TALLINN UNIVERSITY OF TECHNOLOGY
School of Business and Governance
Department of Law

Ida Valajärvi

THE LACK OF EFFECTIVE ENFORCEMENT OF GDPR OUTSIDE THE EU

Bachelor's thesis
European Union and International law

Supervisor: Evelin Pärn-Lee, LL.M.

Tallinn 2019

I declare that I have compiled the paper independently
and all works, important standpoints and data by other authors
have been properly referenced and the same paper
has not been previously been presented for grading.
The document length is 9742 words from the introduction to the end of summary.

Ida Valajärvi ……
(signature, date)
Student code: 166539HAJB
Student e-mail address: ida.valajarvi@gmail.com

Supervisor: Evelin Pärn-Lee, LL.M.:
The paper conforms to requirements in force

……
(signature, date)

Chairman of the Defence Committee: / to be added only for graduation theses /
Permitted to the defence
……
(name, signature, date)

TABLE OF CONTENTS

ABSTRACT

The aim of this thesis is to examine whether the extraterritorial enforcement of General Data Protection Regulation is effective enough to actually respond the aims of the Regulation. Also, whether there are alternative solutions for traditional strong enforcement in case of the enforcement in third countries is not sufficient enough. The EU General Data Protection Regulation (GDPR) is not international law, but an EU law with extraterritorial impact; thus it may have an influence on businesses beyond the boundaries of the European Union and EEA. In order to be respected, extraterritorial laws need to fit in the common notions of international law. However, GDPR extends the EU's jurisdiction to reach third countries in the field of data protection in an unforeseen way. The extended application of EU data protection law is essential to secure fundamental values in the internet era; however, such a broad scope of application may result in difficulties with actual enforceability of the Regulation. In order to receive answers to these questions, the author examines enforcement in the light of article 3 of GDPR, its scope of application and the means of enforcement actions which are available for the implementation of GDPR. The hypothesis of this research is that the EU is unable to enforce GDPR effectively in third countries.

The methodology which is used in this thesis is qualitative and theoretical research method and EU legislation both contemporary as well as previous are exploited in examining these research questions. Additionally, scientific books and articles written by scholars to provide analysis and commentary on the topic.

Keywords: GDPR, Extraterritoriality, Enforcement, Non-EU countries

LIST OF ABBREVIATIONS

DPA	Data Protection Authority
DPD	Data Protection Directive
DPO	Data Protection Officer
CJEU	The Court of Justice of the European Union
EDPB	European Data Protection Board
ICO	Information Commissioner's Office

INTRODUCTION

Protection of personal data is in a significant position in the European Union and recognized as a fundamental right. The EU aims at securing this right for all European data subjects. As a result of data reformation, the General Data Protection Regulation was entered into force, and more harmonized data protection framework was the core aim of the regulation. Additionally, it pursued better enforcement and cooperation between the authorities and data subjects, controllers and processors. The impact of GDPR reaches the entire world and the regulation must, in order to function properly, be enforceable outside of the EU as well. However, questions regarding how the EU can apply and enforce such widely applicable regulation outside of its borders evokes discussion. Although a similar view was already present at the time when Data Protection Directive was in force, and its effect also covered data processing of companies situated beyond the borders of the EU, GDPR's scope is even broader and thus, authenticates the common direction towards jurisdictional overreach.

GDPR is a new a Regulation, and its actual impact and efficiency have still not emerged fully. Even though the EU values data privacy at a high level the approaches in other countries in terms of the data privacy and protection may vary, and the European view may not fully be recognized globally. Hence, it may affect the recognition and enforcement of EU judgements. Also, great importance in terms of implementation and investigative powers is now given to Data Protection Authorities. It however, remains unclear how these powers can de facto be executed efficiently due to their broadness.

The aim of this research is to specify the factors which may have an impact on the efficiency of the enforcement of the General Data Protection Regulation and determine whether it can be enforced effectively. Furthermore, to provide alternative options or other possibilities to secure compliance and enforcement of the regulation in third countries. The hypothesis of this research is that GDPR lacks effective enforcement in third countries since, extraterritorial application and enforcement of laws already is a complex issue, and the supervision and enforcement is difficult to implement outside the EU.

The research method is qualitative and theoretical research. The author uses European Union Legislation for this paper and complements it with scientific articles and books written by scholars and provides distinct viewpoints to examine the research questions. EU legislation, both current and previous is used in order to provide a more comprehensive understanding regarding the problem and to identify changes in the regulation. In addition, the author compares data privacy and protection standpoints from other countries to EU's point of view, in order to take into account also a global perspective to data privacy issues since many of the data processors and controllers are seated outside of the Union. Particularly the U.S. standpoint is taken into consideration.

Chapter one introduces the concept of data protection as a fundamental right in EU and focuses on determining the legal principles behind jurisdiction under public international law which gives the competence for the extraterritorial reach of EU law. Moreover, it determines the change in territorial principles behind the Data Protection Directive and General Data Protection Regulation.

The second chapter introduces the improvement in EU data protection law towards a common trend of extraterritorial application of laws and overreach of jurisdiction and demonstrates the trend from a more practical viewpoint with the help of case law. In addition, it determines situations where General Data Protection Regulation can actually be applied in third countries and emphasizes uncertainty and confusion in the assessment criteria among processors and controllers located in third countries.

The third chapter focuses on the enforcement methods and firstly brings forth methods which are intended to use in enforcing the General Data Protection Regulation. In that way, it draws attention to the issues which may disturb the actual enforcement of General Data Protection Regulation outside the EU form several viewpoints and introduces possible solutions to these matters. Additionally, observation is given to general problems which arise from contemporary regulatory environment in the internet and cyberspace, where data is being continuously transferred cross borders.

The expected outcome of the thesis is that the EU is unable to enforce the General Data Protection Regulation effectively in third countries because the jurisdictional overlap may create problems in recognition of judgements and enforcement actions. It is also noteworthy that the European view on data privacy and protection might not be recognised globally. Additionally, the supervision for non-compliance of the Regulation is demanding in global worldwide web.

1. FOUNDATIONS ON EU'S COMPETENCE TO APPLY GDPR TO NON-EU COMPANIES

1.1. Public International Law Principles as a base of jurisdiction

The EU recognizes personal data protection as a fundamental right in both the Treaty of Functioning of EU article 16 and article 8 of The Charter of Fundamental Rights.[1] Currently, GDPR is possibly the most extensive existing data protection legislation[2] since the only binding global treaty on data protection is CoE Convention 108 which, however is an open Convention and only binding on the states that have ratified it.[3]

GDPR extends its scope of application beyond the borders of the European Union[4] and its impact thus, reaches companies outside the territory.[5] The EU is creating standards for data protection and aims at ensuring the realization of the fundamental right for data protection via its data protection legislation.[6] The EU's competence to claim jurisdiction that reaches beyond its borders stems from principles of international law.[7] Data Protection law also demonstrates the challenging contemporary stage where international law crosses at the same time with both, public and private international law.[8] Under Public International law, states may claim jurisdiction considering acts

[1] *Handbook on European data protection law*. (2018). Luxembourg: Publications Office of the European Union page 28
[2] Zarsky, T. Z. (2017). Incompatible: The GDPR in the age of big data. *Seton Hall Law Review* Vol. 47, No, 4, 995-1020 p. 995
[3] *Handbook on European data protection law*. (2018). *Supra nota* 1 p. 24
[4] Hert, P. D., & Czerniawski, M. (2016). Expanding the European data protection scope beyond territory: Article 3 of the General Data Protection Regulation in its wider context. *International Data Privacy Law, 6*(3), 230-243. p. 230
[5] Politou, E., Alepis, E., & Patsakis, C. (2018). Forgetting personal data and revoking consent under the GDPR: Challenges and proposed solutions. Journal of Cybersecurity, 4(1). 1-20 p. 1
[6] Brière, C., & Weyembergh, A. (2018). The needed balances in EU criminal law: Past, present and future. Oxford: Hart Publishing p. 229
[7] Svantesson, D. B. (2013). Extraterritoriality in the context of data privacy regulation. *Masaryk University Journal of Law and Technology* 7(1), 87 87-96 p. 92
[8] Svantesson, D. B. (2014). The extraterritoriality of eu data privacy law its theoretical justification and its practical effect on u.s. businesses. *Stanford Journal of International Law* 50(1), 53-102 p. 102

which are happening beyond their borders.[9] Claiming jurisdiction over states´ borders however, is more common for other legal fields than data protection law such as human rights law.[10] Nevertheless, the internet is borderless and accessible universally and in order to secure data and privacy protection in the worldwide web extraterritorial scope of jurisdiction is fundamental, and GDPR was laid down in order to adapt the legislation to correspond contemporary global web environment and the challenges and prospects it brings forth.[11]

The term jurisdiction means the state's ability to administrate the conduct of juridical persons as well as natural persons,[12] and it can be divided into four different categories thus, prescriptive, investigative, judicial and enforcement.[13] Although in principle jurisdiction should be practised in the state's territory there are specific principles under international law which provide the exercise of such powers.[14] Those principles from where the jurisdiction stems from are subjective territoriality, objective territoriality, nationality, passive personality, protective and universal principles.[15]

1.1.1. From Objective Territoriality Principle to Passive Personality Principle

GDPR's territorial scope is defined in article 3 of the regulation and states as follows:

"1. 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.

