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

Linda Lehtiniemi

ANALYSING THE CHALLENGES OF ARTICLE 17 OF THE EU GENERAL DATA PROTECTION REGULATION FOR MULTINATIONAL CORPORATIONS

Bachelor's thesis
Programme HAJB08/17, specialisation European Union and international law

Supervisor: Jenna Uusitalo, MA

Tallinn 2020

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 12 317 words from the introduction to the end of conclusion.

Linda Lehtiniemi ……

(signature, date)

Student code: 184027HAJB

Student e-mail address: llehti@taltech.ee

Supervisor: Jenna Uusitalo, MA:

The paper conforms to requirements in force

……

(signature, date)

Chairman of the Defence Committee:

Permitted to the defence

……

(name, signature, date)

TABLE OF CONTENTS

ABSTRACT

Article 17, the so-called right to be forgotten was one of the notable changes when the GDPR came into force. Article enforcement is meaningful from the perspective of multinational corporations since they have an increasing amount of personal data of their personnel and customers.

The aim of this thesis is to survey the challenges arisen from Article 17 and to present proposed solutions. This research is conducted with both qualitative and quantitative methods and is based on the EU legislation, relevant academic literature and interviews of representatives of multinational corporations. The research questions are to clarify what challenges Article 17 poses to multinational corporations and how the challenges can be resolved in a legal sense. The hypothesis is that fulfilling the ruling of Article 17 caused challenges for multinational corporations since it required to change the way to process personal data in order to be prepared for possible removal requests.

The results illustrate that the multinational corporations have encountered many challenges in complying with the ruling of Article 17 since it is possible to have personal data distributed across multiple places. According to the ECJ's assessment of the case C-131/12, the following process of a removal request needs to be detailed and extensive, thus, maintaining such a process is time-consuming and costly. Relevant case law or other guidance is needed as the current situation of uncertainty is difficult for both corporations and individuals. However, more important at the moment is to apply the existing regulation already in a uniform way to guarantee legal certainty.

Keywords: GDPR, right to be forgotten, challenges, multinational corporations

LIST OF ABBREVIATIONS

DIR95	Directive 95/46/EC
ECJ	European Court of Justice
EU	European Union
GDPR	General Data Protection Regulation 2016/679
MNCs	Multinational corporations
MS	Member State of the European Union
RtbF	Right to be forgotten

INTRODUCTION

The world is more globalised and technologised than it has ever been. The collection of personal data keeps increasing, and corporations have vast amounts of collected information about their personnel and customers.[1] Since the world is changing the legislation needs to change with it. As usual, when come changes, come challenges. The research problem of this thesis is to survey what are the challenges caused by Article 17 for multinational corporations (MNCs) when they are applying the General Data Protection Regulation (GDPR). The aim is to discover the challenges and to present proposed solutions to these challenges. The research questions are to clarify what challenges Article 17 poses to multinational corporations and how the challenges can be resolved in a legal sense. The hypothesis is that fulfilling the ruling of Article 17 caused challenges for MNCs since it required to change the way to process personal data in order to be prepared for a possible removal request.

I became intrigued by this subject because it is very topical at the moment since the GDPR came into effect on May 2018. Due to my research, I have noticed the GDPR brought many changes. Corporations have surprisingly large amounts of information about their data subjects, and I wanted to focus my thesis on the major challenges from the perspective of MNCs. I choose especially the perspective of MNCs due to the world's globalisation and the commonplace nature of cross-border issues. Furthermore, since the GDPR got into force, the rights of the data subjects have increased while the responsibilities and obligations of MNCs have also increased. Because the topic is broad, but the length of the thesis is limited, I focus on Article 17 Right to erasure "right to be forgotten" (RtbF). I decided to take precisely this Article because based on my own research, going through the literature and interviewing the representatives of MNCs, this was the one that came up as one of the most challenging. This Article creates new challenges for many MNCs to meet; they must change their procedures and be prepared for new requests.

First, I will go through the relevant concepts to define them better. I present the differences between the GDPR and the previous European Union (EU) Data Protection Directive, officially Directive 95/46/EC (DIR95) to clarify the changes. Also, I will go through the impact of the new regulation on MNCs. I will concentrate on both the negative and positive sides. After the general introduction to the topic, I will go through the basics of the RtbF and take the general view of the challenges that Article 17 brought to the MNCs. I will explain in detail the aspects that connect to the challenges

[1] Oostveen, M. (2016). Identifiability and the applicability of data protection to big data. *International Data Privacy Law*, 6(4). Oxford University Press, 299-309. 299.

brought by the RtbF. I target my attention to MNCs that operate inside the EU but also touch on challenges that may appear from the RtbF when MNCs operate outside of the EU. Thus, I will also briefly focus on EU cross-border issues that arise if the MNCs do not operate only inside the EU, but for instance, in the United States or Asian markets as well. After I have presented the challenges that may be caused by Article 17, I will examine the European Court of Justice (ECJ) case law. I will present judgment of the case C-131/12 to examine how the ECJ has acted concerning the corporation in the case of a removal request based on DIR95. Since these new obligations are here for a reason, there will be consequences if the MNCs do not fulfil the needed requirements. Thus, I will also go through the possible sanctions. I will propose suggestions on how these legal challenges can be resolved based on my research and findings. In the end, I will conclude by presenting the main results of my thesis and explaining further research possibilities.

This research is conducted with both qualitative and quantitative methods and is based on the EU legislation, relevant academic literature and interviews of representatives of multinational corporations. I am using a quantitative method to understand MNCs as a subject and their challenges when applying the RtbF. I accomplished this by interviewing the representatives of the MNCs. By looking at the observable data, I am looking to understand the challenges that Article 17 poses to MNCs. To most of the representatives, I sent a questionnaire with four open questions; one was about the GDPR in general, three of them concerned the RtbF and the challenges that may appear when applying it and one was about the possible sanctions. (See Appendix 1.) In addition, with a few of the representatives, I had the opportunity to meet in person and discuss the matter. All of the answers given were processed anonymously. All corporations were of different sizes, from 50 to 10,000 employees and from different industries from the commercial sector to the technology industry. All of them operate in at least one country other than their home country because I wanted to focus on the impact caused by Article 17, especially to MNCs. I decided to interview different sizes of corporations from different industries to get a comprehensive overview. I want to emphasise that I am not drawing the conclusion based on this sample, but they rather support my findings through a practical example. Altogether, I got answers from ten different MNCs. The sample is not, and its purpose is not to be representative; therefore, I do not represent the obtained results as a general fact. Instead, these interviews gave me valuable information and a deeper understanding of how MNCs are applying the GDPR on a practical level, the challenges arisen and how they are dealing with these challenges. These interviews are to support my research and extend the perspective about what MNCs go through on a daily basis to get as realistic a picture as possible on this matter. I am grateful for all the replies received from the corporations.

