Trade Agreement with South Korea. The e-commerce chapter of the U.S.-Korea FTA requires that "each Party shall, to the extent possible, refrain from imposing or maintaining unnecessary barriers to the cross-border flow of electronic information."[87] In the financial services chapter, there is also a provision stating that "the Parties shall authorize the financial institutions of the other Party to transmit information and conduct cross-border data processing, electronically or otherwise, for the purposes of their normal business activities."[88] Such provisions on cross-border data flows also demonstrate a low level of data protection. Thus, the United States intends to influence global trends in data protection by leading the way in establishing a data protection framework that meets its national interests.

4.5 Possible measures to be taken by the EU to reduce trade barrier

In the face of the negative impact on international trade arising from the extraterritorial application of the GDPR, the EU can make improvements in two ways. Firstly, from the legislative level, the EU can give more explanations and guidelines on the extraterritorial application. For the complex issue of extraterritorial application, the EU's current guidance is obviously not sufficient, there are still gaps in the interpretation of many key concepts, and there are also confusing areas for the specific operation of non-EU companies. Therefore, the EU and the EDPB could issue more detailed and operational guidelines to help non-EU entities understand more easily and thus reduce the compliance burden.

Second, the EU could propose asymmetric enforcement. Such an enforcement approach uses the market power of different entities as an indicator of enforcement, with stricter enforcement standards for dominant firms. If a data protection crisis occurs in a dominant enterprise, it involves more data subjects and the extent of harm is greater, compared to a non-dominant enterprise. Moreover, dominant firms typically have more capital to build data protection systems, and it is easier for them to comply with the GDPR than for non-dominant firms. Therefore, such asymmetric

[87] See U.S.-Korea Trade Agreement 2007, Article 15.8
[88] Ibid

enforcement is more sensible and less likely to have a negative impact on fair competition in the market.[89]

4.6 Conclusion

The GDPR has had a significant impact on international trade. For third countries, the GDPR is intended to introduce data protection measures, but at the same time imposes significant obligations on non-EU businesses, creating a barrier to trade of sorts.

This chapter analyses the GDPR in terms of whether it potentially violates the GATS, focusing on national treatment and most-favored-nation (MFN) treatment, and whether the GDPR constitutes a barrier to trade. National Treatment requires that Members do not treat suppliers of services and services from other Members less favorably than like services and suppliers from their own country. By analyzing the differential treatment of non-EU service suppliers and internal EU suppliers under the representative regime, it can be seen that the regime may result in non-EU suppliers being at a competitive disadvantage and thus violating the National Treatment provision. In the context of MFN treatment, GDPR adequacy decisions have been found to be potentially discriminatory. MFN treatment requires that services and service suppliers of one Member should be given immediate and unconditional treatment no less favorable than that given to other Members. For example, the difference in treatment between South Korea and the United States in the process of obtaining an adequacy decision shows a potential MFN violation.

The chapter also analyses the social, regulatory, and technical dimensions of trade barriers created by the GDPR. For third countries, possible countermeasures include applying for a adequacy sufficiency decision, upgrading the level of domestic data protection, and promoting data protection standards in the national interest. For the EU, possible measures include the adoption of more interpretations and guidelines at the legislative level and the implementation of asymmetric enforcement.

[89] Graef I and Van Berlo S, 'Towards Smarter Regulation in the Areas of Competition, Data Protection and Consumer Law: Why Greater Power Should Come with Greater Responsibility' (2021) 12 European Journal of Risk Regulation 674

5 Conclusion

In order to strengthen the protection of personal data of EU data subjects, the GDPR came into force in 2018. it is not just a law for the EU, but extends its application to a wide range of non-EU data processing. the GDPR's territorial scope provisions, which stem from Article 3, create establishment criteria and locational standards that can regulate the processing of data by entities outside of the EU. Such extensive extraterritorial application has significantly increased the level of data protection, but it has also given rise to a number of controversies and concerns.

The paper begins by exploring in detail the conditions for the application of Article 3 of the GDPR, focusing on two key criteria: the establishment criterion and the targeting criterion. Before elaborating on these criteria, the definitions of data controller and data processor are introduced. Using case law and the EDPB's relevant guidelines, the paper discusses the criteria for determining establishment in the EU and the specific meaning of "In the context of the activities of an establishment". Next, it interprets the targeting criteria of Article 3 of the GDPR and focuses on the offering of goods or services to EU data subjects and the monitoring of their behavior. It is followed by an assessment of the GDPR's territorial scope. While it enhances the protections of the GDPR, there is also legal application uncertainty, which poses a compliance burden for businesses and challenges to practicing the GDPR.