2. This Regulation applies to the processing of personal data of data subjects who are in the Union by controller or processor not established in the Union, where the processing activities are related to:

[9] Klabbers, J. (2017). *International law*. Cambridge: Cambridge University Press p. 105
[10] Ibid p. 105
[11] *Handbook on European data protection law*. (2018). *Supra nota* 1 p. 28
[12] Crawford, J. (2012). *Brownlies Principles of Public International Law 8th ed.* Oxford University Press. p.456
[13] Svantesson, D. B. (2013). *Supra nota* 7 p. 92
[14] Crawford, J. (2012). *Supra nota* 12. p. 456
[15] Svantesson, D. B. (2013) *supra nota* 7. p. 92

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

3. This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law."[16]

In order to understand the change in GDPR´s applicability a comparison between the principles of international law behind Data Protection Directive hereafter, DPD and GDPR is useful. There are differences in their territorial scope although both apply to companies seated outside of the EU.[17] DPD's scope was targeted on rather geographical factors of the apparatus used in the data processing.[18] This can be deducted from article 4 of the directive which states that if the equipment used for processing of personal data is situated in the EU the directive applies.[19] In comparison GDPR's scope refers to the targeting of data subjects situated in the EU.[20] The difference between the principles of territoriality in the legislation is that DPD's scope could be stated to fall within the principle of objective territoriality.[21] Objective territoriality means that a state can use jurisdiction on the basis that the action in question has caused harm or damage inside the territory of that state[22] whereas formatting of article 3 of GDPR seems to fit the definition of passive personality.[23] As to the definition passive territoriality means that the countries may exercise jurisdiction over actions that violate their citizens irrespective of the location of the occurrence.[24] Passive personality principle itself is often vastly disputed[25] due to its proneness to underestimate other states' legal systems[26] which may cause problems in the use of states' jurisdiction.

[16] GDPR Article 3
[17] Svantesson. D. B. (2013) *Supra nota 9* p. 94
[18] Svantesson. D. B. (2013) *Supra nota 9* p. 94
[19] Directive 95/46/EC of the European Parliament of the Council, 24 October 1995, *on the protection of individuals with regard to the processing of personal data and the free movement of such data* art 4
[20] Svantesson. D. B. (2013) *Supra nota 9 p. 94*
[21] Ibid p. 94
[22] Evans, M. D. (2006). *International Law* (Second ed.). Oxford University Press p. 344
[23] Svantesson, D. B. (2013). *Supra nota* 7 p. 94
[24] Shaw, M. N. (2003). *International Law* (Fifth ed.). Cambridge University Press p. 589
[25] Evans, M. D. (2006). *supra nota 22* p. 352
[26] Klabbers, J. (2017). *Supra nota* 9 p. 102

2. APPLICATION TO NON-EU COMPANIES

2.1. Extraterritorial Scope of Application

There are different approaches regarding the use of state's jurisdiction in the field of data protection law such as the applicability of the law could be combined with the enforceability of the legislation thus, the jurisdiction would be restricted only to those cases where it is possible to enforce the legislation in practice.[27] That is a rather strict view of the law which would in that case only rest on power.[28] However, there is a clear a connection between applicability and enforceability thus, both must be examined in order to understand connection with the enforcement of GDPR.

As it can be interpreted from Article 3 of the regulation the territorial scope of GDPR is extended outside the EU however, the application of data protection laws has changed during their development and implementation.[29] Practical examples can be found form case law. Multinational companies have tried to escape their responsibility and the jurisdiction of courts by pleading on their complex corporate structure.[30] In 2003 CJEU Lindqvist case was the first occasion where the application of EU data protection law outside of EU needed to be assessed.[31] What was important in the case is the fact that Data Protection Directive would have been applied to the entire internet and made it subject to EU data protection laws[32] which resulted in non-application of the Directive.[33] However, this approach has changed and there is a common movement towards jurisdictional overextension.[34]

---

[27] Kuner, C. (2015). Extraterritoriality and regulation of international data transfers in EU data protection law. *International Data Privacy Law,* Vol. 5, No, 4, 235-245 p. 236
[28] Ibid p. 236
[29] Ibid p. 236
[30] Wright, D., & De Hert, P. (2016). *Enforcing Privacy: Regulatory, legal and technological approaches*. Springer p. 217
[31] Kuner, C. (2014). The European Union and the Search for an International Data Protection Framework. *Groningen Journal of International Law, 2*(2) 55-71 p.55.
[32] Kuner, C. (2015). *Supra nota* 27 p. 237
[33] Ibid p. 237
[34] Svantesson, D. J. (2015). The Google Spain Case: Part of a Harmful Trend of Jurisdictional Overreach. *RSCAS.* 45 1-21 p.5

The contemporary approach to the territorial application of EU data protection law was verified in practice in the Google Spain case[35] where CJEU was able to claim jurisdiction over Google although arguments trying to flee form courts' jurisdiction were presented.[36] In the case a Spanish national Mario Costeja González complained to the Spanish Data Protection Supervisor since information which he considered as irrelevant and outdated was yet found from Google search engine.[37] The information was first published by a Spanish newspaper La Vanguardia and concerned the auctioning of immovable property related to the seizure of social security claims.[38] He claimed that La Vanguardia and Google Spain or Google Inc. are obliged to remove or conceal his personal information so that such information could no longer appear in Google's search results. [39]The seizure directed at him had been solved many years ago and the reference to it was no longer relevant.[40] The Spanish Data Protection Agency found that La Vanguardia was not guilty since the magazine had complied with all the legal requirements regarding the publishing of such information, however Google's involvement with the data processing resulted in liability of removal of the content.[41] Internet Searching Engines irrespective of the place of their actual location can be subject to EU law since they operate via their establishment located in EUs territory.[42] As a result, Google appealed against the decision.[43] The case was referred to CJEU by the Spanish National High Court.[44] CJEU ruled that Google in the case was found as a controller according to article 2(d) of DPD.[45] In addition, the actions of Google were determined as data processing of personal data in the meaning of article 2(b) of DPD.[46] As for Google Spain the inextricable link was found between Google Spain and Google Inc. since it was defined to be an establishment of its parent company of Google Inc.[47] The link made available the extraterritorial application of EU data protection legislation thus, DPD since data processing was executed by the establishment of the data controller.[48] Same ample perception of data controller was also

[35] Bu-Pasha, S. (2017). Cross-border issues under EU data protection law with regards to personal data protection. *Information & Communications Technology Law, 26*(3), 213-228 p. 216
[36] Wright, D., & De Hert, P. (2016). *Supra nota* 30 p. 217
[37] Court Decision, 13.5.2014, Google Spain, EU:C:2014:317, C-131/12, point 14
[38] Ibid point 14
[39] Ibid point 15
[40] Ibid point 15
[41] Ibid point 63
[42] Ibid point 40
[43] Synodinou, T., Jougleux, P., Markou, C., & Prastitou, T. (2018). *Eu Internet Law: Regulation and enforcement*. Springer. p. 101
[44] Google Spain 13.5.2014 C-131/12 *Supra nota* 37
[45] Google Spain 13.5.2014 C-131/12 *Supra nota* 37parapragph 43
[46] Ibid point 28
[47] Ibid point 47
[48] Ibid point 43

established in case Wirtschaftsakademie Schleswig Holstein, and both of these judgements legitimize broader application of the interpretation in GDPRs scope.[49]

2.2. EDPB Guidelines

Since The GDPR came in to effect in 25th of May 2018, there has been uncertainty about the application of the regulation with respect to Non-EU seated companies and there are various writings available to guide businesses to asses whether they fall under the scope of application and are required compliance with the Regulation. The sanctions of non-compliance are extensive;[50] thus, the administrative fines may raise up to 10 000 000 euros, and as far as undertakings are concerned to 2% of their total yearly revenue from the previous fiscal year.[51] Depending on the infringement the administrative fines can increase up to 20 000 000 euros and regarding undertakings to maximum of 4% of the total annual revenue. [52] In that regard, the companies both in the EU as well as outside the area have taken compliance with the regulation seriously.