1. THE GDPR AND THE RIGHT TO BE FORGOTTEN

1.1. Concepts

In order to analyse Article 17 properly, it is important to understand the relevant concepts. These are defined in Article 4 of the GDPR. Here I go through the concepts that appear explicitly in Article 17 and are relevant from the perspective of MNCs and this paper. First of all, here, MNCs stand for corporations in the EU which process personal data and operate at least in one country in addition to their home country. This country can be in or outside of the EU. MNCs have operations simultaneously in several different countries.[2]

The concept of personal data is one of the most significant since the data subject has the possibility to erase it due to the ruling of Article 17. All MNCs have personal data, starting from the employee databases, payrolls and customer databases.[3] The personal data are worth protecting from the perspective of MNCs since it has the potential to create added value for them. In general, personal data refers to information relating to an individual. More specifically, it means any information related to an identified or identifiable natural person, the data subject, that allows a person to be directly or indirectly identified by combining an individual piece of information with another piece of information. For instance, by reference to an identifier such as name, an identification number or location data.[4] Personal data are, for instance, name, home address, telephone number, e-mail address, identity card number, car registration number, IP address and patient records. Instead, a corporation's business ID, a shared e-mail address or anonymised data are not regarded as personal data. The GDPR protects personal data, regardless of the technology used to process it or the way the data are stored. The data can be stored in an IT system, a video surveillance system or a paper archive, for instance. As long as the information can be used to identify a person directly or indirectly, or to return the information in an identifiable form, it remains personal data and thus can be asked to be erased by the data subject due to ruling of the RtbF.[5]

[2] Cohen, S. (2007). *Multinational Corporations and Foreign Direct Investment*. Oxford, United Kingdom: Oxford University Press. 36.
[3] Krystlik, J. (2017) With GDPR, preparation is everything, *Computer Fraud & Security*, 2017(6). Elsevier, 5-8. 7.
[4] 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). Oxford University Press, 1-20. 3.
[5] *What is personal data?* Office of the Data Protection Ombudsman. Retrieved from https://tietosuoja.fi/en/what-is-personal-data, 2 March 2020.

Especially in the case of MNCs, the processing of the data often crosses borders.[6] In most cases, the corporation works as a data controller. In this paper, while I refer to a data controller, the focus is on the corporation. The data controller is a natural or legal person, public authority, agency or another body that determines the purposes and means of the processing of personal data alone or together with others.[7] It is important to distinguish the controller from the data processor. The difference is that processor processes personal data on behalf of the controller.[8] Processing means any kind of operation or set of operations which is performed on personal data or sets of personal data, whether by automated means or not. Processing may include, for instance, collection, recording, organisation, structuring, storage, adaptation, use, restriction, erasure or destruction, just to name a few.[9] Thus, when MNCs' processing is wholly or partly automatic or personal data form a part of the register, such processing must comply with the requirements of the GDPR.

A data breach means a security breach leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.[10] If a breach happens, the corporation needs to inform a supervisory authority who is an independent public authority.[11] Data breaches can be very harmful to MNCs due to the valuable nature of personal data. When the personal data can no longer be attributed to a specific data subject without the use of additional information, it is a case of pseudonymisation. It is required to keep such additional information separate and ensure with technical and organisational measures that the data cannot be combined with a natural person.[12] Personal data can also be encrypted, which means it becomes unintelligible to any person who is not authorised to access it, and those who have a secret decryption key are able to access the information.[13] Lastly, when talking about anonymisation, it means the processing of personal data in such a way that the person can no longer be identified. Anonymised data are no longer considered personal data. Thus, they are not subject to the GDPR and cannot be subject to the removal request either according to Article 17.[14]

6 Wolters, P.T.J. (2017). The security of personal data under the GDPR: A harmonized duty or a shared responsibility? *International Data Privacy Law*, 7(3). Oxford University Press, 165-178. 165.
7 GDPR, Art.4(7).
8 *Ibid*., Art.4(8).
9 *Ibid*., Art.4(2).
10 *Ibid*., Art.4(12).
11 Nieuwesteeg, B., Faure, M. (2018). An analysis of the effectiveness of the EU data breach notification obligation. *Computer Law & Security Review*, 34(6). Elsevier, 1232-1246. 1233.
12 GDPR, Art.4(5).
13 Spindler, G., Schmechel, P. (2016). Personal Data and Encryption in the European General Data Protection Regulation. *JIPITEC*, 7(2), 163-177. 169.
14 *Pseudonymised and anonymised data*. Office of the Data Protection Ombudsman. Retrieved from https://tietosuoja.fi/en/pseudonymised-and-anonymised-data, 26 April 2020.

1.2. Legal background

The data protection is a fundamental right.[15] From my point of view, after reading the relevant literature, the RtbF was a needed change. In today's world technology develops fast, and when it does, it brings new challenges. During this technological development in this globalised world where personal data are collected increasingly, the EU saw an issue that the current legislation did not respond to. The EU considered it necessary to reform and modernise the legislation. Thus, the GDPR was created to respond to current challenges and harmonise data protection across the EU. The regulation came into force on May 2018, and at the same time, it replaced DIR95. The aim of the regulation is to provide the EU with a modern, strong, coherent and comprehensive data protection framework.[16] The purpose of the regulation is to improve the protection of personal data. As I see it, creating the RtbF was one of the answers to reach the goal.

Although the GDPR was expected to benefit MNCs by increasing productivity and efficiency as well as achieve savings by enabling more integrated EU-wide data protection policies, it brought new challenges to them.[17] The GDPR applies to the MNCs that process personal data and are located in the EU, regardless of where the processing of personal data itself takes place. The regulation applies not only to European corporations but also to all corporations located outside of the EU if they process personal data in relation to the offering of goods or services to individuals in the EU or monitors the behaviour of individuals within the EU. Non-EU based corporations processing EU citizens' data have to appoint a representative in the EU.[18]

1.2.1. Directive 95/46/EC

In order to understand the present, one needs to understand the past. Thus, I will briefly examine DIR95 and its differences in relation to RtbF. The GDPR replaced DIR95 and is the updated version to meet current challenges. The RtbF is one of the changes in the GDPR, compared to DIR95. Article 17 of the GDPR corresponds to Article 12 (b) in DIR95 Right of access. DIR95 Article 12 states MSs

[15] OJ C 326, 26.10.2012.
[16] Andreasson, A., Riikonen, J., Ylipartanen, A. (2019). *Osaava tietosuojaastaava ja EU:n yleinen tietosuoja-asetus*. Helsinki, Finland: Tietosanoma. 27.
[17] Tikkinen-Piri, C., Rohunen, A., Markkula, J. (2018). EU General Data Protection Regulation: Changes and implications for personal data collecting companies. *Computer Law & Security Review*, 34(1). Elsevier, 134-153. 140.
[18] *Data Protection under GDPR*. Official website of the European Union. Retrieved from https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_en.htm, 21 April 2020.

are required to guarantee every data subject the right to obtain from the controller as appropriate the rectification, erasure or blocking of data the processing of which does not comply with the provisions of DIR95, particularly caused by the incomplete or inaccurate nature of the data.[19] Thus, DIR95 has already guaranteed the data subject the right to erasure if the processing does not comply with the DIR95's provisions. This is obtained especially in case of incomplete or inaccurate data. The RtbF sets up new conditions for data subject's right to erasure, and due to these changes, the data subjects do not need grounds provided by DIR95 such as incompleteness or inaccuracy of the data to erase it. A data subject may ask for personal data to be deleted once the data are no longer necessary.[20] There has been a clear desire to emphasise the RtbF as it has been extended as its own article. Due to this, deleting data is easier than in the previous directive, which causes challenges to the MNCs. Corporations need to understand what the article was before to detect changes and to change their actions in the necessary direction to fulfil new obligations.

