# AMERICAN UNIVERSITY OF ARMENIA

## COLLEGE OF HUMANITIES & SOCIAL SCIENCES

**LL.M. Program**

TITLE

# "THE ANALYSIS OF THE ESTABLISHMENT OF THE GENERAL DATA PROTECTION REGULATION AND THE AFTERMATH OF THE EXPANSION OF THE EXTRATERRITORIAL SCOPE FOR NON-EU COUNTRIES"


STUDENT'S NAME

**ANDREA ARINA KAJAKDJIAN**

SUPERVISOR'S NAME

**PROF. LILIT BANDURYAN**


NUMBER OF WORDS

**10533**




40 Marshal Baghramyan Avenue

Tel: (37410) 51 27 55

0019, Yerevan, Armenia

law@aua.am


Tel: (37410) 51 27 55

## Acknowledgments

*I have received a great deal of support and assistance throughout the writing of this Thesis Paper. I would like to thank my Supervisor, Ms. Banduryan, for her expertise, assistance and guidance throughout the process of writing my thesis.*

*I would also like to thank the LL.M Department, for giving us the freedom to explore topics of our own interests for this paper, as well as my sincere gratitude to them and the exceptional faculty, that has taught me so much during the past 2 years.*

*Last of all, I would like to thank my family and friends, for being patient and sympathetic, as well as providing happy distractions throughout this stressful process. Your encouragement and support is what got me here today.*



**40 Marshal Baghramyan Avenue**

**Tel: (37410) 51 27 55**

**Tel: (37410) 51 27 55**

**0019, Yerevan, Armenia**

**law@aua.am**

# Contents






40 Marshal Baghramyan Avenue

Tel: (37410) 51 27 55

0019, Yerevan, Armenia

law@aua.am


Tel: (37410) 51 27 55

## LIST OF ABBREVIATIONS

| | |
|---|---|
| GDPR | General Data Protection Regulation |
| DPD | Data Protection Directive |
| CJEU | Court of Justice of the European Union |
| OECD | Organization for Economic Co-operation and Development |
| ECHR | European Convention on Human Rights |



40 Marshal Baghramyan Avenue
0019, Yerevan, Armenia
Tel: (37410) 51 27 55
Tel: (37410) 51 27 55
law@aua.am

## Introduction

In May 2018, the new European Union data protection law took effect, known as the General Data Protection Regulation (Hereinafter the "GDPR").[1] The GDPR builds on many existing concepts of European Data Protection legislations and creates new rights for users whose data are processed.[2] As a regulation, it is directly applicable to all of the member states of the European Union without any legislative measures at national level. The result is new responsibilities to comply with data handling organizations. The Regulation addresses two main ideas: strengthening and unifying data privacy rules for individuals in the European Union; and extending data protection territorial scope by regulating the export of European citizens' personal data outside the EU.

While some analysts claim that, the general privacy policies of different websites, mobile applications and operating systems are also similar across borders due to the diffusive and universal nature of the Internet,[3] at the same time, apart from a few international and regional legal instruments, laws on data protection are largely determined by national parliaments and could therefore differ.

The GDPR is the ''modernized'' and upgraded version of the Data Protection Directive (Hereinafter the ''DPD''), whose provisions were defined to protect EU residents' personal data prescribing the limits of EU-based controllers' activities, however, with the expansion of the Internet, transnational data flow has become unavoidable.[4] While the DPD discussed the transfer of data from the EU to third countries, there were some limitations when it came to its extraterritorial application as well as the liability for damages. However, nowadays, when there

[1] Regulation (EU) 2016/679 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 2016, OJ L119/1.

[2] Hintze, M. (2017). *Viewing the GDPR through a De-Identification Lens: A Tool for Clarification and Compliance.*
[3] Anabela Susana De Sousa Gonçalves, '*The Extraterritorial Application of the EU Directive on Data Protection'* Spanish Yearbook of International Law (2015) 195.
[4] Shakila Bu-Pasha (2017*) Cross-border issues under EU data protection law with regards to personal data protection*, Information & Communications Technology Law, 26:3, 213-228,DOI: 10.1080/13600834.2017.1330740



40 Marshal Baghramyan Avenue Tel: (37410) 51 27 55

Tel: (37410) 51 27 55

0019, Yerevan, Armenia law@aua.am

is any connection with the EU, the GDPR[5] attempts to govern both actors with some improved obligations.

The main shift that happened from the Directive to the Regulation is that regulations are passed by both the EU Council and European Parliament, or by the Commission alone. As soon as they pass, they become the most direct form of EU law since they have a binding legal force on Member States with a similar effect as national laws. National governments do not need to take any actions themselves to implement EU regulations. As Article 288 of the Treaty on the Functioning of the European Union defines a regulation as "Article 288 (example Article 249 TEC): ''[…] a regulation shall have general application. It shall be binding in its entirety and directly applicable in all Member States. [. . . ]". However, there are some exceptions to this, as Article 85 of the GDPR suggests that '' Member States shall by law reconcile the right to the protection of personal data pursuant to this Regulation with the right to freedom of expression and information, including processing for journalistic purposes and the purposes of academic, artistic or literary expression.''

While there is already much written on the GDPR's impact on the European Union, not much has been discussed clearly on the territorial aspect of the Regulation. Most of the available sources are very scientific and specific to the IT jargon, which makes it difficult for others to understand where they fall under the regulation. This paper aims to analyze the impact of the GDPR extraterritorial application from the perspective of Non-EU companies in a clearer way.

The GDPR became part of the solution to bring awareness for the importance of data privacy on an international scale and fight against data exploitation.[6] Its extraterritorial application was further settled after the European Court of Justice ordered a company called *Wirtschaftsakademie Schleswig-Holstein* to deactivate its fan page on Facebook, on grounds that neither the company nor Facebook was giving notice to their users that their personal data was being collected.[7] This

[5] The General Data Protection Regulation 2016/679.
[6] General Data Protection Regulation (GDPR), Privacy International, <https://privacyinternational.org/topics/general-data-protection-regulation-gdpr.>
[7] Case C-210/16. Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH-.



40 Marshal Baghramyan Avenue Tel: (37410) 51 27 55

Tel: (37410) 51 27 55

0019, Yerevan, Armenia law@aua.am

is fundamental to change the relationship of Social Media platforms such as Facebook with their customers and bring international awareness to the extraterritorial application of the GDPR. Same with the case of Cambridge Analytica, the ICO confirmed a maximum financial penalty for Facebook, which clearly affirms that the GDPR is a regulatory change that will have an impact far beyond the arena of technology.[8]

Because the extraterritorial application tackles a wide range of potential scenarios, the study will analyze the direct extraterritorial application of the GDPR as the offering of goods or services as well as the monitoring of their behavior as far as the behavior takes place in the Union.[9] There is however also situations where the GDPR creates indirect obligations to comply for non-EU organizations carrying out business with EU organizations. In order to perform an analytical study, this paper will be based on several methodology approaches:

- A Theoretical Research – to explore and analyze the works of scholars, academic papers of practicing professionals, and
- A Descriptive Breakdown – to assess the relevant articles of the GDPR.