European Data Protection Board (EDPB) was established to substitute The Article 29 Working Party and has many of the same functions as its predecessor.[53] EDPB has issued guidelines regarding the application of article 3 in November 2018[54] As to Non-EU companies the issues with respect to the application have been clarified although some issues may still remain. If Non-EU based companies' data processing falls within GDPR's scope of application and incurs non-compliance, such businesses are under the risk of big administrative fines. EDPB recommended to the interpretation an approach with three main criteria which must be taken into account when assessing the applicability of Article 3 of the Regulation.[55]

[49] Finck, M. (2018, November 16). Google v CNIL: Defining the Territorial Scope of European Data Protection Law. Accessible:https://www.law.ox.ac.uk/business-law-blog/blog/2018/11/google-v-cnil-defining-territorial-scope-european-data-protection-law 17 February 2019
[50] Voigt, P., & Von Dem Bussche, A. (2018). *Eu General Data Protection Regulation (GDPR): A practical guide*. S.l.: Springer International Publications p. 210
[51] Regulation (EU) 2016/679 of the European Parliament and of The Council, 27 April 2016, *General Data Protection Regulation* art 85
[52] Ibid art 85
[53] Petrovici, A. N. (2018, May 25). Europe's new data protection rules and the EDPB: Giving individuals greater control. Accesible: https://edpb.europa.eu/news/news/2018/europes-new-data-protection-rules-and-edpb-giving-individuals-greater-control_en 18 February 2019
[54] Guidelines 3/2018 on the territorial scope of the GDPR (Article 3) European Data Protection Board p. 1
[55] Ibid p. 3

2.2.1. Establishments in the EU

The first matter to be taken into consideration is the definition of an establishment. There is no clear definition of establishment in the regulation[56] although guidance can be deducted from recital 22 which states that an establishment requires effective and real action which is executed via stable arrangements.[57] The manner how it is executed is not decisive. It can be established in several ways such as through legal person, branch or subsidiary.[58] In practice it means that a company with only one employee or agent being present in the territory of EU may provoke GDPR to apply.[59] A Similar approach can be found in CJEU case law.[60] Although such an approach may seem relatively large-scale to Non-EU companies, EDPB clarifies that accessibility of a web site in the territory does not evoke the application alone.[61]

2.2.2. Processing of data

The second factor in the determination of whether GDPR applies to non-EU based companies relates to processing. Significant factor about the processing is that the EU establishment itself does not have to carry out the processing, on the contrary it can be executed by controller or processor not seated in the union and yet still fall under the scope of application provided that it is realized in a way that there is an inseparable link between the actions.[62] Such an approach was found already in Google v Spain case while DPD was still in force.[63] The last criterion for application is the affirmation that the localization of data processing is an irrelevant factor when detecting whether or not the processing is executed by an EU establishment.[64]

[56] Ibid p.5
[57] Regulation (EU) 2016/679 *Supra nota* 51 Recital 22
[58] Guidelines 3/2018 *supra nota* 54 p. 5
[59] Ibid p.5
[60] Court decision, 5.6.2018 Wirtschaftsakademie Schleswig-Holstein, EU:C:2018:388 (C-210/16)
[61] Guidelines 3/2018 *Supra nota* 54 p. 5
[62] Ibid p. 6
[63] Court Decision, 13.5.2014, Google Spain *Supra nota* 37 point 47
[64] Guidelines 3/2018 *Supra nota* 54 p. 8

2.2.3. Targeting of data subjects in EU

As for companies outside the EU article 3 and its format and with that regard, application has resulted in different interpretations and probably the most complicated issue of article 3 has been targeting of consumers.[65] One topical issue about targeting is that how to determine whether targeting of data subjects in EU occurs as well as the broadness of the conception thus if targeting occurs it may lead to an interpretation that it is directed widely to different Member States or countries in general, or no countries at all.[66]

According to the guidelines targeting, expands the application beyond the establishment criteria; thus, a company without an establishment in the EU may still fall into the scope of application due to targeting.[67] Determinative factor whether or not GDPR applies is the physical localization of the data subject regardless of his or her citizenship.[68] When specifying the location of the data subject, it must be assessed at the actual occurrence of potential provoking action hence, the data subject must be in the territory at the time of the occurrence of the action that may evoke the regulation to apply. [69]

Article 3(2) refers to the providing of goods and services.[70] The Defining factor is not relied upon whether a payment happens, on the contrary, a mere offering may trigger the application.[71] The intention of a processor or a controller must be assessed as well concerning the offering.[72] In addition, a link between both conducts offering as well as processing must be found. There are a variety of factors which help to evaluate whether there is a link provided in the guidelines which include among other things currency and language used in the offering.[73]

[65] Madge, R., & Madge, R. (2018, May 12). GDPR's global scope: The long story. Accesible: https://medium.com/mydata/does-the-gdpr-apply-in-the-us-c670702faf7f 18 February 2018
[66] Svantesson, D. J. (2015). Extraterritoriality and targeting in EU data privacy law: The weak spot undermining the regulation. *International Data Privacy Law, 5*(4) 226-234 p. 228
[67] Guidelines 3/2018 *Supra nota* 54 p. 13
[68] Ibid p.13
[69] Ibid p.13
[70] Regulation (EU) 2016/679 *Supra nota* 51 Art 3(2)
[71] Guidelines 3/2018 *Supra nota* 54 p. 14
[72] Ibid 14-15
[73] Ibid 15-16

Concerning monitoring regardless of no clear intention to target found, yet still "monitoring" in the meaning of article 3(2) b means that either the controller or the processor has a clear aim for the accumulation of data as well as for the reutilisation later on.[74] Such intentions for the utilization of data must be taken into account.[75]

2.2.4. Obligation to assign an EU representative

In addition, concerning Non-EU companies both controllers and processors depending on the situation, provided that they fall within the scope of GDPR have an obligation to nominate a representative in the Union in order to comply with article 3(2).[76] However, they can be freed from the responsibility to do so, if they fall in with article 27 criteria thus, if the processing is executed by a public body or authority, or when the processing cannot be categorised as extensive or considerable, and is not related to any special categories of data nor criminal sentences or violations.[77] Additionally, the handling of data as referred is not defined as dangerous to a natural person whose data is being processed.[78] As to the representative in the light of article 3(1)'s establishment criterion, representatives are not considered as establishments nor having equal effect as DPOs in the Union.[79]

[74] Ibid p.18
[75] Ibid p.18
[76] Ibid p. 19
[77] Regulation (EU) 2016/679 *Supra nota* 51 Art 27
[78] Guidelines 3/2018 *Supra nota* 54 p. 21
[79] Ibid p. 20

3. MEANS OF ENFORCEMENT OF GDPR AND PROBLEMS REGARDING THEM

3.1. The Importance of Data Protection Authorities in Enforcing GDPR

Before assessing DPAs' duties, it must be taken into account that before GDPR and harmonization of data protection laws in the EU, there were differences between the enforcement of DPD between the Member States because there had to be space left for countries to implement DPD.[80] One major issue was that there was not a clear statement in DPD that DPAs were able to inflict fines;[81] thus, both courts as well as DPAs imposed sanctions which were consecrated in administrative law and criminal law and the type of sanctions and varied from monetary sanctions to non-monetary sanctions.[82] All the more, nowadays the most essential role regarding implementation is in the Data Protection Authorities hands. DPA's have powers both to investigate and also to enforce punishments.[83] In terms of investigative powers DPAs are able to assign both the controller and the processor of personal data, to provide information which is necessary to fulfil investigative operations, perform inquiries in the form of data protection checks and also to inform the processor or controller about the alleged breach of the regulation.[84] Furthermore, DPAs have the right to access personal data and material which is essential for the execution of their obligations as a supervisory authority and also to be able to have access to the equipment and other material used for data processing by the processor or controller.[85]