1.3. Multinational corporations' perspectives

After the GDPR entered into force, there was a two-year transition period during which MNCs had to adjust their activities to comply with the regulation. It became fully applicable from 25 May 2018 for all MNCs. The GDPR shall be binding in its entirety, and it shall apply directly in all MSs unless it has used the margin of manoeuvre provided in the regulation to specify their rules.[21] Due to the GDPR, the scope of data protection expands in the way that it applies to any MNCs that collect and process information related to EU citizens, and it does not matter where the MNCs are based or where the data are stored.[22]

MNCs' collection of personal data keeps growing. They have large amounts of collected information about their data subjects. The data can be collected through an agreement, consent or customer relationship, for instance. Especially behind the data collection of IT corporations is the so-called Big Data boom, during this time, MNCs began collecting and storing all possible information about their customers. Information was collected, for instance, to target advertising or to be resold, but also if in the future, the data will be used for other purposes or will be processed into more usable and valuable data. Big data has the potential to enable corporations to create significant revenues. Nevertheless,

[19] OJ L 281, 23.11.1995.
[20] Tikkinen-Piri, C., Rohunen, A., Markkula, J. (2018), *supra nota* 10, 142.
[21] Andreasson, A., Riikonen, J., Ylipartanen, A. (2019), *supra nota* 10, 27.
[22] Tankard, C. (2016). What the GDPR means for business. *Network Security*, 2016(6). Elsevier, 5-8. 6.

the rising trend in the collection and use of personal data creates issues, in particular regarding privacy and data protection rights of individuals.[23] Since personal data are valuable information, Article 17 is here to provide individuals control over their data and for its part is created to prevent partly any possible undesirable consequences of data collection. However, it is uncertain whether it is enough to prevent these adverse consequences.[24]

It must be possible for MNCs to prove in practice that the obligations laid down in Article 17 have been fulfilled, inter alia by means of documents.[25] The regulation includes accountability, mere compliance is no longer sufficient, and the management of a corporation must be able to demonstrate how it has taken the necessary technical, administrative and organisational measures to ensure compliance with data protection obligations.[26] Thus, it is not enough for MNCs to comply with Article 17 ("do it") but must be able to demonstrate ("prove it") that the controller respects the ruling of the RtbF. It is clear that MNCs face many challenges in reaching this target. There are different ways how the ruling of Article 17 is applied in the practical operation of MNCs.[27] The same result could be extracted from the interview. The way depends on, for instance, the industry, corporation's size, nature of activity, sensitivity of the data processed, purpose and internationalisation.

1.3.1. Positive impact

When MNCs' employees in all countries, are knowledgeable and they do not process data or removal requests in uncertainty, they can ensure that the data subjects' rights are fulfilled in the case of a removal request. Thus, the beneficiaries of innovative data protection are the corporation's data subjects, employees, and the corporation itself. However, I think that especially individuals will benefit from this positive change of corporations, the change proves that the corporation takes their rights seriously. Based on my opinion, the RtbF for the data subject is achieved through well-designed and implemented processing of personal data. By doing so, MNCs may also avoid legal consequences such as administrative fines. This enables the corporation to succeed both in the domestic and international markets.[28] I think that updated data privacy supports the establishment of a confidential customer relationship. A corporation, in accordance with the regulation obligations, such as Article

[23] Oostveen, M. (2016), *supra nota* 6, 299.
[24] *Ibid*., 299.
[25] Andreasson, A., Riikonen, J., Ylipartanen, A. (2019), *supra nota* 10, 24.
[26] *Ibid*., 25.
[27] *Ibid*., 22.
[28] *Ibid*., 10, 19-20.

17, appears to be an outsourced service provider and an attractive business partner. This proves to be a competitive advantage as the customer can trust that his or her valuable information will be processed legally.[29] Risk minimisation, building a good reputation and maintaining consumer confidence are all important matters for the success of a business.[30] From this, I can conclude that it is worth investing in data protection and make efforts to fulfil the ruling of Article 17 because it pays for itself.

1.3.2. Negative impact

The main obligations regarding the processing of personal data come directly from the GDPR, and all MNCs processing personal data must comply with the regulation as of 25 May 2018. However, MSs have the right to adopt complementary data protection legislation in so far as the GDPR leaves some room to manoeuvre in relation to certain matters. The national Data Protection Act complements and clarifies the GDPR. The act does not constitute a stand-alone law but applies in parallel with the regulation.[31] When the GDPR started to apply on May 2018, the guiding national legislation did not exist in all MSs. For instance, in Finland, there was no such legislation in autumn 2018 until the national Data Protection Act came into effect on December 2018.[32] This is a very difficult case when it comes to MNCs which are partly based in Finland because the regulation within Article 17 has required interpretation many times and in many ways. It is likely that retroactive legislation requires changes to decisions already made. This, in turn, increases costs and takes time away from corporations again.[33] Based on my understanding and interviews, if data protection issues are poorly managed, this creates uncertainty, which can reduce overall employee satisfaction and thus, the productivity and efficiency of the entire corporation. Without the knowledgeable personnel, there would be a huge deficiency which would endanger the realisation of individuals' rights ruled by Article 17, which would result in the worst-case scenario cause administrative fines. The ignorance and lack of communication is a risk for MNCs, meaning that data protection issues are not discussed enough in the corporation and, due to lack of knowledge, personnel may not be able to work properly according to the requirements provided by Article 17. If this happens, the data subject's rights cannot be fulfilled as the RtbF demands.

[29] *Ibid*., 50.
[30] *Ibid*., 13.
[31] Tietosuojalaki 5.12.2018/1050.
[32] *Ibid*.
[33] Andreasson, A., Riikonen, J., Ylipartanen, A. (2019), *supra nota* 10, 9.

2. CHALLENGES

2.1. Basis of the right to be forgotten

The RtbF is a right which is given to all citizens in the EU. However, the right to get data erasure is not absolute and has its limits. It applies when the data are no longer necessary or is irrelevant for the original purpose for which it was collected in the first place.[34] If a data subject no longer wants data controller to process or store the personal data, and if there is no legitimate reason to keep it, then the data should be removed from the corporation's systems. However, corporations are required to collect personal data only for relevant purposes.[35] The RtbF should enable European citizens, especially teenagers, to have control over their own identity online.[36] One major idea behind the RtbF is the case where the data subject has given the consent as a child, and during that time has not been fully aware of the risks that are involved by the processing, and wants to remove such personal data later on.[37] I think a change like this is very decent from the perspective of individuals. The right should address the fact that the internet has nearly an unlimited search and memory capacity and even a little amount of personal data can have a substantial impact, even after years when they were shared or made public.[38]

The GDPR Article 17 paragraph 1 states:

1. The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:

a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;

b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing;

[34] *Factsheet on the "Right to be Forgotten" ruling (C-131/12)*. European Commission. Retrieved from https://www.inforights.im/media/1186/cl_eu_commission_factsheet_right_to_be-forgotten.pdf, 20 March 2020.
[35] Burdon, M. (2020). *Digital Data Collection and Information Privacy Law*. Cambridge, United Kingdom: Cambridge University Press. 171.
[36] Sartor, G. (2015). The right to be forgotten in the Draft Data Protection Regulation. *International Data Privacy Law*, 5(1). Oxford University Press, 64-72. 70.
[37] GDPR, Preamble 65.
[38] Sartor, G. (2015), *supra nota* 14, 64.

c) the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2);

d) the personal data have been unlawfully processed;

e) the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject;

f) the personal data have been collected in relation to the offer of information society services referred to in Article 8(1).