The paper then provides an in-depth analysis of the problems and conflicts in the scope of the territorial application of the GDPR. Despite the relative completeness of the GDPR's provisions and guidelines, there are still situations that confuse non-EU entities in its interpretation and practical application. In particular, the territorial scope and data transfer rules, which have similar objectives but unclear interactions, have led to conflicting applications. The data transfer rules protect data transfers by taking additional measures, while the territorial scope directly applies the GDPR to data processing outside the EU, which confuses and burdens businesses in their approach to compliance. To address these issues, it is recommended that data transfers be redefined, the scope of the application be broadened, and the territorial scope and data transfer rules be merged to create a more comprehensive system of rules. Meanwhile, the ineffective implementation of the representation system is mainly due to the high cost of setting up representatives and the lack of effective representation services. To address this issue, non-EU companies can be induced to pay more attention to representative set-up and GDPR compliance by guiding the commercialization of representative services, providing training, and increasing penalties.

Finally, the paper focuses on analyzing the impact of the extraterritorial application of the GDPR on international trade and proposes countermeasures. GDPR, as an EU regulation with broad extraterritorial application, imposes non-negligible data protection obligations on non-EU firms, leading to a certain degree of trade barriers, while protecting data privacy. Using GATS as a basis for analysis, the possibility of whether the GDPR potentially violates GATS is explored, particularly with respect

to National Treatment and Most Favoured Nation treatment. The analysis finds that the GDPR representation regime may create unfavorable competitive conditions for non-EU suppliers, potentially violating the national treatment provisions; meanwhile, there are potential MFN violations of the GDPR adequacy decisions, such as the difference in treatment between South Korea and the United States with respect to the adequacy decisions. In addition, social, regulatory, and technical level barriers to trade arising from the GDPR are identified, and third-country and EU countermeasures are proposed. Response measures for third countries include applying for adequacy decisions, upgrading the level of domestic data protection, and promoting data protection standards in line with national interests. For the EU, it is suggested that the negative impact of the GDPR on international trade can be mitigated through the development of additional interpretations and guidelines and the implementation of asymmetric enforcement.

References

Official documents

European Union

Council Regulation (EU) 2016/679 of the of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L119/1

Council Directive 95/46/EC of the 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 [1995] OJ L281/31

Chapter of Fundamental Rights of European Union [2012] OJ C326/391

Council Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament [2011] OJ L304/64

Council Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services [2015] OJ L241/1

Council pursuant to Regulation (EU) 2016/679 o on the adequate level of protection of personal data under the EU-US Data Privacy Framework [2023]

Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR, European Data Protection Board, 2021

Guidelines 3/2018 on the territorial scope of the GDPR (Article 3), European Data Protection Board, 2018

World Trade Organization

General Agreement on Trade in Services (GATS) 1869 U.N.T.S. 183; 33 I.L.M. 1167 (1994)

General Agreement on Tariffs and Trade (1994) 1867 U.N.T.S. 187; 33 I.L.M. 1153 (1994)

European Communities and their Member States - Schedule of Specific Commitments GATS/SC/31 (1994)

South Korea

Personal Information Protection Act 2023

U.S.-Korea Trade Agreement 2007

Spain

Organic Law 3/2018, of December 5, on Personal Data Protection and guarantee of digital rights

Case law

Court of Justice of the European Union

Case C-131/12 Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González [2014] ECR 317

Case C-230/14 Weltimmo s.r.o. v Nemzeti Adatvédelmi és Információszabadság Hatóság [2015] ECR 639

Case C-311/18 Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems [2020] ECR 559

Case C-585/08 Peter Pammer v Reederei Karl Schlüter GmbH & Co. KG [2010] ECR 273

World Trade Organization

Argentina – Measures Relating to Trade in Goods and Services (DS453), Report of the Appellate Body, 14 April 2016

China — Certain Measures Affecting Electronic Payment Services (DS413), Report of the Panel, 16 July 2012

China — Measures Affecting Trading Rights and Distribution Services for Certain Publications and Audiovisual Entertainment Products (DS363), Report of the Panel, 12 August 2009

European Communities — Regime for the Importation, Sale and Distribution of Bananas (DS27), Report of the Appellate Body, 9 September 1997

The High Court of England and Wales

Sanso Rondon v LexisNexis Risk Solutions UK Ltd [2021] EWHC 1427 QB-2020-002788

Literature

Articles

Article 29 Data Protection Working Party, ‘Update of Opinion 8/2010 on applicable law in light of the CJEU judgement in Google Spain’ [2016]

Article 29 Data Protection Working Party, ‘Opinion 1/2010 on the concepts of "controller" and "processor"’ [2010]

Bauer M and Lee-Makiyama H, ‘The Costs of Data Localisation: Friendly Fire on Economic Recovery’ [2014] ECIPE occasional paper

Greer D, ‘Safe Harbor--a Framework That Works’ (2011) 1 International Data Privacy Law 143

Graef I and Van Berlo S, ‘Towards Smarter Regulation in the Areas of Competition, Data Protection and Consumer Law: Why Greater Power Should Come with Greater Responsibility’ (2021) 12 European Journal of Risk Regulation 674

Ko H and others, ‘Structure and Enforcement of Data Privacy Law in South Korea’ (2017) 7 International Data Privacy Law

Kuner C, ‘Territorial Scope and Data Transfer Rules in the GDPR: Realising the EU’s Ambition of Borderless Data Protection’ [2021] SSRN Electronic Journal <https://www.ssrn.com/abstract=3827850> accessed 3 May 2024