Regarding corrective powers supervisory authorities are able to warn that the intended processing executed by controller or processor is likely to contravene with GDPR's provisions as well as give notice when processing operations have been in breach with the provisions of the Regulation.[86] In terms of compliance with data subjects rights the DPA can request for compliance.[87] Also when

[80] Giurgiu, A., & Larsen, T. A. (2016). Roles and Powers of National Data Protection Authorities. *European Data Protection Law Review, 2*(3), 342-352 p. 344
[81] Ibid p. 344
[82] Ibid p. 334
[83] Ibid p. 334
[84] Regulation (EU) 2016/679 *Supra nota* 51 art 58
[85] Ibid art 58
[86] Ibid art 58
[87] Ibid art 58

the processing operations are not in accordance with the articles of the Regulation, DPAs can order processor or controller to correct that and set a time period for the execution of necessary changes.[88] In case of breach of the data subjects rights DPAs can command data controller to inform about such breach.[89]Bans or restrictions for processing either perpetual or temporary are also in the hands of authorities additionally to order erasure or rectification of data.[90] They can also withdraw certification and prohibit certification body to issue certifications and lastly impose administrative fines and prohibit data transfers to a recipient in a third country or to an international organisation.[91]

As it can be concluded from the list of tasks and powers supervisory authorities have, they are rather extensive.[92] In terms of effective enforcement, DPAs must execute their powers in a lawful manner.[93] DPAs tasks can be seen as overreaching the common conception of strict enforcement duties[94] thus, DPAs have for example consultative tasks as well. The tasks however are lacking in sufficient directions or guidelines on how are they related.[95] Another missing factor is an assurance that they will be executed effectively and lawfully. [96] Also there are doubts concerning the capability of DPAs to enforce due to lacking experience of such operations as well as a result of budgetary shortage and an absence in qualification.[97] DPAs list of extensive powers in terms of investigation as well as enforcement makes them as genuine regulators.[98] The actual application and therefore, the legitimacy of enforcement as well might remain inconsistent because of the resources of DPAs to actually investigate does not correspond to the number of businesses not complying with GDPR.[99]

[88] Ibid art 58
[89] Ibid art 58
[90] Ibid art 58
[91] Ibid art 58
[92] Team, I. P. (2017). *EU General Data Protection Regulation (GDPR): An Implementation and Compliance Guide - Second Edition*. IT Governance. p. 283
[93]Hijmans, H. (2018).How to Enforce the GDPR in a Strategic, Consistent and Ethical Manner? *European Data Protection Law Review, 4*(1), 80-84 p.82
[94] Ibid p. 81
[95] Ibid p. 82
[96] ibid p. 83
[97] Eijk, N. V. (2017). About Finding Practical Solutions (Without the GDPR). *European Data Protection Law Review*, 3(3), 310-312. p. 312
[98] Ibid p. 312
[99] Svantesson, D. J. (2018). European Union Claims of Jurisdiction over the Internet - an Analysis of Three Recent Key Developments. *Journal of Intellectual Property, Information Technology and E-Commerce Law,9*(2) 113-125. p. 118

3.1.2. The Interaction between EU Representatives and Data Protection Authorities

EU Representatives are not a new concept regarding EU data protection laws.[100] Data protection directive contained an obligation to appoint an EU representative in the area of EU.[101] However, the provision was not completely trouble-free since irrespective of the obligation; there were no punishments for non-compliance.[102] Thus, if a non-EU company did not appoint a representative it was left up to the Member States to decide how to proceed with the sanctions.[103] Assigning a representative was not considered as a prerequisite nor had an effect on the lawfulness of data protection operations[104] When there were no general sanctions determined in the directive it affected the efficiency of enforcement.[105] Generally representatives were seldom appointed and DPAs did not draw attention to the failure of appointing them.[106]

The obligation to assign a representative has not changed in GDPR.[107] However, as the laws have been harmonized the issue of different implementation of articles has passed as the regulation is directly applicable.[108] As stated in article 27 of the Regulation non-EU based businesses are obliged to assign a representative in the Union.[109] In terms of enforcement according to article 83 failure to appoint a representative is subject to sanctions[110] thus, at least in this area the actual enforceability could have since improved. Companies are more likely to appoint a representative when there is a sanction in case of non-compliance[111] and no room for the implementation of the articles in the countries.

In terms of EU based companies, there is an obligation according to 37 to appoint a Data Protection Officer or Data Protection Team.[112] DPOs and EU representatives have different duties.

---

[100] Kuner, C., & Kuner C. (2012). *European data protection law: Corporate compliance and regulation.* Oxford: Oxford University Press. p. 134
[101] Ibid p. 134
[102] .Ibid p. 134
[103] Ibid p. 134
[104] Ibid p. 134
[105] Ibid p. 134
[106] Ibid p. 134
[107] Regulation (EU) 2016/679 *Supra nota* 51 Art 27
[108] Pormeister, K. (2017). Genetic data and the research exemption: Is the GDPR going too far? *International Data Privacy Law,7*(2), 137-146. p. 138
[109] Regulation (EU) 2016/679 *Supra nota* 51 art 27
[110] Regulation (EU) 2016/679 *Supra nota* 51 art 83
[111] Kuner, K. (2015) *Supra nota* 24 p. 237
[112] Regulation (EU) 2016/679 *Supra nota* 51 art 37

The difference between DPOs and EU representatives can be found in their legal obligations. DPOs are designated to facilitate compliance with the Regulation thus, they provide guidance and consultation in terms of compliance inside companies or organisations who carry out data processing activities. [113] The appointment is obligatory if a public authority is responsible of executing data processing, if the processing is large scale or is related to sensitive data.[114]
In other cases, DPO's assignment is not obligatory; however, companies can designate one if desired. [115]

As to EU representative, the role is distinct. Representatives are appointed to act on behalf of the companies seated outside the Union; thus, represent the businesses.[116] They must either have a personal residence in the EU or business residence in the territory.[117] There are no preconditions for proficiency nor association of the representatives thus, the companies and organisations can freely choose a representative.[118] In addition, there is no restriction for how many controllers or processors the representative can be appointed for however, there cannot be any conflicts of interest in such situations. [119] The representative must be designated for one EU country where data processing occurs and that is sufficient for compliance with the regulation thus, there is no obligation to assign various representatives in several EU Member states where the processing action takes place.[120]

Appointing a representative can be seen as a burden form the viewpoint of controllers and processors;[121] however, the connection with representatives and DPAs is an important factor in terms of enforcement actions against them. Representatives must be available when needed not only for the DPA but also for the data subjects.[122] Comparing DPOs and representatives the first mentioned have protection against prosecutions either from data subjects or DPAs however, the same doesn't apply for EU representatives.[123] They are the ones responsible in case of non-

[113] *Handbook on European data protection law*. (2018). *Supra nota* 1. p. 175
[114] Ibid p. 175
[115] Ibid p. 175
[116] Regulation (EU) 2016/679 *Supra nota* 51 art 27
[117] Ibid art. 27
[118] Ibid art 4 (17)
[119] Voigt, P., & Von Dem Bussche, A. (2018) *Supra nota 49*. p. 134
[120] Ibid p. 134
[121] Kuner, C., & Kuner C. (2012) *Supra nota* 100 p. 131
[122] Shaw, T. (23 November 2018) How do the DPO and EU representative interplay? Accessible: https://iapp.org/news/a/how-do-the-dpo-and-eu-representative-interplay/ 3 March 2018
[123] Ibid

compliance and when the controller or processor is unable to be contacted thus, the representative can be the named party in terms of actions taken against the controller or processor.[124] and in addition liable for possible penalties imposed on them.[125] At the same time they are a party that the EU can achieve effective and legitimate jurisdiction over. [126] In case of Non-EU courts do not cooperate with EU authorities with respect to enforcing regulations fines or other sanctions, the enforcement action may persist territorial despite of extraterritorial application[127] and therefore the function of the representative is important.

Regarding representatives' vital role as noted the company can freely choose their representative and the representatives have no qualification requirements.[128] They merely must have either personal or business residence in the territory of EU[129] They can at least to some extent be compared to DPOs. DPOs have conditions regarding their skills however, GDPR does not guarantee any indications how to safeguard that DPOs have all these skills.[130] Even though the tasks of DPOs and representatives are different still some verification could be introduced to the representatives as well in order to assure proper compliance.