In Article 17, paragraph 2 states that the controller has an obligation under paragraph 1 to erase the personal data if the personal data have been made public.[39] The controller needs to take reasonable steps, including technical measures, and to take into account available technology as well as the cost of implementation, to inform controllers which are processing the personal data about the data subject's request for erasure by such controllers with any links to, or copy or replication of, that personal data.[40] However, Article 17 paragraph 3 lists the exceptions of paragraphs 1 and 2.[41]

One example of an exception that came up in the interviews could be that according to the Finnish national law, a corporation is under the obligation to give an employee an employment certificate if it is requested within ten years of the termination of employment.[42] However, there is a discrepancy in a case where the same employee resigns and makes a removal request to the corporation based on the RtbF. In that case, the corporation needs not to delete the certificate since this kind of certificate can be seen to be in compliance with a legal obligation which requires processing by a MS's, here Finland, law to which the corporation is subject.[43]

According to the GDPR's preamble paragraph 65 one of the aims of the RtbF is to enable erasure of unlawfully stored and processed personal data. Thus, the data subject's RtbF is based on unlawful processing and not on the content of the personal data. However, the content of the personal data may have an effect on how well the process is deemed to comply with Article 17. All the legitimate grounds for data processing are listed in Article 6. From the MNCs' point of view, the most common are, for instance, when the data subject has given consent to the processing or the processing is

[39] GDPR, Art.17(2).
[40] *Ibid*.
[41] *Ibid*., Art.17(3).
[42] Työsopimuslaki 26.1.2001/55. See § 7.
[43] GDPR, Art.17(3).

necessary for the performance of a contract where the data subject is party or processing is necessary for compliance with a legal obligation to which the controller is subject.[44]

2.2. General analysis of the challenges

Article 17 is one of the notable changes since it brought more rights for the individuals.[45] Individuals' rights involve a challenge for MNCs, for instance, concerning what information is necessary for the operation of the corporation compared to information that can be influenced by individuals. The corporation would make a mistake and break the law if it would oppose an individual's right to delete personal data on the grounds that it would be necessary to retain such information for strategic reasons, for instance. Based on the interview, these issues are currently being considered and will continue to be considered in the future.

The RtbF states that the data subject has the right to erasure of personal data relating to the data subject by the controller without unnecessary delay. Thus, the data controller has an obligation to delete the personal data without undue delay, unless, for instance, the data controller has a legitimate reason to process the data.[46] At its worst, the personal data are spread across multiple information systems, servers, drives, and Excel.[47] This requires IT capabilities to ensure that data subject's rights are enforced and that personal data are not left unauthorised in various systems such as log files, backups, or printouts. Time and resources also pose challenges in a removal request to a corporation if it does not have a specific person who is instructed to take care of the issue within a specified time.

It could be said this right is a breakthrough in the EU legal system, since it does not only include the right to be erased (or "forgotten"), but it also includes the right to especially "be forgotten". While the former defines the obligation of the controller to delete the data, the latter implies more that the data must be deleted from any possible locations. Therefore, for the RtbF to be fully enforced, the MNCs must ensure that the data have been deleted not only from their own files but also from possible data processors', employees' and any possible third parties' file systems from all possible countries. However, it should be noted that the legal obligations mentioned in the exceptions in this article,

[44] GDPR, Art.6(1).
[45] Lambert, P. (2018). *Understanding the New European Data Protection Rules*. Boca Raton, USA: CRC Press. 199.
[46] *Ibid*., 199-200.
[47] Politou, E., Michota, A., Alepis, E., Pocs, M., Patsakis, C. (2018). Backups and the right to be forgotten in the GDPR: An uneasy relationship. *Computer Law & Security Review*, 34(6). Elsevier, 1247-1257. 1254.

which concern the retention of data by data controllers, take precedence over the matters mentioned in paragraph 17 (1).

One of the common challenges facing many MNCs, mentioned in the interview as well, is that data subject's information is located across many systems, and there is no overall picture.[48] In many cases, these systems cannot even communicate with each other. Employee e-mails may also contain contacts and personal information, for instance, curriculum vitae and job applications. Knowledge of the location of all personal information simply does not exist. This makes retrieving and deleting data cumbersome, inefficient and time-consuming. Due to information about data subject being stored in multiple locations, and the information having different details depending on the system, it can be challenging to identify what information is relevant concerning exactly the data subject who sent the removal request. One of the biggest challenges is to ensure that, for instance, backups of employee files and local archives of e-mails do not contain any personal data that are within the scope of the removal request after the deletion has been completed.[49] From my point of view, especially MNCs, which are operating in more than one country face their own challenges since the GDPR aims to legislate all personal data regardless of where the data are located. Data will be the focus of legal attention and subjected to this new regulation instead of a country's laws. This means at least theoretically speaking that the physical location of the data is no longer relevant. Thus, when ruling on the RtbF it does not matter whether the data are in a data centre in the United States or China, or in the City of London, the legal constraint remains the same in theory.[50]

2.3. In the case of a removal request

Article 17 process begins when the data subject submits a removal request to the controller. However, in order to invoke the RtbF, a data subject must first be able to identify the data controller.[51] Interruption of the processing of the data requires that the data are erased from all parts of the corporation's servers in all countries. When a corporation's data are scattered in several places, partly in the cloud and partly behind a strong firewall in its own data centre, the challenge for data management and finding correct data in the case of removal request can be quite daunting.

48 *Ibid*., 1254.
49 *Ibid*., 1253.
50 Krystlik, J. (2017), *supra nota* 8, 8.
51 Fazlioglu, M. (2013). Forget me not: The clash of the right to be forgotten and freedom of expression on the Internet. *International Data Privacy Law*, 3(3). Oxford University Press, 149-157. 151.

As mentioned above, there are grounds for erasure defined in Article 17, paragraph 1. It also matters on what grounds the corporation is processing the data. Article 17 does not, however, from my point of view, require the data subject to invoke to a specific ground for erasure when making a removal request. Such a requirement of a thorough knowledge of the legislation would unduly restrict the protection of the personal data of the data subject. However, as I see it, in the removal request it must be identified what information is being deleted because the request does not necessarily require all of the data to be erased. In the case of a removal request, there are also especially defined time limits set up for MNCs[52], and if there is no knowledgeable person to deal with these issues, time limits may cause trouble if MNCs have no awareness of where all the data are located.

2.3.1. Making the decision of erasure

The time limits for the removal decision are written down in Article 12 of the GDPR. It requires the controller to provide the data subject with information on the action taken based on the request for removal within one month of receipt of the request for removal.[53] In the event of a complex request or if there is a large number of requests, the time limit may be extended by a maximum of two months.[54] If the controller does not delete the data, it is required to provide the data subject a reply, stating the reasons, and the remedies available. This must be done within one month of receiving the request.[55]

As I see it, the implementation of Article 17 is not a straightforward task. As a matter of fact, it may even feel impossible in some of the cases. In the corporation databases, if the information of the data subject is not linked to the publication or database requested for deletion, it may be incredibly difficult for the corporation to determine what information is included in the removal request. However, the obligation to state reasons implies that each removal request must be dealt with separately. The controller must also carefully examine the grounds for a removal request in accordance with the jurisprudence of the ECJ and must give a reasoned decision.[56] If it is clear from the request for removal that the controller no longer has any reason to process the personal data requested for deletion, the data shall be deleted.