In light of these factors, this study will be divided into several parts. First, we will define the scope of Article 4 of the DPD as well as the early case law that shaped the territoriality scope of the GDPR. After which we will explore the direct extraterritorial application of the GDPR under art.3 as a provider of goods and services and as a processor and monitor of behavior. We will identify the rules and conflicts of International Law governing extraterritorial jurisdiction claims, the limited scope of International Customs and General Principles of law concerning them, and finally, discuss the direct and indirect enforcement of the Regulation for non-EU members, followed by a Conclusion to summarize the main findings of the study.

[8] What Are the GDPR Implications in Light of Facebook's Cambridge Analytica Fine?, Lawyer Monthly (2018), <https://www.lawyer-monthly.com/2018/10/what-are-the-gdpr-implications-in-light-of-facebooks-cambridge-analytica-fine/>

[9] GDPR, Article 3(2) <https://gdpr-info.eu/art-3-gdpr/>



40 Marshal Baghramyan Avenue Tel: (37410) 51 27 55

Tel: (37410) 51 27 55

0019, Yerevan, Armenia law@aua.am

## I- The Transformation of the Extraterritorial Scope from the DPD to the GDPR

This section outlines the relevant articles for the extraterritorial application of the DPD and its transformation in the GDPR. The DPD was the only legislation in its scope that clarified the jurisdictional range when trying to find some legal limitations in the EU data protection legislations.[10] Nowadays, the Right to Privacy is one of the most established areas of law in the European Union. The European Convention on Human Rights (ECHR) Article 8, which is signed by all EU member states, provides a ‘’right to respect for private and family life ‘’ and though subject to certain restrictions, asserts that ‘’ Everyone has the right to respect for his private and family life, his home and his correspondence’’. In the end of the 20th century, the Organization for Economic Co-operation and Development (OECD) published its "Recommendations of the Council Concerning Guidelines Governing the Protection of Privacy and Trans-Border Flows of Personal Data" where it included 7 principles for the protection of personal data.[11] While those principles were non-binding, they were all incorporated into the EU Directive, and later on, the European Commission proposed a new Directive, because it realized that the differences of data protection legislation were hindering the free flow of data within the Union. The draft of the DPD and its earlier proposals indicate that the drafters of the directive aimed to delimit the applicable law to avoid processors trying to escape the jurisdictional reach of the directive.[12] If data processors were able to avoid having the DPD cover their activities by

[10] Kuner, Christopher, *‘Jurisdiction on the Internet: Part I’*, International Journal of Law and Information Technology, Vol 18(2), 2010, pp. 176- 193

[11] Guidelines on the Protection of Privacy and Transborder Flows of Personal Data The Organization for Economic Co-Operation and Development, last modified 5 January 1999.

[12] Dan Jerker B Svantesson, *Extraterritoriality and targeting in EU data privacy law: the weak sport undermining the regulation,* International Data Privacy Law, 2015, Vol. 5, No. 4, p. 84



40 Marshal Baghramyan Avenue Tel: (37410) 51 27 55

Tel: (37410) 51 27 55

0019, Yerevan, Armenia law@aua.am

relocating outside of the EU territory, this would mean that this instrument was purely territorial in its nature. This is why the drafters of the DPD broadened the scope of its application to include an extraterritorial range. For this legislation, the European Commission had the aim to ‘’revise and clarify the existing provisions on applicable law [ultimately to] provide for the same degree of protection of EU data subjects, regardless of the geographic location of the data controller”.[13]

The language of the Directive in article 4 claims the following:

1. Each Member State shall apply the national provisions it adopts pursuant to this Directive to the processing of personal data where :
    a. The processing is carried out in the context of the activities of an establishment of the controller on the territory of the Member State; when the same controller is established on the territory of several Member States, he must take the necessary measures to ensure that each of these establishments complies with the obligations laid down by the national law applicable;
    b. The controller is not established on the Member State's territory, but in a place where its national law applies by virtue of international public law;
    c. The controller is not established on Community territory and, for purposes of processing personal data makes use of equipment, automated or otherwise, situated on the territory of the said Member State, unless such equipment is used only for purposes of transit through the territory of the Community.
2. In the circumstances referred to in paragraph 1 (c), the controller must designate a representative established in the territory of that Member State, without prejudice to legal actions which could be initiated against the controller himself.

The DPD stated overall that each member state should apply its own national data protection law when a controller is carrying out a processing activity through an establishment on the territory of a Member State. Although recital 19 of the DPD asserted that an establishment on a Member

[13] European Commission, *‘A comprehensive approach on personal data protection in the European Union’*, COM (2010) 609 final of 4.11.2010, p. 11



40 Marshal Baghramyan Avenue Tel: (37410) 51 27 55

Tel: (37410) 51 27 55

0019, Yerevan, Armenia law@aua.am

State's territory "implied the effective and real exercise of activity through stable arrangements", the DPD did not provide a legal definition of 'establishment'. On the other hand, the establishment does not need to be independent of the controller to be considered as a controller himself.

A distinction that is significant here is when looking at the extraterritorial application according to the DPD was the distinction between data controller and data processor, because the directive's requirements centered upon components of an entity as a controller or processor and their location. Since a processor should process data according to the instructions given by a controller, this was used to subsequently help enlighten the jurisdictional range of the DPD.[14]

According to the DPD, the controller was defined as '' the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data […]".[15] This definition ascertains that the controller was responsible for the personal data. In contrast, the DPD defined the processor as '' a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller". [16] Accordingly, the processor and the controller could be unconnected legal entities.[17]

While the terms controllers and processors are defined in the GDPR in the same way as defined in the DPD,[18] nonetheless, the GDPR convenes new obligations on both the processor as well as the controller.[19] Similarly, the DPD referred to the territory in its articles as ''national law applicable'', while the GDPR refers to it as ''in the Union'', which suggests a territory that is not necessarily physical. In the *Salemink* case, the Advocate General asserted its opinion that '' for EU purposes, the 'territory' of the Member States in the area (not necessarily territorial, in the

[14] Kuner, Christopher, *supra* note at 11, pp. 70
[15] Directive 95/46/EC, Art. 2(d)
[16] DPD, Art. 2(e)
[17] Article 29 Working Party, 00264/10/EN WP 169 Opinion 1/2010 on the concepts of "controller" and "processor", 16 February 2010, p. 1
[18] GDPR, Arts. 4(7) and 4(8).
[19] Ustaran, Eduardo, '*EU General Data Protection Regulation: things you should know'*, Privacy and Data Protection, Vol. 16(3), 2016, p. 4.



40 Marshal Baghramyan Avenue Tel: (37410) 51 27 55

Tel: (37410) 51 27 55

0019, Yerevan, Armenia law@aua.am

spatial or geographical sense) of exercise of the competences of the Union". This defines the link between sovereignty and territory closer to a dependence rather than a necessary truth. [20]

The main aim of the GDPR is to protect the personal data of the residents of the European Union. As an upgrade from the DPD, the Commission drafted the regulation in such a way that it weighs on the conduct of the operator, which trails a ''destination'' approach.[21] Article 3(1) of the GDPR applies to the application of the scope of jurisdiction, which repeats the same jurisdiction nexus of the DPD article 4(1)(a) as discussed above. The addition by the parliament was made in line with the C-131/12 *Google Spain* and the concepts behind the commission's script.[22] This Court of Justice of the European Union (Hereinafter CJEU) case held that the Google who is the operator, is responsible for the processing activities that it carried out on web pages published by third parties. Therefore, by applying this case, a non-EU processor could fall within the scope of this article if it has a subsidiary or a branch in the Union and the data processing activities are inseparable from the activities performed in the EU.