3.2. Recognition of Judgements and their Enforcement in Third Countries

The enforcement jurisdiction is not a disputed issue when a state uses its jurisdiction in its own territory however, problems may arise when it is used in extraterritorial manner.[131] Thus, enforcement relies upon a principle, according to which a state cannot enforce its laws in another states territory unless, the state which is the target of enforcement measures has given a consent to

[124] Regulation (EU) 2016/679 *Supra nota* 51 Recital 80
[125] Kuner, C. (2012) The European Commission's Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection Law. *Bloomberg BNA Privacy and Security Law Report,* 1-15 p. 12
[126] Shaw, T. (23 November 2018) *Supra nota* 122
[127] Kohl, U. (2007). Jurisdiction and the Internet. *Jurisdiction and the Internet*. p. 25
[128] Determann, L. (12 June 2018) Representatives under Art. 27 of the GDPR: All your questions answered. Accessible: https://iapp.org/news/a/representatives-under-art-27-of-the-gdpr-all-your-questions-answered/ 12 March 2018
[129] Regulation (EU) 2016/679 *Supra nota* 51 art 27
[130] Lachaud, E. (2014). Should the DPO be certified? *International Data Privacy Law, 4*(3), 189-202 p. 192
[131] Crawford, J. (2012). *supra nota* 12 p. 478

that.[132] In examining enforcement of legislation the most important factor may be the enforceability rather than enforcement concretely especially in cross-national framework, thus the main factor is assertion of foreign law.[133]

In Civil and administrative jurisdiction context enforcement in extraterritorial manner is largely based on both recognition of judgements and their implementation in foreign countries.[134] In addition, extraterritorial claims are required to in spite of potential difficulties in de facto enforcement because it demonstrates that companies regardless of their location are pursued to be handled in a similar way.[135] They may also have an influence on companies despite of actually being enforced because they can have a deterrent impact.[136]

The new data protection reform was established in 2014.[137] The problem which had arisen before data reformation was that due to increasing usage of cloud computing services more data was retained as well as processed outside EU which resulted in lack of effective enforcement of both national and EU privacy legislation.[138] Enhancing its effectiveness was one of the grounds for data protection reformation.[139] When the EU moved from DPD to GDPR the change affected also enforcement mechanisms as well as procedural matters and made them more encompassing.[140] Nevertheless, in cyberspace the implementation may not be as effective as in physical world thus, the power of states to enforce legislation is weaker[141] and order to secure its effectiveness collaboration between states as well as private bodies is essential.[142] GDPR promises improvement in collaboration.[143] The risk of sanctions being enforced against companies affects their behaviour as well and is an effective way of having an impact on the data processing executed by

[132] Ibid p. 479
[133] Kohl, U. (2007). *Supra nota 127* p. 111
[134] Crawford, J. (2012). *Supra nota* 12 p. 83
[135] Wright, D., & De Hert, P. (2016). *Supra nota* 30 p. 201
[136] Ibid p.201
[137] Kulesza, J. (2014). USA Cyber Surveillance and EU Personal Data Reform: PRISM's Silver Lining? *Groningen Journal of International Law, 2*(2), 72-89 p. 85
[138] Ibid p. 85
[139] Ibid p. 85
[140] Wagner. J. (2018). The transfer of personal data to third countries under GDPR: when does a recipient country provide an adequate level of protection? *International Data Privacy Law* Vol. 8, No. 4 318-337 p. 335
[141] *Global networks and local values: A comparative look at Germany and the United States*. (2001). Washington: National Academy Press p.11
[142] Hert, P. D., & Czerniawski, M. (2016). *Supra nota* 4 p. 239
[143] Buttarelli, G. (2016). The EU GDPR as a clarion call for a new global digital gold standard. *International Data Privacy Law, 6*(2), 77-78.p. 77

companies[144] there is still a need to further examine whether such claims can be enforced effectively.

3.2.1. The New Jurisdictional Regime of GDPR

Concerning data protection GDPR is article 79(2) determines a new jurisdictional regime.[145] In the time of application of DPD the judicial jurisdiction was determined by Brussels I Regulation however, GDPR has changed this approach and now constitutes an individual legal regime for data privacy-related issues.[146] It could be concluded that GDPR would create more harmony as well as legal certainty as opposed to the old DPD's scope where each Member State had slightly different approaches to enforcement as well as judicial culture.[147] There is a need to discuss article 79(2) in order to further reflect the effect on Non-EU based data controllers and processors. However, it must be noted that enforceability of legislation in international framework is not only combined with jurisdictional claims yet the link between adjudicatory jurisdiction and enforcement is not to be overlooked.[148]

The basic rule of Brussels 1a Regulation is that the defendant can sue where he or she is domiciled and that is the base for international disputes in the EU.[149] This includes also data privacy- related breaches[150] however, GDPR enables the data subject to sue also where the processor or controller has its establishment as well as in the place where the data subject has his or her habitual residence.[151] Brussels I on the other hand enables the data subject to sue in Member State where

[144] Wright, D., & De Hert, P. (2016). *Supra nota* 30 p. 201
[145] Regulation (EU) 2016/679 *Supra nota* 51Art 79(2)
[146] Revolidis, I. (2017). Judicial Jurisdiction over Internet Privacy Violations and the GDPR: A Case of Privacy Tourism? Masaryk University Journal of Law and Technology, 11(1), 7-37.p.12
[147] Albrecht, J. (2016). How the GDPR will change the world. European Data Protection Law Review (EDPL) 2(3), 287-289 p. 288
[148] Revolidis, I. (2017). *Supra nota* 146 p .22
[149] Ibid p. 21
[150] Ibid p. 21
[151] Regulation (EU) 2016/679 *Supra nota* 51 Art 79(2)

his centre of interests are under article 7(2).[152] In the context of foreign legislation problems arise since countries may have a different approaches to jurisdiction in the internet and may not be in mutual consensus with the Brussels I regulations law regime nor with GDPRs regime.[153]

3.2.2. Non-enforcement of Foreign Public law

Although DPAs are in an important role in the enforcement of GDPR problems may still arise due to their role as public authorities.[154] This may lead to "public law taboo" which means the rejection of enforcement of external public law.[155] The role of DPAs as public authorities could be seen more firm in GDPR now than in DPD because of the wording of GDPR well states their status as public authorities.[156] Many examples of public law taboo can be found in U.S. tax laws or antitrust law[157] however, whether in terms of tax laws or data protection laws if courts abroad are inclined to enforce foreign judgements it makes the law more effective.[158] The reason why public law taboo and refusal of enforcement of foreign laws can be justified is that commonly public law is exercised inside state's territory[159] however, private individuals may now take enforcement action directly against violators in accordance with articles 79 and 82 of GDPR.[160] Usually private rights have tendency to be enforced in other countries more likely than DPAs actions.[161]

This is a significant advancement in EU data protection laws since it makes it easier for private persons to execute their rights.[162] This could be seen as counterbalance to the problem arising from DPAs status and the possibility of non-enforcement and non-recognition of judgements in third countries.[163] However, it should be taken into account that although generally private rights might

[152] Regulation (EU) No 1215/2012 of the European Parliament and of the Council, 12 December 2012 on jurisdiction and the recognition and enforcement of judgements in civil and commercial matters art 7(2)
[153] Ibid p. 23
[154] Brkan, M. (2015) Data protection and European private international law: observing a bull in a China shop, *International Data Privacy Law*, Vol. 5, No. 4, 257–278 p. 262
[155] Dodge, W. S. (2002). Breaking the public law taboo. *Harvard International Law Journal* 43(1), 161-236 p. 161
[156] Brkan, M. (2015) *Supra nota* 153 p. 262
[157] Dodge, W.S. (2002) *Supra nota* 155 p. 162
[158] Ibid p. 162
[159] Ibid p. 162
[160] Bakhoum, M. (2018). *Personal Data in competition, Consumer Protection and Intellectual Property Law: Towards a Holistic Approach?* Springer. p. 324
[161] Wright, D., & De Hert, P. (2016) *Supra nota* 30 p. 201
[162] Bakhoum, M. (2018) *Supra nota* 160 p. 324
[163] Ibid p. 326. 201

be enforced more likely all countries do not recognise privacy enforceable under private law.[164] In addition resources in many situations are rather used in domestic issues than promoting cross-border enforcement actions and cooperation.[165]