[52] GDPR, Art.12(3).
[53] *Ibid*.
[54] *Ibid*.
[55] *Ibid*., Art.12(4).
[56] C-131/12, EU:C:2014:317.

2.3.2. Applications and files

After the decision of erasure has been made, the corporation needs to look for all the necessary data to fulfil the ruling of RtbF. There may be many files on an employee's personal computer, and it is possible the data has been moved to several places. In addition, the data can exist on an employee's own files such as e-mail, smartphone, external hard drive, cloud services, USB flash drive or other databases and short-term backups, for instance. Since in this paper I am talking about MNCs which are located in several countries, the data might also be scattered across borders. The employee uses the corporation's applications, files and databases, which all need to be checked in order to fulfil the right of the data subject who made the request. All other applications on the employee's computer and smartphone must be checked as well. The issue here is that there can be many employees in different countries who have data stored or then one employee who has data in several places.[57] The challenging part here is to locate all the data stored in applications and files in all countries where the data might be and which the request concerns. On the other hand, based on the interview, MNCs can have internal guidelines that certain specified data cannot be stored in a personal computer, for instance. Such a procedure may help to comply with the ruling of Article 17.

2.3.3. Clouds and data centres

Corporations challenges do not end to applications and files. Clouds, not just cloud backups, are another challenging area when it comes to Article 17 since the data are digitised, migrating the data to the cloud in addition to archiving data for everyday use. Some corporations may prefer external IT service provider such as a public cloud service provider because they want to avoid maintenance costs caused by a data centre.[58] The increase in cloud services raises the question of protecting European information from a new perspective. When information is provided to an external cloud service provider, it forces the corporation to ensure that the cloud service is able to provide an adequate level of security and generate event logs. When a corporation deploys a cloud service, in the event of a removal request, it must rely on the cloud service provider being able to erase the necessary information since there is no certainty where the data is exactly located, and data protection differs across countries and continents.[59] Thus, it has significant importance to MNCs to keep track of the contents of each backup. I think based on the interviews if MNC's storage use is variable cloud could

[57] Politou, E., Michota, A., Alepis, E., Pocs, M., Patsakis, C. (2018), *supra nota* 16, 1254.
[58] *Ibid*., 1255.
[59] *Ibid*.

be better, but if the corporation needs regular bigger storage then data centre could work because through own data centre the corporation can be sure that the data is processed correctly in the case of a removal request and the data is located countries who are bind by the GDPR. On the other hand, some MNCs may have data hosted outside of the EU. The reason can be that these are tied to their corporate structures, or some of the business applications may not offer the hosting within the EU.[60] In the case like this, the MNCs must ensure that the cloud provider will be duty-bound to comply with the restrictions imposed by the GDPR in processing data.

Based on the interviews, usually, the data has two copies and backup. Thus, the data can be stored both in the cloud and on the data centre storage systems. However, in the case of a removal request, for instance, for large MNCs with old servers it is time-consuming to try to find the wanted data. Once it has been found, it is possible that the only way to erase the data is an old-fashioned way, to overwrite. Thus, there are challenges to fulfil the ruling of Article 17 in both styles of storing information.

2.3.4. Archives and backups

This section covers the RtbF with respect to backup and archiving, which are taking place within each corporation that handles personal data. Physical or cloud backups and archives have become especially challenging since they need to be checked as well in the case of a removal request in order to ensure the rights of the data subject are fulfilled. In particular, already well-established backup and archiving procedures in MNCs are affected significantly by the RtbF erasure requirements.[61] Archives are for data's long-term retention and include not so regularly used data[62], whereas backup is a copy of computer data that is stored separately elsewhere, thus it can be restored if the data are lost for some reason. Backups can be considered fundamental processes within the business' continuity plan since they allow quick recovery if an information system suffers a disaster. The disaster may be caused by, for instance, cyber-attacks, physical damages, hardware failures, system crashes or data corruption. Therefore, backups' goal is not only data preservation but also quick recovery.[63]

60 Krystlik, J. (2017), *supra nota* 8, 5.
61 Politou, E., Michota, A., Alepis, E., Pocs, M., Patsakis, C. (2018), *supra nota* 16, 1252.
62 *Ibid*., 1248.
63 *Ibid*., 1256.

The challenge mainly concerns situations where a removal request is being made, and the corporation already made the backup or archived the data. Usually, each backup file includes many user's data and to make it more complicated, the data can be located even in multiple backup files from several applications used in a corporation. One example of a situation where the personal data erasure may cause a considerable challenge is to have backups on disks, which may vary from optical CDs and DVDs to BlueRay discs and hard discs or tapes. In the case of such backups, it is not possible to delete single records from the backup as easily without restoring the full database like in some export formats. This is time-consuming, costly and complex.[64]

The abovementioned issues raise questions and challenges as MNCs are aware that non-compliance will have huge consequences. In this context, it has been discussed by experts whether RtbF should apply to archives or backups at all, taking into account the enormous cost and effort involved in practice.[65] Both parties have valid arguments. Some see that RtbF should not apply archives or backups because of the significant practical effort and high costs. Personally, I agree with the most experts' opinions that the RtbF should apply to all archives and backups since within the text of the GDPR or in the RtbF, there is no explicit derogation on the matter. It is therefore legitimate to claim that the RtbF is indeed applicable to both and thus poses major challenges for corporations.

2.3.5. Data breach

Data breaches have become more common.[66] Such a breach refers to cases where the data have been compromised.[67] In the case of these, to fulfil the obligations ruled by Article 17 might become challenging since the technological developments have led to the digitalisation of MNCs in many parts of their operations.[68] Upgrading the IT systems to the latest version is also highly recommended for security reasons. When the IT systems are connected to the internet, they are open to many types of hackers, and if the hacker gains access to the systems, for instance, by clicking a link, there may

64 Politou, E., Michota, A., Alepis, E., Pocs, M., Patsakis, C. (2018), *supra nota* 16, 1256.
65 *Ibid*., 1255.
66 Romanosky, S., Ablon, L., Kuehn, A., Jones, T. (2019). Content analysis of cyber insurances polices: How do carriers price cyber risk? *Journal of Cybersecurity*, 5(1). Oxford University Press, 1-19. 12.
67 Malatras, A., Sanchez, I., Beslay, L., Coisel, I., Vakalis, I., D'Acquisto, G., Sanchez, M.G., Grall, M., Hansen, M., Zorkadis, V. (2017). Pan-European personal data breaches: Mapping of current practices and recommendations to facilitate cooperation among Data Protection Authorities. *Computer Law & Security Review*, 33(4). Elsevier, 458-469. 459.
68 Agrafiotis, I., Nurse, J.R.C., Goldsmith, M., Creese, S., Upton, D. (2018). A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate. *Journal of Cybersecurity*, 4(1). Oxford University Press, 1-15. 1.

be personal data that are accessed by outsiders.[69] For the MNCs to delete the data subject's personal data from any possible locations, they should know where the data are located and have the access to it. Such a breach at the corporation may cause challenges since they may lose access to the data and the potential impact of such a breach is uncertain. If there is no established practice in the case of a possible breach, understanding of the consequences and evaluating the damages can be challenging for corporations.