The scope of application of the GDPR is divided into two situations: when the controller is established in the Union and when it is not. If the controller is established in the Union, it falls under article 3(1), and accordingly, ''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.''. In its turn, this rule is divided into two parts, on the one hand, it is still similar to what the DPD provided, as a processing of data for activities of the controller or processor established in the Union. On the other hand, the second part broadens vastly the application of the regulation further than the EU original borders are.[23]

With the DPD, an important factor to determine the applicable law was the place of processing. However with the GDPR, the place is no longer an important criteria to determine the applicable

[20] AG Opinion, Salemink, Case C-347/10, 8 Sept., 2011, paras 54-57
[21] Adele Azzi, "*The challenges faced by the Extraterritorial Scope of the General Data Protection Regulation".* p.129
[22] Recital 19 of the Commission's proposal
[23] Carol A F Umhoefer and Caroline Chancé, ' Europe: The Applicability Of EU Data Protection Laws To Non-EU Businesses', DLA Piper LLP (2016) available at <http://www.lexology.com/library/detail .aspx?g=95e11bfd-2931-44da-ac29-371614c516bd>



40 Marshal Baghramyan Avenue Tel: (37410) 51 27 55

Tel: (37410) 51 27 55

0019, Yerevan, Armenia law@aua.am

law as it has to be done in the context of the activities of an establishment of a controller or a processor' though, the location can be outside the Union, as long as the establishment of the controller is present within the EU. For that reason, the Google Spain issue that had occurred since the processing was in the United States will no longer be problematic after the GDPR.

What differs mostly is the text of Article 3(2), which prompts more circumstances than the DPD. Article 3(2) applies EU rules to non-EU operators who process personal data of individuals in the EU in two situations: offering goods and services and the monitoring of the behavior of the people in the EU. Without referring to the word ''extraterritorial'', this provision permits non-EU data subjects to be brought under the GDPR, regardless of whether a payment is required for the actions.[24]

The basis of jurisdiction is similar to the language provided in the Brussels I Regulation, which states that once a processor directs his activity towards consumers residing in a particular Member State, the consumers cannot be deprived of the protection and non-derogable rules that comes with the Regulation.[25] This is also known under the logic of '' you are targeted by EU law only if you target''. [26] Recital 23 provides a full grasp of the degree of application and claims that passive features cannot fall under the scope, such as the mere access of a website or the asking of email addresses or the use of a specific language. Those are not sufficient to establish such intentions. Therefore as the Recital asserts, the factors need to be ''*apparent*''.[27]

By offering goods or services to EU data subjects, the processor can become the controller, and fall under the scope of article 3(2)(a). However, although the scope has broaden up since the DPD, there is still confusions in some specific scenarios; such as when non-EU companies who act globally and do not specifically target EU and perform all tasks in a third country, will the GDPR cover the data processing if EU data subjects use such companies' websites connected to

[24] Paul de Hert, Michal Czerniawski; *Expanding the European data protection scope beyond territory: Article 3 of the General Data Protection Regulation in its wider context*, International Data Privacy Law, Volume 6, Issue 3, 1 August 2016, Pages 230–243
[25] Regulation (EU) No 1215/2012 of 12 December 2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters, Art. 17(1)(c).
[26] Paul de Hert, Michal Czerniawski, at *supra* note 24.
[27] GDPR, Recital 23


40 Marshal Baghramyan Avenue Tel: (37410) 51 27 55
Tel: (37410) 51 27 55
0019, Yerevan, Armenia law@aua.am

their activities? The wording suggests a very broad interpretation for the processing activities, which merely facilitates the offering of goods or services by controllers.

While there is no clear idea on what offering of goods or services entails, Recital 20 claims that is ‘’apparent that the controller is envisaging the offering’ of goods/services to European data subjects’’. The standard of envisaging of this article is similar to the criteria of ‘’orienting’’ businesses established by the CJEU in *Pammer and Hotel Alpenhof* case and the *Google Spain* case. This shows that the question of applicable law has shifted to a global level where the EU authorities and the third countries will have to raise issues of application of EU law prior to addressing the issue of compliance of the GDPR. This is bound to cause controversy because third countries by only offering goods or services to EU subjects will fall under the GDPR. In this regard, this will bring all internet providers under the scrutiny of the GDPR as soon as they interact with EU subjects. Another controversy is regarding the mere presence of data subjects in the Union, without having to reside in it permanently.

Furthermore, under article 3(2)(b), the GDPR applies to non-EU operators processing personal data relating to the monitoring of conducts/behaviors of EU citizens, as long as such behaviors take place in the Union. It follows that most EU data processing will be triggered under the GDPR, especially when it is carried out by companies for their businesses. However, it will not apply to non-EU entities if for example, they collect data on EU consumers in order to classify data subjects based on their characteristics and to obtain aggregated overviews of their customers without making individual predictions.[28]

To determine if the monitoring of the data subjects is relevant under this article, the recital states that ‘’the potential subsequent use of personal data processing techniques which consists of profiling a natural person, particularly in order to take decisions concerning her or him for analyzing or predicting her or his personal preferences, behaviors and attitudes’’.[29]

[28] Article 29 Data Protection Working Party, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 p. 7.
[29] GDPR, Recital 24



40 Marshal Baghramyan Avenue Tel: (37410) 51 27 55

Tel: (37410) 51 27 55

0019, Yerevan, Armenia law@aua.am

As well as, the factors of monitoring include, but are not limited to their personal inclinations, interests, position or movement etc… that could be established through online identifiers tools such as IP addresses and cookies that serve the purpose of profiling data subjects.[30] Thus, monitoring involves not only social media networks, email providers, or operators of search engines, but also a vast majority of websites that collect surfing behavior through either cookies, ad banners, or JavaScript.[31] As opposed to the provisions provided under article 3(2)(a), neither subsection (b) nor Recital 24 specify a necessary degree for the ‘’intention to target’’ by either the controller or the processor to define whether the monitoring could prompt the application of the GDPR. Using the word "monitoring," however, implies that the controller has a specific purpose in mind for the gathering and salvage of relevant data on the behavior of an individual within the EU. The purpose of the controller to process the data and, in specific, any subsequent behavioral examination or describing techniques involving that data will need to be considered.

Therefore, article 3(2) substantially increases the scope of EU data protection rules and is larger than any other jurisdiction the world has done so far. Even though it refers to the operator's alleged voluntary conduct to justify the regulation's application, the application of the regulation almost "follows" EU data in practice. In view of the sudden application of EU rules to many websites worldwide, one might wonder on what legal basis the regulation is based on its legitimacy and authority.[32] Hence, the GDPR applies when the processing events are ‘’related’’ to the contribution of goods or services, or to the monitoring of the behavior of subjects in EU. While it has been contended that this analysis leads us to consider that the GDPR applies as soon as the activities concern subjects in the EU.[33] Since the word ‘’related’’ is reflected as a vague term, this could suggest that the connection does not need to be that resilient between the processing and the offering of goods or services or even the monitoring. Nevertheless, this does not cause any issues as the GDPR applies the minute any type of connection is found.

[30] GDPR, Recital 30.
[31] Lokke Moerel, *The long arm of EU data protection law: Does the Data Protection Directive apply to processing of personal data of EU citizens by websites worldwide?* International Data Privacy Law, 2011, Vol. 1, No. 1.
[32] Adele Azzi, at *supra* note 21.
[33] Malcolm, W, Overseas or Cross-Border Transfers of Personal Data: Schrems, Brexit and the General Data Protection Regulation, in: Jay, R, Guide to the General Data Protection Regulation: A Companion to Data Protection Law and Practice, p 156.