3.2.3. Different Approaches to Data Protection Laws

Before GDPR came into force the actual enforcement against big U.S. based multinational companies such as Google or Facebook have by Data Protection Authorities has resulted in relatively limited penalties although,[166] DPAs brought cases actively against these companies. [167] The problem with DPD's applicability and by that way also enforceability suffered from the limitations in regional legislation which was adapted according to DPD.[168]One of GDPR's objects was to coordinate data protection legislation in the Europe however, at the same time it creates standards for data protection and the regulation facilitates EU's possibilities to encourage states globally to adopt its values.[169]

One problem relating to enforcement is different approaches to data privacy between EU and third countries for example the grounds of the laws are different in EU and the U.S.[170] As explained the right to privacy is a fundamental right in the EU[171] and there must be a clear consent from the data subject in order to carry out processing[172] however, in the U.S. the Constitution does not include the right to privacy[173] and there is no need for a consent in case of subsequent use of data.[174] Different approach to privacy protection can be seen in various cases where EU DPAs have taken

[164] Wright, D., & De Hert, P. (2016) *Supra nota* 30 p.195
[165] Brkan, M. 2015 *Supra nota* 153 p. 335
[166] Houser, K., & Voss, W. G. (2018). GDPR: The End of Google and Facebook or a New Paradigm in Data Privacy? *Richmond Journal of Law & Technology,* Vol. 25, No, 1, 1-109 p. 7
[167] Ibid p. 7
[168] Ibid p. 8
[169] Stronger protection, new opportunities (24.1.2018) – Commission guidance on the direct application of the General Data Protection Regulation as of 25 May 2018 p. 5 Accesible: https://ec.europa.eu/commission/sites/beta-political/files/data-protection-communication-com.2018.43.3_en.pdf March 5 2018
[170] Baumer, D. L., Earp, J. B., & Poindexter, J. (2004). Internet privacy law: A comparison between the United States and the European Union. *Computers & Security, 23*(5), 400-412. P. 400
[171] *Handbook on European data protection law*. (2018) *supra nota* 1 p. 17
[172] Ibid 1 p. 111-112
[173] Solove, D. (2010) *Understanding privacy.* Harvard University Press. p. 2
[174] Houser, K., & Voss, W. G. (2018) *Supra nota* 166 p. 24

enforcement action against big U.S. companies such as Google.[175] For example in 2014 Google had used data which it had obtained from data subjects' Gmail accounts in order to provide targeted advertisement to the users.[176]However, Italian DPA brought enforcement action against Google since the information was used for subsequent processing without data subjects' consent.[177] Italian DPA requested that information about the purpose of data processing must be provided and consent form data subjects must be obtained.[178] This case among the others confirmed that subsequent processing is not allowed without consent under EU data protection law.[179]

The same can be examined also when different rights contradict for example there is a conflict between U.S. freedom of expression and right to be forgotten determined in EU data protection law which could lead to non-enforcement of EU orders and non-cooperation.[180] The U.S. has its own concept regarding jurisdiction over the internet which can affect enforceability of GDPR because the approach to internet jurisdiction may not confront with the one of GDPRs, determined in article 72(2).[181] The U.S. viewpoint to Freedom of Speech might create issues in recognition of foreign enforcement actions since the U.S. Privacy act enables the courts to deny recognition of foreign judgements in case if the judgement does not meet with the U.S. approach to freedom of speech which is determined in The American Constitution.[182]

3.2.4. Europeanisation of Data Protection Laws and Cooperation between Countries

Some of the third countries have developed privacy laws which are quite similar or at least laws which are in mutual understanding such as Argentina, Israel, and Canada.[183] This strengthens EUs position in the data protection field globally. Also Japan has regulated its data protection laws to

[175] Ibid p. 30
[176] Ibid p.30
[177] Houser, K., & Voss, W. G. (2018) *Supra nota* 166 p. 31
[178] Rauhofer, J. (2015). Of Men and Mice: Should the EU Data Protection Authoritiess Reaction to Googles New Privacy Policy Raise Concern for the Future of the Purpose Limitation Principle? *European Data Protection Law Review (EDPL), 1*(1), 5-15. p. 12
[179] Houser, K., & Voss, W. G. (2018) *Supra nota* 166 p. 33
[180] Ambrose, M. L. (2014). Speaking of forgetting: Analysis of possible non-EU responses to the right to be forgotten and speech exception. *Telecommunications Policy, 38*(8-9), 800-811. p. 809
[181] Revolidis, I. (2017). *Supra nota* 146 p. 23
[182] Ibid p. 23
[183] Kuner, C. (2009). An international legal framework for data protection: Issues and prospects. *Computer Law & Security Review,* 25(4), 307-317 p. 310

be in accordance with GDPR in May 2017.[184] Before privacy law amendment the EU did not consider Japan as having an adequate level of protection according to EU Commission's white list. However, the modifications in Japan's privacy laws were able to bring the country amongst the listed countries.[185] Significant change in the reformation was establishing of Personal Information Protection Commission which has as its primary task to ensure establishment and enforcement of privacy laws.[186] The reformation helps also EU to enforce legislation since there is a mutual consensus in the privacy laws.

Furthermore, when assessing article 45 of GDPR which focuses on transfers which are based on an adequacy decision[187] it sets requirements which countries must meet in order to correspond EUs level of protection of personal data.[188] This also means that enforcement and procedural requirements must be met.[189] Even though the EU does not require that laws of countries would be modified to be identical to the ones in EU but to provide adequate level of protection, however it might require third countries to adjust their laws and enforcement mechanisms to correspond EUs standards.[190]

In order to make GDPR actually enforceable and bring all of the enforcing and implementing actors together DPAs, EDPB, data subjects as well as DPOs and European Commission not to forget controllers and processors should cooperate.[191] Territorial scope of GDPR is remarkably extensive and implementation becomes difficult without sufficient collaboration and coordination between the actors. At the same time it encourages businesses as well as organisations to a more open way of processing.[192] GDPR alleges stronger collaboration among both authorities and data controllers and processors[193] however, cooperation can result in raised bureaucratic burden which

[184] Albrecht, J. (2016). Supra nota 147 p. 288
[185]Takase, K. (n.d.). GDPR matchup: Japan's Act on the Protection of Personal Information. Accessible: https://iapp.org/news/a/gdpr-matchup-japans-act-on-the-protection-of-personal-information/ 5 March 2018
[186] Ibid
[187] Regulation (EU) 2016/679 *Supra nota* 51 art 45
[188] Brkan, M. (2015) *Supra nota* 153 p. 335
[189] Wagner, J. (2018) *Supra nota* 65 p. 335
[190] Brkan, M. (2015) *Supra nota* 153 p. 335
[191] Kersten, J. (2018, August 09). Who's Enforcing GDPR? - European Data Protection Board Accessible: https://kirkpatrickprice.com/blog/whos-enforcing-gdpr 5 March 2018
[192] Ibid
[193] Buttarelli, G. (2016). *Supra nota* 143. p. 77

can create more costs and thus, require more resources[194]which DPAs already lack.[195] Resources are required especially when the matter relates to cross-border enforcement actions and cooperation of different authorities in third countries.[196]

3.1. Implicit and Deterrent effect of Enforcement Actions

Although it can be argued if strong type of enforcement is even needed because law can be seen as an element of how to rule behaviour, and court actions are not always necessarily required.[197] Generally, there are two main reasons for strong enforcement of legislation first of which is when there is a possibility of strong sanctions it promotes companies to act in a desirable way, and secondly the power must be used or else the enforcement power will eventually fail to fulfil its purpose.[198] The area of internet jurisdiction is itself complex in terms of enforceability and scholars have emphasised this issue for a long time.