The accidental disclosure of personally identifiable information may stem from loss or theft of digital or printed information. For instance, the theft of computers containing personal information of personnel or customers of a corporation may cause either by a hacker, thief or malicious employee.[70] This may have a substantial impact if there is personal information included and the data subject uses the RtbF. It is possible that the corporation does not have any clue where the stolen devices or data are located and thus cannot guarantee that Article 17 obligations are fulfilled, unless the personal data on the device are successfully protected by pseudonymisation, encryption or anonymisation, for instance. There has also been discussion claiming that previously, there was no requirement for private corporations to let individuals know about data breaches.[71] However, there is now, since the regulation demands them to notify the supervisory authority of serious data breaches within 72 hours.[72]

2.4. Coordinating with the ECJ jurisprudence

2.4.1. Google Spain v. González

The RtbF under DIR95 has been assessed in the case C-131/12. Here, the ECJ made an assessment and ensured that the interpretation is observed.[73] The ruling of the ECJ placed the RtbF in the middle of the global privacy debate.[74] In practice, the most direct way to proceed if a data subject wants the data being erased is to contact the corporation who has originally disclosed the information even

[69] Lee, N. (2013). *Counterterrorism and cybersecurity*. New York, USA: Springer. 130.
[70] Romanosky, S. (2016). Examining the costs and causes of cyber incidents. *Journal of Cybersecurity*, 2(2). Oxford University Press, 121-135. 123.
[71] Jasmontaite, L. (2018). Gry Hasselbalch and Pernille Tranberg, Data Ethics – The New Competitive Advantage. *International Data Privacy Law*, 8(2). Oxford University Press, 175-177. 176.
[72] GDPR, Art.33(1).
[73] Kenealy, D., Peterson, J., Corbett, R. (2015). *The European Union: How does it work?* (4th ed.) Oxford, United Kingdom: Oxford University Press. 62.
[74] McCarthy, H. (2016). All the World's a Stage: The European right to be forgotten revisited from a US perspective. *Journal of Intellectual Property Law & Practice*, 11(5). Oxford University Press, 360-371. 360.

though the regulation does not require this. However, in order for the information to disappear completely, it requires contacting the corporation so they can remove that information from their servers.

Mr González searched Google for his name, and the Google search resulted in links to the newspaper articles from 1998 in which an announcement mentioning Mr González's name appeared in connection to a real-estate auction connected with attachment proceedings for the recovery of social security debts. Mr González requested the newspaper to remove his personal information from webpages, and he requested Google Spain or Google Inc. to remove or conceal the personal data relating to him, which appears at the search results. The claim against the newspaper was rejected, and with regard to the claim against Google, the court turned to the ECJ.[75]

In Google's case, it being a controller, liability the ECJ considered that it processed the personal data in connection with searches made as a data controller for the purposes of the legitimate interests pursued by the controller or by the third party.[76] The interests were, in the case, the economic interest of the controller and the interest of the public to have access to the information. According to the ECJ, the interest of the controller is not in itself sufficient to justify further processing. As a general rule, the protection of privacy also overrides the public's right to information. However, in individual cases, the nature and sensitivity of the information and the position of the data subject, for instance, as a public figure, may affect this balance.[77] In its decision, ECJ highlighted the importance of respecting fundamental rights, in particular the right to privacy.[78] In the end, Google was obliged to remove links to web pages published by third parties and links containing information relating to a person from the list of results displayed following a search made based on that person's name.[79] The ECJ pointed out that the controller must carefully examine the grounds for the request and that the assessment of the grounds for the request must take into account all the circumstances of the data subject's specific situation.[80] In addition, the controller must always ensure the lawfulness of the processing.[81]

[75] C-131/12, EU:C:2014:317, paragraphs 14-20.
[76] *Ibid*., 73-74.
[77] *Ibid*., 81.
[78] *Ibid*., 34-38 and 66-68.
[79] *Ibid*., 88.
[80] *Ibid*., 76-77.
[81] *Ibid*., 72.

This judgment gives an example of how a removal request should be evaluated. The process in MNCs that follows a removal request based on this judgment must be detailed and extensive. This may cost a lot of money to maintain such a process. Thus, the case law showed that the conditions set for the controller to fulfil the obligations ruled by the RtbF are high, and search engines such as Google need to take responsibility as data controllers for the content that they link to and may be required to purge their results even if the material was previously published legally. The removal request must be promptly investigated and carefully justified. This article sets the criteria high, and MNCs may have challenges meeting them.

On the other hand, some authors have also argued that the emergence of the RtbF in the GDPR diverges significantly from the right specified in this decision which actually regulated a "right to be delisted" since it aimed at the technological intermediary and not the original publisher of the information.[82] This way, the RtbF of the GDPR adds to the data protection principle of data subject's rights of data erasure, for instance.[83] Also, many scholars are critical of the RtbF since it has the potential to lead to private censorship.[84] As well as the exercise of the RtbF may possibly prevent every kind of further data processing.[85] As mentioned earlier, the personal data has the potential to create added value to the MNCs. Thus, if all the data disappear, including the consents, it may create an enormous loss for the corporation if many data subjects exercise their RtbF. Thus, I think these authors have valid arguments as well, and it will be interesting to see what kind of jurisprudence the ECJ will provide in the future concerning the RtbF of the GDPR.

82 Politou, E., Michota, A., Alepis, E., Pocs, M., Patsakis, C. (2018), *supra nota* 16, 1248.
83 *Ibid*.
84 Eskens, S. (2019). A right to reset your user profile and more: GDPR-rights for personalized news consumers. *International Data Privacy Law*, 0(0). Oxford University Press, 1-20. 13.
85 Li, W. (2018). A tale of two rights: Exploring the potential conflict between right to data portability and right to be forgotten under the General Date Protection Regulation. *International Data Privacy Law*, 8(4). Oxford University Press, 309-317. 313.

3. EVALUATION OF CONSEQUENCES

3.1. Sanctions

Fulfilling the obligations of Article 17 are not the only challenges in itself, because if a corporation does not comply with the obligations, it is possible that it will receive sanctions. Sanctions, such as administrative fines, have been imposed to enforce the implementation of this regulation. MNCs are heavily affected by fines. However, when comparing general fines practices in different countries, they are still looking for their place.[86][87] In addition, according to my interviews, MNCs have not provided a clear picture of the practices of supervisory authorities, which could be used to determine the level of fines or how easily fines will be imposed in practice. Fines may be imposed in place of or in addition to measures imposed by the supervisory authority. In a case of a minor infringement, a reprimand may be issued instead of a fine.[88] Sanctions stemming from MNCs' inability to fulfil the requirements of Article 17 have not only been made uniform, but they have also been increased considerably. I think that administrative fines are raised significantly in order to be taken seriously.

The GDPR lists a number of factors that affects determining administrative fines. Due regard should be given, for instance, the nature, gravity and duration of the infringement. The intentional or negligent character of the infringement may be considered as well as the actions made by the controller to mitigate the damage suffered by data subjects. Also, any relevant previous infringements by the controller should be paid appropriate attention.[89] However, administrative fines are imposed according to the circumstances of each individual case. It is possible for MNCs to have a warning for first offences. For a minor breach, the corporation can be fined up to 2% of its worldwide revenue or 10 million euros, whichever is higher. Then for more serious violations, corporation can be fined up to 4% of worldwide revenues or 20 million euros, whichever is higher.[90]

Even though the GDPR is an EU regulation and it can be applied in a certain territory, it has an impact on the rest of the world as well. For instance, in the case of a breach of Article 17, for an American

[86] *British Airways faces record £183m fine for data breach*. BBC News. Retrieved from https://www.bbc.com/news/business-48905907, 16 February 2020.
[87] *Baden-Württemberg supervisory authority issues first German GDPR fine*. European Data Protection Board. Retrieved from https://edpb.europa.eu/news/national-news/2018/baden-wuerttemberg-supervisory-authority-issues-first-german-gdpr-fine_en, 11 May 2020.
[88] GDPR, Preamble 148.
[89] GDPR, Art.83(2).
[90] Tankard, C. (2016). What the GDPR means for business. *Network Security*, 2016(6). Elsevier, 5-8. 6.

corporation that has presence in the EU, there is a risk existing that the American parent corporation will have to pay the administrative fines calculated from the worldwide revenue.[91] It should be noted that in the case of a data breach not only controllers but also processors are liable for the damages caused to the data subject.[92] Thus, if the corporation uses a data processor and the processor makes a breach, it may therefore be liable for damages resulting from the processing of personal data.