40 Marshal Baghramyan Avenue Tel: (37410) 51 27 55

Tel: (37410) 51 27 55

0019, Yerevan, Armenia law@aua.am

Concerning the liability aspect, under the Directive, the controller is liable for all of the actions and joint controllers were in general only liable for the injury for which they were accountable. Accordingly, data subjects may not have been able to get full reparation for damages resulting from joint processing under certain circumstances.

In the GDPR however, both the controller and the processor can be responsible for injuries and can be appealed by the data subject.[34] The GDPR also overturned the approach towards joint controllers by making all of them fully accountable to the data subject. The data subject is therefore entitled to bring a claim against any of the joint controllers. Only when the data subject has been fully recompensed, the joint controller(s) who paid that sum may pursue to recover damages from other joint controllers that were intricate in the processing. Controllers that prove that they were in no way responsible for the harm can be exempted from this.[35] Consequently, even if a joint controller has only minimal responsibility for an injury, they endure liability to pay the affected data subjects "full compensation." This is why joint controllers might seek contractual obligations from each other before the processing begins.

[34] GDPR, Recital 80.
[35] GDPR Art.26, GDPR, Recital 79.



40 Marshal Baghramyan Avenue
Tel: (37410) 51 27 55
Tel: (37410) 51 27 55
0019, Yerevan, Armenia
law@aua.am

## II- The Pre-GDPR Case Law that shaped the regulation

In recent years, there were several rulings given by the CJEU that influenced the Regulation. The landmark *Lindqvist* case of the CJEU affirmed that EU law does not apply to the global internet. In this case, the CJEU made pronouncements claiming that simply being present in the Union and uploading personal data to webpages does not constitute as a transfer of personal data to a third State. This decision was important to limit the scope of application of the law, and the Court noted that not all states with internet consumers who access EU pages required authorized acknowledgments of adequate data protection.

The wording of the jurisdiction in the DPD stated that the location of the established controller and its equipment were important to trigger the application of the Directive.[36] If personal data is processed in part or in whole outside of the territory of the EU, but there is still a significant linkage with the EU through the institution of the controller and the variety of their actions, the DPD could have been applied. Before the Court of Justice intervened, the directive was applicable, when ‘’the processing [was] carried out in the context of the activities of an establishment of the controller on the territory of the Member State’’.[37] Thus, the Directive could not reach a controller that processed EU data entirely outside of the union, even if the controller had establishments within the EU. This was until the *Google Spain* case, where the processing carried out by Google Inc., in the United States was being profited through the activities happening in the EU establishment. The Court claimed that there was an economic link between the EU establishment and the data processing in the US; therefore, the US Inc. was bound by the DPD when processing Europeans personal data.[38]

The Directive was also applicable when the controller was not established in the Union, but ‘’for the purposes of processing personal data, [the controller] makes use of equipment (…) situated

[36] DPD, Art. 4
[37] DPD, Article 4(1)(a).
[38] Case C-131/12, *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González* (2014)



40 Marshal Baghramyan Avenue Tel: (37410) 51 27 55

Tel: (37410) 51 27 55

0019, Yerevan, Armenia law@aua.am

[in the EU]".[39] The placing of cookies were considered as ''equipment'', as well as JavaScript and Spywares. With the GDPR however, this was extending under the monitoring of the behavior of the people in the EU.[40]

Following the *Google Spain* case, the CJEU further confirmed in the *Weltimmo* case the wide scope of establishment.[41] The court held that the institution of a legal entity registered in the EU was not necessary for an EU establishment to exist. The mere existence of a website in a local language, local bank account, postbox and local representatives were all required for an establishment to be considered initiated in a member state of the Union.[42] This decision was in support of broadening the interpretation of the ''establishment'' necessary to give effect to the objective of the DPD, which ''consists of ensuring effective and complete protection of the right to privacy and in avoiding any circumvention [of the law]''.[43] The court therefore claimed that this concept extends to ''any real and effective activity – even a minimal one – exercised through stable arrangements'' and the mere presence of only one representative in the EU can in some circumstances give rise to an ''establishment''.[44]

Furthermore, the GDPR adopts the words ''offering goods or services'' instead of ''directing activities'' that was used in 2011 draft version of the European Commission's proposal for the GDPR.[45] Article 2(2) of the draft stated that the Regulation applies when the controller is not established in the Union, but the processing targets subjects residing in the EU, or when the processing serves to monitor their behaviors.[46] While the wording was changed in the final version of the Regulation, the drafters still had in mind the EU case law where the wording ''directing activities'' were used beforehand.

---

[39] DPD, Article 4(1)(c).
[40] Lokke Moerel, *supra* note at 31.
[41] Case C-230/14 *Weltimmo.*
[42] *Ibid,* paras. 32-33
[43] *Ibid,* para. 30
[44] *Ibid,* paras. 30-31.
[45] The European Commission's Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation), Version 56 (draft).
[46] Kuner, C, The European Commission's Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection Law, p 6.



40 Marshal Baghramyan Avenue Tel: (37410) 51 27 55

Tel: (37410) 51 27 55

0019, Yerevan, Armenia law@aua.am

This concept was used in the joined cases of *Pammer* (C-585/08) *and Hotel Alpenhof* (C-144/09) already stated in Chapter I. The cases were joined, as the Austrian Supreme Court believed that the cases had similarities.[47] The *Pammer* case concerned a dispute between Mr. Pammer, an Austria resident and a Travel Freight company established in Germany, where Mr. Pammer claimed payment before an Austrian court, after the description of the booked travel did not correspond to the conditions on the freight. The *Hotel Alpenhof* case concerned a dispute between the Hotel operating in Austria and a consumer residing in Germany. The customer, who had found and reserved at the hotel on the internet, refused to pay for the rooms because of the faults of service, even after being offered a discount. The hotel also brought an action before the Austrian court. Both cases have a defendant raising a plea before the court, with an action in question that lacks jurisdiction. The questions referred to the CJEU for preliminary ruling was the interpretation of the ‘’directing activities’’ in Article 15(1)(c) of the Brussels I Regulation[48], as well as the same wording used in the draft of the GDPR. The court ruled that ‘’ it should be ascertained whether, before the conclusion of any contract with the consumer, it is apparent from those websites and the trader’s overall activity that the trader was envisaging doing business with consumers domiciled in one or more Member States, including the Member State of that consumer’s domicile, in the sense that it was minded to conclude a contract with them.’’[49] The court furthermore presented a non-exhaustive index of concerns demonstrating that the undertakings are directed to a specific territory, such as ‘’the international nature of the activity, mention of itineraries from other Member States for going to the place where the trader is established … ‘’[50]

This ruling was followed by subsequent rulings, namely *Mühlleitner* (C-190/11) and *Emrek* (C-218/12), which also concerned the interpretation of the Brussels I Regulation article 15(1)(c). The *Mühlleitner* case concerned a question on whether article 15(1)(c) was limited to distance contracts. While the *Emrek* case concerned the question whether there needed to be a causal link between a website and the conclusion of a contract. The court established that there is no

[47] Joined cases C-585/08 and C-144/09, para 32.
[48] *Ibid*, para 31 and 47.
[49] *Ibid*, para 92.
[50] *Ibid*, para 93.