The first enforcement notice where the company had no presence in EU was given by ICO UK to a Canadian company called AggerateIQ Data Services Ltd and required AIQ to terminate data processing operations relating to UK citizens' data relating which was collected from political organizations.[199] AIQ utilized the data in order to allocate relevant advertising towards people regarding politics.[200] The political organizations such as BeLeave contributed data to AIQ and political advertisement was focused on people in social media channels.[201] The first enforcement notice was based on article 3(2) of GDPR even though AIQ had no physical presence in the EU

[194] Barnard-Wills, D., Chulvi, C. P., & Hert, P. D. (2016). Data protection authority perspectives on the impact of data protection reform on cooperation in the EU. *Computer Law & Security Review,32*(4), 587-598 p. 596
[195] Leenes, R., Brakel, R. V., Gutwirth, S., & Hert, P. D. (2018). *Data protection and privacy: The internet of bodies*. Oxford: Hart Publishing. p. 239
[196] Wright, D., & De Hert, P. (2016). *Supra nota* 30. p. 201
[197] Svantesson, D. J. (2017). Solving the Internet jurisdiction puzzle. Oxford, United Kingdom: Oxford University Press.p. 130
[198] Hijmans, H. 2018. *supra nota* 93 p. 83
[199]Enforcement notice 24.10.2018 ICO v AggerateIQ Data Services Ltd point. 3 accessible: https://ico.org.uk/media/action-weve-taken/enforcement-notices/2260123/aggregate-iq-en-20181024.pdf 14 March 2018
[200] Ibid paragraph 5 and 6
[201] Ibid paragraph 6

however, according to article 3(2) if monitoring relating to data subjects' behaviour occurs in the EU GDPR applies.[202] The articles which were breached according to the notice were 5(a) – 5(c) and article 6 of the regulation[203] hence, there should have been a clear purpose for the data processing clearly informed to the data subjects, thus the processing was stated to be conducted in an unlawful manner.[204] In addition, transparency was neglected.[205] However, AIQ claimed that the scope of application was too broad regarding the facts yet retired the appeal later when ICO narrowed the scope of the enforcement notice.[206] The final notice included only special categories of data.[207] In the end AIQ accepted the notice when the scope was narrowed down and AIQ voluntarily removed the data.[208] Although the scope was narrowed down the risk for sanctions in case of non-compliance is high and ICOs requirements were voluntarily accepted.[209] Data Protection Authorities have the authority to issue enforcement notices, thus request compliance with the regulation which is a part of their corrective powers.[210] Regarding this case compliance was established even though in a narrower sense.[211]

In terms of enforcement there are other factors than direct ways of enforcement that can affect the matter one of which is reputational effect thus if breaking the law is seen as a morally negative factor the reputation of the lawbreaker is also affected.[212] Reputational factors and risks the in reputation may cause losses to the company[213] in addition to legal costs stemming from non-compliance. Therefore, not only direct and strong methods of enforcement should be taken into account when assessing it. Also considering the lack of resources for DPAs actions relatively high fines for violation of GDPR could be seen as deterrence.[214] In a situation where supervision is more efficient and thus, the chance of uncovering non-compliance is higher high fines are not

[202] Regulation (EU) 2016/679 *Supra nota* 51 art 3(2)
[203] Enforcement notice 24.10.2018 ICO v AggerateIQ *Supra nota* 198 paragraph 12
[204] GDPR articles 5(a)-5(c) and 6
[205] Enforcement notice 24.10.2018 ICO v AggerateIQ Supra nota 198 paragraph 12
[206] AggregateIQ challenges ICO jurisdiction (2018,October30). Accessible: https://globaldatareview.com/article/1175033/aggregateiq-challenges-ico-jurisdiction 15 March 2018
[207] Ibid
[208] Ibid
[209] ICO narrows first-ever GDPR enforcement notice. (2018, October 30). Accesible: https://globaldatareview.com/article/1176139/ico-narrows-first-ever-gdpr-enforcement-notice 15 March 2018
[210] Giurgiu, A., & Larsen, T. A. (2016) *Supra nota* 81 p. 348
[211] ICO narrows first-ever GDPR enforcement notice. (2018, October 30). *Supra nota* 209
[212] Svantesson, D. J. (2017). *Supra nota* 197 p. 131
[213] Aula, P. (2010). Social media, reputation risk and ambient publicity management. *Strategy & Leadership*, 38(6), 43-49. p. 44
[214] Leenes, R., Brakel, R. V., Gutwirth, S., & Hert, P. D. (2018). *Supra nota* 195. p 239

required.[215] Inversely when the possibility of uncovering non-compliance is lower the fines are likely to be higher to promote compliance.[216]

[215] Ibid p. 239
[216] Ibid p. 239

CONCLUSION

Regressing to the starting point of this research the aim of the thesis was to examine whether the enforcement of GDPR outside of EU could be executed efficiently and whether there are possible solutions for the lack of effective enforcement taking into account difficulties arising from the contemporary regulatory environment in the era of internet governance.

This paper hypothesised that the EU is not able to enforce its current broad extent data protection legislation in third countries effectively. After examining the problems which may arise from applying European legislation to third countries the results are complicated. For one part they support the view that the influence of European Data Protection law also affects data protection legislation outside the borders of the European Union and thus increasingly, countries are creating a similar type of legislation. Hence, the enforcement of GDPR could actually become easier. However, although many countries are developing similar laws, there might be a problem with non-recognition of judgements and enforcement since different rights such as freedom of speech in the U.S. and data privacy in the EU as may clash which can result in that problem.

Taking into closer consideration DPAs extensive tasks concerning supervision and enforcement, the fact that such a wide range of powers requires a lot of support both material and non-material creates problems in the enforceability of GDPR. Firstly, DPAs seem to have insufficient resources to execute their tasks in accordance with the broadness of the duties. In addition, their capacity to perform them is questionable due to the absence of experience.

Also in order for the enforcement to be sufficiently effective collaboration is needed for all of the actors in the field of data protection. Nonetheless, even though cooperation is essential, its realisation is not as simple as it seems. If processors and controllers abstain from cooperation with Data Protection Authorities, the stress is on the importance of EU representatives which companies in third countries must assign under GDPR. However, such demand is again emphasising the Eurocentric view of data protection legislation which may not be acknowledged in all countries

and it can result in non-enforcement. Also since there are no qualification requirements for the EU representatives, it can possibly affect the cooperation with DPAs.

Another issue are costs arising from growing demand for cooperation which can create encumbrance for administrative operations. This, may result in the need for more resources and in that way weaken the effectiveness of DPAs enforcement actions. Their role can be seen difficult because of their strong public authority position and even though public international law provides for principles for extraterritorial application of enforcement actions, foreign law is sometimes declined which results in that regard to non-effective enforcement. Thus, considering enforcement of GDPR in third countries from these perspectives it partly seems to lack effectiveness.

However, as for the possible solutions to solve the problems, the Regulation can still be functioning even though strong enforcement would not be fully effective. Implicit ways to affect the behaviour of companies in third countries may be the solution. Thus, strong enforcement although partly ineffective may not even be required. High fines for possible violations can affect companies to act in a desirable way which can be seen as an alternative for strong enforcement.

In case of violations still arise, the possibility of private enforcement actions provided in GDPR may help to reduce problems which stem from public law enforcement. It can counterbalance the issue of non-recognition and non-enforcement since private individuals can intervene themselves with the process. Such claims can have more potential to be enforced in third countries.

Many factors have improved from the Data Protection Directive's regime, and at least harmonization creates more certainty also in terms of enforcement. In order to conduct further research on this matter future court cases in this field will probably give more guidance to these questions in practice and evoke more issues to be considered. Furthermore, the effect of private enforcement actions in comparison to actions by DPAs can be seen more clearly in the future when more actions are taken against violators of data privacy.

LIST OF REFERENCES

Scientific Books:

1. Bakhoum, M. (2018). Personal Data in competition, Consumer Protection and Intellectual Property Law: Towards a Holistic Approach? Springer.

2. Brière, C., & Weyembergh, A. (2018). The needed balances in EU criminal law: Past, present and future. Hart Publishing.

3. Crawford, J. (2012). Brownlies Principles of Public International Law 8th ed. Oxford University Press.

4. Evans, M. D. (2006). *International Law* (Second ed.). Oxford University Press.

5. Klabbers, J. (2017). *International law*. Cambridge: Cambridge University Press.

6. Kohl, U. (2007). Jurisdiction and the Internet. *Jurisdiction and the Internet,* Cambridge University Press

7. Kuner, C., & Kuner, C. (2012). *European data protection law: Corporate compliance and regulation*. Oxford University Press

8. Leenes, R., Brakel, R. V., Gutwirth, S., & Hert, P. D. (2018). *Data protection and privacy: The internet of bodies*. Hart Publishing.

9. Shaw, M. N. (2003). *International Law* (Fifth ed.). Cambridge University Press.

10. Solove, D. (2010) *Understanding privacy.* Harvard University Press.

11. Svantesson, D. J. (2017). *Solving the Internet jurisdiction puzzle*. Oxford University Press

12. Synodinou, T., Jougleux, P., Markou, C., & Prastitou, T. (2018). *Eu Internet Law: Regulation and enforcement*. Springer.