3.2. Towards the future

According to the GDPR, the decision of erasure is made by the controller.[93] The default is therefore that the controller is able to make mainly the right decisions now and in the future. The decision can be appealed to the supervisory authority, but I do not think it was the intention of the legislator that every decision is appealed. Therefore, the MNCs must be able to assess the request in a professional manner and to justify the decision carefully and, if necessary, to prove the measures taken.[94] However, based on what has been previously mentioned, the burden to prove that the erasure has been realised successfully from all available sources may still be technologically questionable. Creating such a process requires a relatively large amount of resources, especially from smaller MNCs. If smaller MNCs do not have the opportunity to carry out such a process, they may, for fear of sanctions, confine themselves to deleting personal data automatically upon request without a separate assessment. However, I think the assessment is worthwhile since, as mentioned before, personal data has the potential to create added value for the corporation.

Without more accurate guidance, the decision practices of different MNCs may differ greatly in the future, as controllers may interpret the requirements of the legislation in different ways. Even the criteria arising from the case C-131/12 judgment cannot be directly linked to anything other than removal requests than for search results. Legislation alone does not provide assistance in justifying removal requests. Since there is no comprehensive case law or well-established guidance on the RtbF yet, thus while waiting, in some cases, MNCs may have to speculate on the content of the legislation.

91 Krystlik, J. (2017), *supra nota* 8, 7.
92 Tikkinen-Piri, C., Rohunen, A., Markkula, J. (2018), *supra nota* 10, 150.
93 GDPR, Art.17(1).
94 GDPR, Art.5(2).

4. PROPOSALS

4.1. Overcoming the challenges

As seen above, Article 17 creates issues for MNCs. However, I prefer to see them as challenges. I see that these challenges are something that put MNCs to the test and to make an effort to successfully fulfil the ruling of Article 17. As it seems in general, the challenges for MNCs created by the ruling of Article 17 are threefold; first, lack of awareness; second, the scattered data and third, uncertainty.

4.1.1. Getting help

In order to meet the challenges arisen from Article 17, the very first step is to know what the requirements are and analyse what the current situation at the corporation is. Only by listing and locating all the data they have, they are able to respond to the removal requests. Once the MNC has surveyed its current situation, it should figure out what concrete changes and actions should be taken in order to fulfil the requirements of Article 17. Measures to meet the requirement of Article 17 and to avoid consequences must be carefully planned. If there is a large gap between the corporation's current practices and the requirements of Article 17, it will require more technical and administrative practical action to catch up.[95]

The GDPR demands MNCs to hire a data protection officer if the core business of the corporation processes large-scale personal data or if the core business of the corporation processes sensitive personal data on a large scale. The corporation may also designate a data protection officer if it deems it necessary.[96] The officer may become necessary to help the corporation to fulfil the purposes of the RtbF since MNCs have challenges with uncertainties in the ruling, especially because they operate in several countries. Thus, with the officer, it is possible to avoid negative consequences for the MNCs, as explained previously. The officer is there for the management and for the personnel to support and help. The officer can train the employees, thus helping the efficiency and productivity by expelling uncertainty.[97] Thus, the officer is able to achieve the positive impact, as has been mentioned at the beginning of this paper, to the corporation. The gap can be caught up and the desired results produced.

[95] Andreasson, A., Riikonen, J., Ylipartanen, A. (2019), *supra nota* 10, 43.
[96] *Ibid*., 14.
[97] *Ibid*., 16.

Since RtbF is a right that data subjects are able to exercise rather easily, the MNCs may well receive more removal requests, thus it is important for a corporation to have knowledgeable personnel who guarantee the practical process of Article 17 since they want to ensure data subject's rights, and thus keep their good reputation intact.

Furthermore, getting help from some other professionals, such as specialist law offices may help. They could give advice and explain the ruling and also draw for instance internal guidelines that may be used to enhance processing, and these guidelines would set certain criteria for employees that must be met in order to delete data. In addition, they may advice to set internal instructions not to store data in certain places, for instance, personal computer or smartphone files, as then there is no need to search for them in the case of a removal request. Furthermore, certain standard phrases given to the data subject justifying the decision to the data subject may also make the processing more efficient. Thus, the tight one-month time limit to respond to a removal request would be simpler to achieve.

Since MNCs have the challenges with scattered data as well, they may consult some IT specialist that after an assessment and an audit may be able to execute analyses and provide best practices for better data managing while taking into account the constraints of Article 17. There are lots of IT best practices starting from the secured e-mail services to Hybrid IT services which allow access to data in different systems, such as cloud and on-premise databases.[98] With the help of a professional, MNCs of all sizes from different industries may be able to find the perfect solution to overcome the challenges that came with the ruling of Article 17. It should be kept in mind, that these systems are complex and change all the time. Thus, the corporation needs to keep up with the development and not to think that the updated practice would be the last one.

However, on the other hand, it needs to be taken into account that it is possible that not every MNC has the resources to hire the data protection officer or specialist from the law office. In such a case, it could at least be considered to nominate someone inside the corporation to be focused on such issues. Furthermore, when it comes to the new updated systems, they may have high costs, and not all of the corporations are ready to invest such amounts. There are also corporations that do not want to move away from old systems because new ones cost a lot of time and money or it is simply very complicated to update the old-fashioned systems to modern ones. They also require commissioning to which they

[98] *Modernize IT Infrastructure in a Hybrid World*. Gartner. Retrieved from https://www.gartner.com/smarterwithgartner/modernize-it-infrastructure-in-a-hybrid-world, 11 May 2020.

may have prejudices. However, I would like to highlight that it is important to keep in mind in such cases that they are not only costs but also profitable investments.

4.2. Special considerations

In the final analysis, controllers are required to implement the ruling of Article 17 in order to follow the regulation and to fulfil the rights of individuals. As a matter of fact, based on abovementioned, this is deemed not to be an easy task. The regulation does not provide any accurate definition of the RtbF regarding its non-trivial practicalities of enforcing such a deletion when personal data have been disseminated to third parties, pseudonymised, anonymised, backed up or archived. [99] In this case, proposed solutions could include cryptographic erasures in which every record in a database is encrypted in advance with a different encryption key and in the case of a removal request the relevant encryption keys could be deleted. One notable point is also that even in the case of a removal request, the data can also be retained if it is properly anonymised since such data are no longer considered personal data.[100] Also, theoretically thinking, MNCs who operate in several countries, also outside of the EU, in this digital and global world, would be helped with uncertainty by worldwide rules.[101] Thus, developing transnational rules of data privacy, including the RtbF, would be one way forward to ensure that the rights of the data subject are met, and privacy protected in this digital era.