40 Marshal Baghramyan Avenue
Tel: (37410) 51 27 55
Tel: (37410) 51 27 55
0019, Yerevan, Armenia
law@aua.am

requirement of a causal link between the website in use for the commercial activity and the consumer's domicile, as well as the conclusion of the consumer contract. Furthermore, it was contended that notwithstanding the fact that there is no necessity for a causal link, this same link could constitute a strong evidence, which could be considered by national courts when determining the directed activities of a trader. In addition, the court referred to the list given in the Joined cases of *Pammer and Hotel Alpenhof*, and added some new factors, like ''the establishment of contract at a distance'', because those factors may help constitute further evidence for a connection between a contract and the 'directed activity'.[51]

While interpreting the targeting approach of Article (3)(2)(a) in light of the EU case law, Advocate General Jääskinen noted in the *L'Oréal and Others case*, that if companies established outside the EU and targeting consumers in the EU do not have to comply with EU rules on consumer protection, intellectual property rights protection and other areas of law, the ''effet utile'' of EU law would not be guaranteed.[52] The same could be argued with regard to EU data protection law and data subject protection present in the EU. If aiming data subjects in the EU is not enough to adopt the GDPR, a company may escape GDPR's reasonably stringent rules by moving to a third country. This was considered as an issue in the DPD, as it required a 'physical' presence in the Union. The wording of the jurisdiction in the GDPR displays an explicit physical territory.[53] which shows that the GDPR has now a wider scope than the DPD, because instead of looking for the establishment/location of a controller, it also looks for the place of the establishment of the processors, as well as instances when data processing does not need to take place in the EU for the Regulation to be applicable.Likewise, a profuse number of controllers and processors that process personal data of subject in the EU are companies that are founded outside the EU. The GDPR would be weak to provide protection to data subject in the EU if the Regulation would not apply to those companies.

[51] Case C-218/12 para 20-32.
[52] Opinion of Advocate General Jääskinen, case C-324/09, para 127; Case C-324/09 para 62-63.
[53] GDPR, Art. 3.



40 Marshal Baghramyan Avenue Tel: (37410) 51 27 55

Tel: (37410) 51 27 55

0019, Yerevan, Armenia law@aua.am

Therefore, in order to ensure the effectiveness of the Regulation, it is necessary to apply to both EU-based and non-EU-based companies.



40 Marshal Baghramyan Avenue
Tel: (37410) 51 27 55
0019, Yerevan, Armenia
law@aua.am
Tel: (37410) 51 27 55

## III- The Governance of International Law in Regards To the Extraterritorial Claims

The GDPR's extraterritorial claim must comply with certain provisions. In fact, jurisdictions, including the EU and its institutions, are bound to comply with public international law when doing so.[54] Therefore, it is necessary to examine the conditions under which public international law could legitimize an extraterritorial claim. The result of this evaluation can either seriously contest such expansion or, on the contrary, support it.

According to Article 29 of the Working Party, cross borders cases present in data protection law is ‘’ a general question of international law’’.[55] Hence, as stated by the *Lotus* case, states have ‘’ a wide measure of discretion […] to adopt the principles which it regards as best and most suitable’’.[56] When it comes to state sovereignty and non-interference, there are some limitations under international law[57]. Nevertheless, the principle of extraterritoriality claim could be weighed under article 38 of the Statute of the International Court of Justice as ‘’ “international conventions [...] establishing rules expressly recognized by the contesting states; international custom, as evidence of a general practice accepted as law; (and) the general principles of law recognized by civilized nations [...]”. While there are no specific international conventions directly related to data protection, the principle of privacy protection is articulated in a couple of conventions in a more general tone, such as the Universal Declaration of Human Rights, and the International Covenant on Civil and Political rights. Therefore, the focus cannot be on International Conventions as a means to govern the extraterritorial scope of the GDPR.

[54] Case C-366/10 , Air Transp. Ass’n of Am. and Others v. Sec’y of State for Energy and Climate Change, 2011, §101.
[55] Article 29 Data Protection Working Party, p. 2.
[56] *SS Lotus, (France v Turkey),* PCIJ Reports, Series A, No 10, p. 19 (1927).
[57] Christopher Kuner, *supra* note at 11, p. 186.



40 Marshal Baghramyan Avenue Tel: (37410) 51 27 55

Tel: (37410) 51 27 55

0019, Yerevan, Armenia law@aua.am

While the DPD was implemented into national law, the GDPR provisions are directly applicable in Members States, and since they reflect EU law, then the Union is bound by the customary international law of jurisdiction.[58]

There must be a sufficient connection under Public International Law before a state can claim either prescriptive or adjudicative jurisdiction.[59] There are about five general principles where a claim of jurisdiction could be based, this includes the territoriality principle, the nationality principle, the effects principle, the protective principle, or the universality principle.[60] Under the principle of territoriality, each state has the right to regulate in its own territory personal matters and events,[61] which is based on the principle of sovereign equality of states as well as the principle of non-intervention.[62]

Under international law and the principle of territoriality, if states wish to be recognized as sovereign within its own borders, it must respect other states' sovereignty and exercise restraint before exercising extraterritorial jurisdiction.[63] However, some states still try to regulate events and conducts taking place abroad, under a variation of reasons or justifications. This was first identified in the Permanent Court of Arbitration *Island of Palmas* judgement; the court established that when settling inter-state relations, they shall begin with the notion that States have exclusive competence regarding their own territories.[64] It is a known fact that States sometime try to regulate matters beyond their own territory and jurisdiction and domestic

[58] CJEU, Air Transport Association of America and Others v Secretary of State for Energy and Climate Change, Case C-366/10, 21 December 2011, paras 101 and 123: "[the EU] is bound to observe international law in its entirety, including customary international law, which is binding upon the institutions of the European Union".
[59] Michal Czerniawski, 'Do we need the 'Use of Equipment' as a factor for the territorial applicability of the EU Data Protection Regime?'
[60] Svantesson, Dan Jerker B., *supra* note at 12, p. 80
[61] Uta Kohl, Jurisdiction and the Internet – Regulatory Competence of Online Activity (Cambridge University Press 2007)

[62] Cedric Ryngaert, Jurisdiction in International Law (Oxford University Press 2008)

[63] Brendan Van Alsenoy and Marieke Koekkoek, 'Internet and jurisdiction after Google Spain: the extraterritorial reach of the 'right to be delisted'' (2015) 5 IDPL105, 108.
[64] *Island of Palmas Case* (or Miangas), United States v Netherlands, Award, (1928) II RIAA 829, ICGJ 392 (PCA 1928), 4th April 1928, at 838



40 Marshal Baghramyan Avenue Tel: (37410) 51 27 55

Tel: (37410) 51 27 55

0019, Yerevan, Armenia law@aua.am

concerns,[65] however when a foreign element is present, it is required to have some limitations[66], a fact that was acknowledged in the International Court of Justice *Barcelona Traction* case.[67] The whole objective of the EU is in no exception of this regard, as the aim is to scrutinize the extraterritorial reach of the GDPR through public international law[68] and while there is a traditional presumption against exercising extraterritorial jurisdiction, even in Lotus case the Permanent Court of International Justice anticipated a shrinkage of physical borders.[69] Unless there is a prohibitive rule, States could be allowed to exercise jurisdiction. As established by the Lotus case,[70] where the court did not rule against Turkey's action as being a violation of international law as there were no prohibitive rule regarding it.[71] The other fundamental approach as supported by customary international law forbids States from practicing their jurisdiction except in the existence of a positive rule allowing them to do so.[72]