13. Wright, D., & De Hert, P. (2016). *Enforcing Privacy: Regulatory, legal and technological approaches*. Springer

Scientific articles:

14. Albrecht, J. (2016). How the gdpr will change the world. *European Data Protection Law Review (EDPL)* Vol. 2, No, 4, 287-289.

15. Barnard-Wills, D., Chulvi, C. P., & Hert, P. D. (2016). Data protection authority perspectives on the impact of data protection reform on cooperation in the EU. *Computer Law & Security Review,* Oxford University Press Vol. 32, No, 4, 587-598

16. Baumer, D. L., Earp, J. B., & Poindexter, J. (2004). Internet privacy law: A comparison between the United
States and the European Union. *Computers & Security, 23*(5), 400-412.

17. Bu-Pasha, S. (2017). Cross-border issues under EU data protection law with regards to personal data protection. *Information & Communications Technology Law,* Taylor & Francis Vol. 26, No, 3, 213-228

18. Buttarelli, G. (2016). The EU GDPR as a clarion call for a new global digital gold standard. *International Data Privacy Law,* Oxford University Press Vol. 6, No, 2, 77-78

19. Dodge, W. S. (2002). Breaking the public law taboo. *Harvard International Law Journal* Vol. 43, No, 1, 161-236

20. Eijk, N. V. (2017). Forewords · About Finding Practical Solutions (Without the GDPR). *European Data Protection Law Review,* Vol. 3, No, 3, 310-312.

21. Hert, P. D., & Czerniawski, M. (2016). Expanding the European data protection scope beyond territory: Article 3 of the General Data Protection Regulation in its wider context. *International Data Privacy Law,* Vol. 6, No, 3, 230-243.

22. Hijmans, H. (2018). Discussion · How to Enforce the GDPR in a Strategic, Consistent and Ethical Manner? *European Data Protection Law Review,* Vol. 4, No, 1, 80-84.

23. Houser, K., & Voss, W. G. (2018). GDPR: The End of Google and Facebook or a New Paradigm in Data Privacy? *Richmond Journal of Law & Technology,* Vol. 25, No, 1, 1-109

24. Kulesza, J. (2014). USA Cyber Surveillance and EU Personal Data Reform: PRISM's Silver Lining? *Groningen Journal of International Law,* Vol. 2*,* No, 2, 72-89

25. Kuner, C. (2009). An international legal framework for data protection: Issues and prospects. *Computer Law & Security Review,* Vol. 25, No, 4, 307-317.

26. Kuner, C. (2015). Extraterritoriality and regulation of international data transfers in EU data protection law. *International Data Privacy Law,* Vol. 5, No, 4, 235-245.

27. Kuner, C. (2014). The European Union and the Search for an International Data Protection Framework. *Groningen Journal of International Law,* Vol. 2, No, 2, 55-71.

28. Kuner,C. (2012). The European Commission's Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection Law. *Bloomberg BNA Privacy and Security Law Report,* 1-15

29. Lachaud, E. (2014). Should the DPO be certified? *International Data Privacy Law,* Vol. 4, No, 3, 189-202

30. Rauhofer, J. (2015). Of Men and Mice: Should the EU Data Protection Authoritiess Reaction to Googles New Privacy Policy Raise Concern for the Future of the Purpose Limitation Principle? *European Data Protection Law Review (EDPL),*Vol, No. 1, 5-15

31. Revolidis, I. (2017). Judicial Jurisdiction over Internet Privacy Violations and the GDPR: A Case of Privacy Tourism? *Masaryk University Journal of Law and Technology,* Vol. 11, No, 1, 7-37

32. Svantesson, D. J. (2015). Extraterritoriality and targeting in EU data privacy law: The weak spot undermining the regulation. *International Data Privacy Law,* Vol. 5, No. 4, 226-234.

33. Svantesson, D. B. (2013). Extraterritoriality in the context of data privacy regulation. *Masaryk University Journal of Law and Technology* Vol. 7, No, 1, 87-96.

34. Svantesson, D. B. (2014). The extraterritoriality of eu data privacy law its theoretical justification and its practical effect on u.s. businesses. *Stanford Journal of International Law* Vol. 50, No, 1, 53-102

35. Svantesson, D. J. (2018). European Union Claims of Jurisdiction over the Internet - an Analysis of Three Recent Key Developments. *Journal of Intellectual Property, Information Technology and E-Commerce Law,* Vol. 9, No, 2, 113-125

36. Politou, E., Alepis, E., & Patsakis, C. (2018). Forgetting personal data and revoking consent under the GDPR: Challenges and proposed solutions. *Journal of Cybersecurity,* Vol. 4, No, 1. 1-20

37. Zarsky, T. Z. (2017). Incompatible: The GDPR in the age of big data. *Seton Hall Law Review* Vol. 47, No, 4, 995-1020

38. Wagner. J. (2018). The transfer of personal data to third countries under GDPR: when does a recipient country provide an adequate level of protection? *International Data Privacy Law* Vol. 8

EU Legislation:

39. Directive 95/46/EC of the European Parliament of the Council, 24 October 1995, on the protection of individuals with regard to the processing of personal data and the free movement of such data

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

41. Regulation (EU) No 1215/2012 of the European Parliament and of the Council, 12 December 2012 on jurisdiction and the recognition and enforcement of judgements in civil and commercial matters

Case Law:

42. Court Decision, 13.5.2014, Google Spain, EU:C:2014:317, C-131/12

43. Court decision, 5.6.2018 Wirtschaftsakademie Schleswig-Holstein, EU:C:2018:388 (C-210/16)

Other Sources:

44. AggregateIQ challenges ICO jurisdiction. (2018, October 30). Accessible: https://globaldatareview.com/article/1175033/aggregateiq-challenges-ico-jurisdiction

45. Aula, P. (2010). Social media, reputation risk and ambient publicity management. *Strategy & Leadership,* Emerald Group Publishing Vol. 38, No, 6, 43-49.

46. Finck, M. (2018, November 16). Google v CNIL: Defining the Territorial Scope of European Data Protection Law. Accesible: https://www.law.ox.ac.uk/business-law-blog/blog/2018/11/google-v-cnil-defining-territorial-scope-european-data-protection-law

47. Global networks and local values: A comparative look at Germany and the United States. (2001). Washington: National Academy Press

48. Guidelines 3/2018 on the territorial scope of the GDPR (Article 3) European Data Protection Board (23 November 2018) Accessible: https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_3_2018_territorial_scope_en.pdf

49. Handbook on European data protection law. (2018). Luxembourg: Publications Office of the European Union.

50. ICO narrows first-ever GDPR enforcement notice. (2018, October 30). Accessible: https://globaldatareview.com/article/1176139/ico-narrows-first-ever-gdpr-enforcement-notice

51. Kersten, J. (2018), August 09). Who's Enforcing GDPR? - European Data Protection Board | KirkpatrickPrice. Accesible: https://kirkpatrickprice.com/blog/whos-enforcing-gdpr

52. Petrovici, A. N. (2018, May 25). Europe's new data protection rules and the EDPB: Giving individuals greater control. Accessible: https://edpb.europa.eu/news/news/2018/europes-new-data-protection-rules-and-edpb-giving-individuals-greater-control_en

53. Determann, L. (12 June 2018) Representatives under Art. 27 of the GDPR: All your questions answered. Accessible: https://iapp.org/news/a/representatives-under-art-27-of-the-gdpr-all-your-questions-answered

54. Shaw, T. (23 November 2018) How do the DPO and EU representative interplay? Accessible: https://iapp.org/news/a/how-do-the-dpo-and-eu-representative-interplay/

55. Stronger protection, new opportunities (24.1.2018) – Commission guidance on the direct application of the General Data Protection Regulation as of 25 May 2018

56. Svantesson, D. J. (2015). The Google Spain Case: Part of a Harmful Trend of Jurisdictional Overreach. *RSCAS*. 45 1-21

57. Team, I. P. (2017). EU General Data Protection Regulation (GDPR): An Implementation and Compliance Guide - Second Edition. IT Governance

58. Voigt, P., & Von Dem Bussche, A. (2018). Eu General Data Protection Regulation (GDPR): A practical guide. s.l. Springer International Publication.