Kuner C, ‘Protecting EU Data Outside EU Borders under the GDPR’ (2023) 60 Common Market Law Review 77

Kuner C, ‘Exploring the Awkward Secret of Data Transfer Regulation: the EDPB Guidelines on Article 3 and Chapter V GDPR’ (2021) <https://europeanlawblog.eu/2021/12/13/exploring-the-awkward-secret-of-data-transfer-regulation-the-edpb-guidelines-on-article-3-and-chapter-v-gdpr/> accessed 30 April 2024

Kuner C and others, ‘The EU General Data Protection Regulation (GDPR): A Commentary’ (2020)

Layton R, ‘The 10 Problems of the GDPR’ (2019)

Long WJ and Quek MP, ‘Personal Data Privacy Protection in an Age of Globalization: The US-EU Safe Harbor Compromise’ (2002) 9 Journal of European Public Policy 325

Meddin E, ‘The Cost of Ensuring Privacy: How the General Data Protection Regulation Acts as a Barrier to Trade in Violation of Articles XVI and XVII of the General Agreement on Trade in Services’ (2020) 35 American University International Law Review 997

Muller G, ‘National Treatment and the GATS: Lessons from Jurisprudence’ (2016) 50 Journal of World Trade 819

Reyes C, ‘WTO-Compliant Protection of Fundamental Rights: Lessons from the EU Privacy Directive’ [2011] Melbourne Journal of International Law 141

Svantesson DJB, ‘Extraterritoriality and Targeting in EU Data Privacy Law: The Weak Spot Undermining the Regulation’ (2015) 5 International Data Privacy Law 226

Taylor M, Transatlantic Jurisdictional Conflicts in Data Protection Law: Fundamental Rights, Privacy and Extraterritoriality (1st edn, Cambridge University Press 2023) <https://www.cambridge.org/core/product/identifier/9781108784818/type/book> accessed 24 May 2024

Teksten RD, ‘A Comparative Analysis of GATS and GATT: A Trade in Services Departure from GATT’s MFN Principle and the Affect on National Treatment and Market Access’ [2000] SSRN Electronic Journal <http://www.ssrn.com/abstract=1664584> accessed 2 May 2024

Vander Maelen C, ‘GDPR Codes of Conduct and Their (Extra)Territorial Features: A Tale of Two Systems’ (2022) 12 International Data Privacy Law 297

Weiler JHH and others, ‘Unit V: The Most-Favored Nation (MFN) Principle’, The Law of World Trade Organization (2017)

Willemyns I, 'The Gats (in)Consistency of Barriers to Digital Services Trade' (2018)

Yakovleva S and Irion K, 'The Best of Both Worlds? Free Trade in Services and EU Law on Privacy and Data Protection' (2016) 2 European Data Protection Law Review 191

Yakovleva S, 'GDPR Transfer Rules vs Rules on Territorial Scope: A Critical Reflection on Recent EDPB Guidelines from both EU and International Trade Law Perspectives' (2021) <https://europeanlawblog.eu/2021/12/09/gdpr-transfer-rules-vs-rules-on-territorial-scope-a-critical-reflection-on-recent-edpb-guidelines-from-both-eu-and-international-trade-law-perspectives/> accessed 30 April 2024

Newspaper Articles

Wilbur Ross, 'EU data privacy laws are likely to create barriers to trade' Financial Times (30 May 2018)

Websites

Dlight Law, 'Data Protection Law in South Korea'<https://dlightlaw.com/en/data-protection-law-in-south-korea/> accessed 18 May 2024

European Union, 'EU trade relations with the United States' (2023) https://policy.trade.ec.europa.eu/eu-trade-relationships-country-and-region/countries-and-regions/united-states_en#:~:text=Although%20overtaken%20by%20China%20in,artery%20of%20the%20world%20economy accessed 6 May 2024

Omkar Sathe, 'EU-India FTA: GDPR's trade barrier needs to be dealt with' (2024) <https://www.orfonline.org/expert-speak/eu-india-fta-gdpr-s-trade-barrier-needs-to-be-dealt-with accessed> 20 May 2024

OECD, 'OECD Digital Services Trade Restrictiveness Index' (2022) <https://goingdigital.oecd.org/en/indicator/73> accessed 20 May 2024

ESET, 'IDC Survey for ESET: Businesses Confused about EU's Data Privacy Regulation; Encryption Desired by Over One Third of the Companies' (2016) <https://www.eset.com/za/about/newsroom/press-releases-za/products/idc-survey-for-eset-businesses-confused-about-eus-data-privacy-regulation-encryption-desired-by-o/> accessed 18 May 2024

Data Privacy Framework Program, 'Benefits of the Data Privacy Framework (DPF) Program' (2023) <https://www.dataprivacyframework.gov/program-articles/Benefits-of-the-Data-Privacy-Framework-(DPF)-Program> accessed 20 May 2024

DLA Piper Intelligence, 'National Data Protection Authority' (2024) <https://www.dlapiperdataprotection.com/index.html?t=authority&c=JP> accessed 18 May 2024