Another approach to consider jurisdiction as an international custom under international law is the conditions concerning duration, uniformity and consistency of practice should be satisfied. While the ''territory principle'' is considered undoubtedly as custom, it comprises however of merely defining jurisdiction by referencing to a place where a wrongdoing is committed.[73] While the US Supreme Court has stated that ''acts done outside a jurisdiction, but intended to produce and producing detrimental effect within it, justify a state in punishing the cause of the harm as if he had been present at the effect",[74] this however cannot be applicable for the GDPR as it is now considered as open ended, particularly in a globalized market where ''everything has an effect on everything''.[75] Taking those grounds into consideration, Article 3(2) still remains as a

[65] Mann, Frederick A. 'The Doctrine of Jurisdiction in International Law', Recueil des Cours 111, 1964, pp. 1–1621, p. 9.
[66] Svantesson, Dan Jerker B., *supra* note at 12, p. 61
[67] Case concerning *Barcelona Traction, Light and Power Co Ltd* (*Belgium v Spain*), Separate Opinion of Judge Sir Gerald Fitzmaurice, (1970) ICJ Reports 65, para. 70.
[68] Van Alsenoy, B., Reconciling the (Extra)territorial reach of the GDPR with public international law. P.90-91
[69] *S.S. "Lotus", France v Turkey*, *supra* note at 56, para 45
[70] *Ibid*, paras 45-49
[71] *Ibid,* paras 45-46
[72] Arrest Warrant (n 16) (Joint separate opinion of Judges Higgins, Kooijmans and Buergenthal), paras 49-50
[73] Svantesson, Dan Jerker B., *supra* note at 12, p. 58
[74] Strassheim v. Daily, 221 U.S. 280, 285 (1911).
[75] Christopher Kuner, *supra* note at 11, p. 186.


40 Marshal Baghramyan Avenue Tel: (37410) 51 27 55
Tel: (37410) 51 27 55
0019, Yerevan, Armenia law@aua.am

controversial basis of jurisdiction, as the regulation places its focus on the location of the violation and discards the location where the processing is occurring.

Another source regarding the legal basis includes general principles of law. While this source is commonly considered as secondary source to custom and treaty, it does nevertheless map the best domestic laws and practices in scope of data protection regulations. The evaluation of some regimes, without going through all national data protection laws, is quite revealing of the degree of legitimacy that the GDPR can recognize and therefore its authority.

If we take a look at national legislations that have extraterritorial claims, we can take in example the Australian system, and their 1988 Privacy Act which applies to all operators with Australian link, or the Personal Data Protection Act of 2012 of Singapore that applies to all individuals in Singapore, whether the operators are in Singapore or not. We can also look at the United States Children's Online Privacy Protection Act, which applies to websites targeting children in the US, or the US Foreign Corrupt Practices Act. Therefore, while International custom displayed a conflicting support for the extraterritorial scope of the GDPR, general principles divulge an inclination to broaden the reach of the territorial scope. Many States seem to recognize the importance of the application of data protection rules outside their territories.

Accordingly there is an understanding that: (i) the EU's data protection law does in fact have extraterritorial impact; (ii) Unless expressly authorized to do so, States may not exercise jurisdiction; (iii) a substantial link should exist between the regulating State and the situation; (iv) The jurisdictional principles of public international law can determine how and when the EU can exercise its extraterritorial jurisdiction.



40 Marshal Baghramyan Avenue
Tel: (37410) 51 27 55
0019, Yerevan, Armenia
law@aua.am
Tel: (37410) 51 27 55

## IV- How the Extraterritorial Scope of the GDPR is Enforced on Non-EU Members

The enforcement of the GDPR, as stated above, like similar national regulations with international scopes have to resort to international law to enforce its provisions on operators, as well as penalties for violations.[76] Under International law, the principle of jurisdiction determines how the EU can lawfully exercise its jurisdiction when enforcing the regulation.[77]

The direct enforcement for non-EU operators is obvious through the articles of the GDPR, as it includes having representatives in the Union, cooperating with other jurisdictions and international measures for noncompliance. However, for its indirect enforcement, there are many ways where non-EU operators could feel obligated to comply with the GDPR to continue carrying out business in the Union.

Article 27 is considered as a ‘’hidden obligation’’ for non-EU operators, by imposing the need to have a representative in the Union.[78] Under article 27 of the GDPR, operators subject to Article 3(2), should designate a representative in the Union, where the data subjects are mostly located, this includes a representative, a legal entity or an individual person. Their tasks include representing foreign operators with their obligations and becoming a focal point of contact with the authority, to cooperate and comply with the regulation.[79] The purpose of this is to simplify the contact between controllers or processors outside the Union holding personal data of EU citizens.

Many questions rose regarding the representative and the probability of them being held liable with the operator for non-compliance. However, Recital 80 does state that the representative ‘’should be subject to enforcement proceedings in the event of non-compliance by the controller

[76] Kurt Wimmer, The Long Arm of the European Privacy Regulator: Does the New EU GDPR Reach U.S. Media Companies? Comm. Law., Summer 2017, at 16.
[77] Int’l Law Comm’n, Rep. on the Work of Its Fifty-Eighth Session, U.N. Doc. A/61/10, at 520–523 (2016).
[78] Tim Bell, Is Article 27 the GDPR's 'hidden obligation'?, available at <https://iapp.org/news/a/is-article-27-the-gdprs-hidden-obligation/>.
[79] GDPR, art. 31, GDPR Recital 80


40 Marshal Baghramyan Avenue Tel: (37410) 51 27 55
Tel: (37410) 51 27 55
0019, Yerevan, Armenia law@aua.am

or processor''. This has been proven in the Netherlands, in a case held under the Directive, against WhatsApp, where the court considered that the Data Protection Officer (DPO) could be held liable for non-compliance.[80] Although the role of the representative somehow differs from the role of the DPO, their roles still overlap in some way. WhatsApp had claimed in its arguments that it could not find a representative to endorse such liabilities, and while this was rejected by the court, this is set to become a big concern for international companies – as the possibility of finding a representative ready to induce all those potential liabilities is very thin and even if they do find, how much of an influence can a representative have over the operator? Other issues that could occur consists of cooperation measures for investigation and the enforcement of the decisions or judgements on other jurisdictions, which should be fixed overtime with international cooperation agreements.

The enforcement of GDPR in non-EU jurisdictions falls within the scope of the ''effects doctrine'', which considers the assertion of jurisdiction '' with regard to the conduct of a foreign national occurring outside the territory a State which has a substantial effect within that territory,'' while no component of conduct is required to take place in the State.[81] Chapter V of the Regulation requires a suitable level of protection in third countries, although the requirements are trifling compared to the full compliance enforced under article 3.

To illustrate, while it is considered controversial to assert jurisdiction under international law, it has however helped regulate conduct that is omnipresent and has cross-jurisdictional subjects. [82] Unlike other regulations targeting industries with a comprehensive national regulatory framework, enforcement of GDPR fines and penalties can be difficult in jurisdictions where technology and data protection regulations are virtually non-existent, let alone in line with the EU data protection approach. Overall, in order to enforce its judgments against entities outside the Union, the EU must rely on the authorities of other jurisdictions. Since the EU commission considers that several non-EU jurisdictions have adequate data protection laws, data processors and controllers can freely transfer data from the EU to such jurisdictions, such as Canada and

[80] Administrative Court of The Hague, 22 November 2016, SGR 15/9125.
[81] Int'l Law Comm'n, Rep. on the Work of Its Fifty-Eighth Session, *supra* note at 47, 523.
[82] *Ibid.* at 525 n.29



40 Marshal Baghramyan Avenue Tel: (37410) 51 27 55

Tel: (37410) 51 27 55

0019, Yerevan, Armenia law@aua.am

Israel. Those jurisdictions can also be said to be in accordance with EU data protection laws and have an interest in enforcing fines where applicable. However, the issue becomes more intricate when a non-EU jurisdiction (such as the United States) has diverse technology companies dealing with cross-jurisdictional data transfers, but lacks inclusive data protection laws comparable to the GDPR. [83] This is the reason why the EU-US Privacy Shield agreement was established in collaboration with the Federal Trade Commission and U.S Department of Commerce.[84] As a regulatory framework, the Privacy Shield sets ground rules for data transfers between the EU and the United States and binds voluntarily listed companies in the Privacy Shield to GDPR implementation actions, including penalties and sanctions.[85] On the other hand, if a U.S. business is not registered with the Privacy Shield, the court will only enforce international judgments if the GDPR judgment does not include constitutional rights, federal or state law rights or concerns of public policy.[86]

An example of this would be a U.S. media company claiming First Amendment rights against a GDPR fine or a DPA judgment, the GDPR fine will be effectively unenforceable if the U.S. courts side with the U.S. media company. Nevertheless, the media company might still comply for the sake of its reputation, as other companies might reject its business because its data protections standards are lower than the normative international ones. This could be considered as a method of indirect enforcement, as companies care about their reputations and could be scared of losing prominent businesses by failing to comply with the GDPR, as other companies not protected under the Privacy Shield would not want to expose themselves to the risk of being fined by the regulation for non-compliance.

[83] General Data Protection Regulation (GDPR), *Third Countries*, GDPR (Oct. 30, 2018), https://gdpr-info.eu/issues/third-countries/.
[84] Patrick Nohe, *The GDPR and Privacy Shield – Compliance for US Businesses*, Hashed Out (Mar. 30, 2018), https://www.thesslstore.com/blog/gdpr-privacy-shield-compliance-us-businesses/.
[85] U.S. Dep't of Com., *EU– U.S. Privacy Shield Framework Principles* 7 (2016), https://www.privacyshield.gov/EU-US-Framework.
[86] Mata v. Am. Life Ins. Co., 771 F. Supp. 1375, 1384 (D. Del. 1991) (the court declined to recognize foreign judgment as the process failed to comport to due process clause of the Fourteenth Amendment)


40 Marshal Baghramyan Avenue Tel: (37410) 51 27 55
Tel: (37410) 51 27 55
0019, Yerevan, Armenia law@aua.am

The reputational impact is massive when it comes to data protection, it is so crucial that it can indirectly broaden the scope of the GDPR.[87] Facebook is now going through this issue, as the Transatlantic Consumer Dialogue penned a letter: "We write to you on behalf of leading consumer and privacy organizations (...) to urge you to adopt the [GDPR] as a baseline standard for all Facebook services. There is simply no reason for your company to provide less than the best legal standards currently available to protect the privacy of Facebook users."[88]

Another incentive that is in link with the reputational impact is that the GDPR boosts self-compliance through its articles, as well as the implementation of new codes of conducts for their operatives and associates.[89] The codes of conducts are made available to the public to encourage companies to comply with the regulation, as it exhibits the accurate process to operate.[90] Article 40 claims the code needs to be in regards to:

Article 40(2): Associations and other bodies representing categories of controllers or processors may prepare codes of conduct, or amend or extend such codes, for the purpose of specifying the application of this Regulation, such as with regard to:

(a) fair and transparent processing;

(b) the legitimate interests pursued by controllers in specific contexts;

(c) the collection of personal data;

(d) the pseudonymisation of personal data;

(e) the information provided to the public and to data subjects;

(f) the exercise of the rights of data subjects;

(g) the information provided to, and the protection of, children, and the manner in which the consent of the holders of parental responsibility over children is to be obtained;

[87] Adele Azzi, at *supra* note 21.
[88] Transatlantic Consumer Dialogue <http://tacd.org/tacd-calls-on-facebook-to-adopt-same-privacy-standards-for-all-consumers-and-give-details-on-how-to-congress/>
[89] GDPR, Art. 40(1) and (3).
[90] GDPR, Art. 40 and 42.



40 Marshal Baghramyan Avenue Tel: (37410) 51 27 55

Tel: (37410) 51 27 55

0019, Yerevan, Armenia law@aua.am

Those can provide expedient insights on how operators need to process their data and what instruments are certified and in compliance with the regulation. This is therefore another tool to indirectly enforce the extraterritorial scope of Non-EU members.

The enforcement of the GDPR can be diminished if non-EU jurisdictions do not have comparable data protection regulations with the European commission or agreements such as the Privacy Shield. The question arises as to whether extraterritorial regulations can be enforced by local courts in such jurisdictions where they consider particular public policy concerns, analogous local data protection regulations and any relevant agreement with the EU.[91] While the GDPR will not always be enforceable on foreign operators, data transfer rules can at least guarantee an adequate level of protection in non-EU countries, therefore Chapter V of the GDPR could be considered as an indirect way of enforcing data privacy principles underlying the regulation.

[91] Al Khonaizi, M., Fines under EU GDPR in non-EU jurisdictions: enforceable or mere reputation risk? MJIL, Vol 40.



40 Marshal Baghramyan Avenue
Tel: (37410) 51 27 55
Tel: (37410) 51 27 55
0019, Yerevan, Armenia
law@aua.am

## Conclusion

This study analyzed and examined Article 3(2) of the GDPR, which states that the GDPR applies "to processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:

a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or
b) the monitoring of their behavior as far as their behavior takes place within the Union."

This article applies to cross-border situations in which the data subject is located in the EU and the controller or processor is located outside the EU. The wording of the article in the Regulation is new compared to the previously applicable DPD article 4(1)(c), which required the controller to use equipment within the EU territory when a controller is not established in the EU.

Article 3 differentiates between a situation where the controller or the processor is established in the EU (article 3(1)) and when they are not established in the EU (article 3(2)), it is therefore important to determine when a controller is established in the EU and when it is not, as well as determine who the processor is targeting. However, the problem with using the targeting criterion in data protection context is that proving an intention to target can be difficult. In addition, whether there is an intention to target data subjects in the EU when a company acts globally and targets the entire world is unclear.

While the 'targeting approach' is new in the framework of data protection law, the concept is fairly used in other fields of EU law. Significant EU case law directs that Article 3(2)(a) appears to be inspired by EU cases in which the Court used the targeting concept, such as in the Court's joint ruling in *Pammer* and *Hotel Alpenhof*. A subjective intention seems to be focused on the GDPR as well as the Court's rulings where the targeting approach is used. Objective factors however, such as language or currency on a website, can also be considered an indication to substantiate a company's subjective aim to target data subjects in the Union.



40 Marshal Baghramyan Avenue
Tel: (37410) 51 27 55
Tel: (37410) 51 27 55
0019, Yerevan, Armenia
law@aua.am

There could be businesses pursuing to become global actors in today's globalization. This means that globally acting businesses do not necessarily target EU data subjects. The question is 'Will the GDPR be applicable to those global actors?' This should be clearly stated in the Regulation if the GDPR is to be applied in cases where the company targets the whole world. The CJEU has made it clear, as already noted, that EU data protection law does not apply to the entire internet: The GDPR should instead be applied when the company targets data subjects in the EU. The GDPR usually gives concrete criteria when it considers that the business has a subjective intention of targeting data subjects present in the EU. However, in my opinion, it should be pointed out that the notion of targeting is a loaded notion that obviously requires a targeting intention. Therefore, if the Regulation applies to companies not explicitly aiming the EU, the consequence is, in my opinion, that the GDPR will apply to all global actors processing personal data of data subjects in the EU. Hence, the factors listed in Recital 23 would lose their meaning and function, as the GDPR would be applicable irrespective of whether or not such factors are present in a specific case. In other words, despite the fact that a company does not specifically target data subjects in the EU, the GDPR would be applicable.

There is a possibility that the GDPR will have a wider territorial scope than that implied by the Article 3(2)(a). As a result, the GDPR's territorial scope could become unpredictable and legal certainty could no longer be guaranteed. This ambiguity could undermine the territorial scope of the GDPR and deteriorate the protection of personal data in the EU delivered under the GDPR.

However, despite its broad territorial scope, generally speaking, after exploring Article 3(2) and comparing it to Article 4(1)(c) of the DPD, it can be noted that the GDPR is a step forward because it better takes technological growths into account.

At the same time, the EU distinguishes itself by applying a very limited nexus to jurisdiction, not only with a heavy compliance burden – especially for small businesses – but also with a substantial level of administrative fines. Therefore, the extraterritorial scope of the GDPR cannot be considered as an exception given the international context and other domestic laws. Extending the scope of data protection laws to reflect the borderless nature of the Internet is now part of a global trend.



40 Marshal Baghramyan Avenue Tel: (37410) 51 27 55

Tel: (37410) 51 27 55

0019, Yerevan, Armenia law@aua.am

However, a number of obstacles remain to be applied by the GDPR through conventional investigation measures and with a limited nexus to jurisdiction. Nevertheless, the EU still benefits rather from the "legitimacy" of extraterritorial claims and is equipped with the appropriate tools to enforce it abroad. That being said, these tools need to be further developed.

It should be noted that even unenforceable extraterritorial claims could still have certain interests. Indeed, it is recognized by numerous jurisdictions with data protection laws that, despite application complications, such laws establish a disincentive for foreign happenings to participate in illegal handlings and have the merit of '' provide consistent treatment for local vis-à-vis overseas organizations''.[92] While a law deficient in its means to implement it may undermine the legal system, "morally justifiable law, including morally justifiable law that cannot be enforced, has a quality that cannot, and should not, be ignored".[93]

[92] Public Consultation Issued by the Ministry of Information, Communications and the Arts of Singapore Proposed Personal Data Protection Bill (19 March 2012) p. 6.

[93] Svantesson, Dan Jerker B., *supra* note at 12, p. 59



40 Marshal Baghramyan Avenue Tel: (37410) 51 27 55

Tel: (37410) 51 27 55

0019, Yerevan, Armenia law@aua.am

## Table of Authorities

LEGISLATION



OFFICIAL DOCUMENTS



CASE LAW



40 Marshal Baghramyan Avenue
Tel: (37410) 51 27 55
0019, Yerevan, Armenia
law@aua.am

Tel: (37410) 51 27 55

LITERATURE

Adele Azzi, "*The challenges faced by the Extraterritorial Scope of the General Data Protection Regulation"* 9

Al Khonaizi, M., Fines under EU GDPR in non-EU jurisdictions: enforceable or mere reputation risk? MJIL, Vol 40. 26



40 Marshal Baghramyan Avenue Tel: (37410) 51 27 55

Tel: (37410) 51 27 55

0019, Yerevan, Armenia law@aua.am

Anabela Susana De Sousa Gonçalves, '*The Extraterritorial Application of the EU Directive on Data Protection'* Spanish Yearbook of International Law (2015) 4

Brendan Van Alsenoy and Marieke Koekkoek, 'Internet and jurisdiction after Google Spain: the extraterritorial reach of the 'right to be delisted'' (2015) 19

Carol A F Umhoefer and Caroline Chancé, ' Europe: The Applicability Of EU Data Protection Laws To Non-EU Businesses', DLA Piper LLP (2016) 9

Cedric Ryngaert, Jurisdiction in International Law (Oxford University Press 2008) 19

Dan Jerker B Svantesson, *Extraterritoriality and targeting in EU data privacy law: the weak sport undermining the regulation,* International Data Privacy Law, 2015, Vol. 5, No. 4, 5

Hintze, M. (2017). *Viewing the GDPR through a De-Identification Lens: A Tool for Clarification and Compliance* 4

Kuner, C, The European Commission's Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection Law 16

Kuner, Christopher, *'Jurisdiction on the Internet: Part I'*, International Journal of Law and Information Technology, Vol 18(2), 2010, 7

Kurt Wimmer, The Long Arm of the European Privacy Regulator: Does the New EU GDPR Reach U.S. Media Companies? Comm. Law., Summer 2017 22

Lokke Moerel, *The long arm of EU data protection law: Does the Data Protection Directive apply to processing of personal data of EU citizens by websites worldwide?* International Data Privacy Law, 2011 15

Malcolm, W, Overseas or Cross-Border Transfers of Personal Data: Schrems, Brexit and the General Data Protection Regulation, in: Jay, R, Guide to the General Data Protection Regulation: A Companion to Data Protection Law and Practice 12

Patrick Nohe, *The GDPR and Privacy Shield – Compliance for US Businesses*, Hashed Out 24



40 Marshal Baghramyan Avenue Tel: (37410) 51 27 55

Tel: (37410) 51 27 55

0019, Yerevan, Armenia law@aua.am

Paul de Hert, Michal Czerniawski; *Expanding the European data protection scope beyond territory: Article 3 of the General Data Protection Regulation in its wider context*, International Data Privacy Law, Volume 6, Issue 3, 1 August 2016, 10

Shakila Bu-Pasha (2017*) Cross-border issues under EU data protection law with regards to personal data protection*, Information & Communications Technology Law 4

Tim Bell, Is Article 27 the GDPR's 'hidden obligation'?, 22

Ustaran, Eduardo, '*EU General Data Protection Regulation: things you should know'*, Privacy and Data Protection, Vol. 16(3), 2016 9

Uta Kohl, Jurisdiction and the Internet – Regulatory Competence of Online Activity (Cambridge University Press 2007) 19

Van Alsenoy, B., Reconciling the (Extra)territorial reach of the GDPR with public international law. 19

ADDITIONAL INTERNET SOURCES

General Data Protection Regulation (GDPR), *Third Countries*, GDPR 24

Transatlantic Consumer Dialogue 25

What Are the GDPR Implications in Light of Facebook's Cambridge Analytica Fine?, Lawyer Monthly (2018), 6



40 Marshal Baghramyan Avenue Tel: (37410) 51 27 55

Tel: (37410) 51 27 55

0019, Yerevan, Armenia law@aua.am