[99] Politou, E., Michota, A., Alepis, E., Pocs, M., Patsakis, C. (2018), *supra nota* 16, 1248.
[100] *Personal data deletion*. European Commission. Retrieved from https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/dealing-citizens/do-we-always-have-delete-personal-data-if-person-asks_fi, 10 May 2020.
[101] Fabbrini, F., Celeste, E. (2020). The Right to Be Forgotten in the Digital Age: The Challenges of Data Protection Beyond Borders. *German Law Journal*, 21. Cambridge University Press, 55-65. 65.

CONCLUSION

This study aimed to identify the challenges for MNCs arisen from Article 17 and to present proposed solutions to these legal challenges. Understanding these challenges has high practical relevance to MNCs, as the regulation with its obligations brings novelty to the corporation's practical operations. The RtbF brings considerable changes to corporations' data protection implementation since the data subject has the right for removal request. If corporations have no knowledge where or in which country the data is located, they are at risk to suffer consequences. The hypothesis of this research was that to fulfil the ruling of Article 17 caused challenges for MNCs since it required to change the way to process personal data in order to be prepared for a possible removal request. The survey and analysis presented above prove that the hypothesis of this thesis is true. Due to these changes, corporations need to review their strategies, information systems, and documentation to ensure their alignment with the GDPR provisions. The MNCs should first acquire sufficient knowledge of the GDPR requirements before conducting their reviews, paying attention to the aspects identified in this thesis.

As this thesis proves, applying the RtbF is neither an easy task nor a straightforward process. In the case of a removal request, if corporations do not have clear guidance or an assigned person to take care of it, there will be issues. Thus, it is paramount to locate all the possible personal data. If MNC feels unsure, it can hire a data protection officer or specialist from the law office to guide them and ensure it is possible to fulfil Article 17 obligations in the case of a removal request. In addition, an IT specialist may be able to execute analyses and provide best practices for better data managing. According to ECJ's assessment of the case C-131/12, the process following a removal request needs to be detailed and extensive, thus maintaining such a process is time-consuming and costly. Thus, it is more efficient for the corporations to ensure their actions correspond as perfectly as possible to the ruling of Article 17 so that in the case of a removal request personnel know what to do, and data subjects' rights are ensured. Also, since the GDPR brought a change in that corporations, if necessary, need to prove what they have done to fulfil the obligations of Article 17, it is better for them to conduct preparatory actions as well as possible from the outset. This way, they protect themselves from possible sanctions, guarantee data subjects' rights and at the same time raise their reputation since the data protection is highly valued nowadays in this world of digitalisation.

New regulation always brings challenges. As I have mentioned before, there has been a debate about whether the RtbF should apply to the archives, for instance. Article 17 left many questions

unanswered. Here, more precise regulation would help. Legislators have more likely followed a technology-agnostic approach while defining their functional requirements. However, this approach is on an abstract level taking into account the implementation. It can be said that legislators have purposely avoided recommending specific technical frameworks or privacy methods. The purpose of this approach may be to maintain a possibility to adapt Article 17 within the GDPR ruling to future technological innovations.

As shown in this paper, Article 17 is not the only article in the GDPR that poses challenges to MNCs. In this regard, I see as a possible future research possibility to survey challenges caused by the ruling of Article 33 for MNCs. This is because, in my opinion, between these two articles, there are many similarities with the challenges. Generally, Article 33 demands the controller to make a notification to the supervisory authority within 72 hours in the case of a serious data breach. And, from my point of view, the similarities start from the lack of awareness of the MNCs and the need to locate all the scattered data in order to be aware of which part of the data is affected by the breach and whom it affects. Also, in both of these articles, there has been set a challenging time limit to be met. It would be interesting to compare the results obtained with each other, this would also help for its part to raise awareness and simplify the interpretation of the GDPR.

As mentioned previously, the data protection is a fundamental right. The GDPR is new, and the challenges it poses are real. The regulation brought new rights to individuals, and the RtbF was one of them. However, the corporations may not have recognised all of these new challenges, this in turn, endangers the realisation of individuals' rights. I think this research may help corporations to recognise the potential challenges caused by the ruling of Article 17 and to overcome them. Thus, this research is important from the perspective of both MNCs and individuals. The case law of Article 17 will bring relief to corporate uncertainty in the future, but until then, playing it safe attracts many. This means that it is preferable to erase rather than not to erase data. I would say maintaining privacy is as important in business today as maintaining customer relationships. It is interesting to see what solutions the ECJ will find in the future regarding the RtbF. These assessments or other guidance would help MNCs in case of unawareness about how Article 17 should be applied correctly. As I see it, instead of waiting for relevant case law or more precise regulation, it should be kept in mind that the existing regulation already should be applied in a uniform way. This would guarantee future legal certainty since the goal is good processing of personal data in all industries currently and in the future.

LIST OF REFERENCES

Scientific books

1. Burdon, M. (2020). *Digital Data Collection and Information Privacy Law*. Cambridge, United Kingdom: Cambridge University Press.

2. Cohen, S. (2007). *Multinational Corporations and Foreign Direct Investment*. Oxford, United Kingdom: Oxford University Press.

3. Kenealy, D., Peterson, J., Corbett, R. (2015). *The European Union: How does it work?* (4th ed.) Oxford, United Kingdom: Oxford University Press.

4. Lambert, P. (2018). *Understanding the New European Data Protection Rules*. Boca Raton, USA: CRC Press.

5. Lee, N. (2013). *Counterterrorism and cybersecurity*. New York, USA: Springer.

Scientific articles

6. Agrafiotis, I., Nurse, J.R.C., Goldsmith, M., Creese, S., Upton, D. (2018). A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate. *Journal of Cybersecurity,* 4(1). Oxford University Press, 1-15.

7. Eskens, S. (2019). A right to reset your user profile and more: GDPR-rights for personalized news consumers. *International Data Privacy Law*, 0(0). Oxford University Press, 1-20.

8. Fabbrini, F., Celeste, E. (2020). The Right to Be Forgotten in the Digital Age: The Challenges of Data Protection Beyond Borders. *German Law Journal*, 21. Cambridge University Press, 55-65.

9. Fazlioglu, M. (2013). Forget me not: The clash of the right to be forgotten and freedom of expression on the Internet. *International Data Privacy Law*, 3(3). Oxford University Press, 149-157.

10. Jasmontaite, L. (2018). Gry Hasselbalch and Pernille Tranberg, Data Ethics – The New Competitive Advantage. *International Data Privacy Law*, 8(2). Oxford University Press, 175-177.

11. Krystlik, J. (2017) With GDPR, preparation is everything, *Computer Fraud & Security*, 2017(6). Elsevier, 5-8.

12. Li, W. (2018). A tale of two rights: Exploring the potential conflict between right to data portability and right to be forgotten under the General Date Protection Regulation. *International Data Privacy Law*, 8(4). Oxford University Press, 309-317.

13. Malatras, A., Sanchez, I., Beslay, L., Coisel, I., Vakalis, I., D'Acquisto, G., Sanchez, M.G., Grall, M., Hansen, M., Zorkadis, V. (2017). Pan-European personal data breaches: Mapping of current practices and recommendations to facilitate cooperation among Data Protection Authorities. *Computer Law & Security Review*, 33(4). Elsevier, 458-469.

14. McCarthy, H. (2016). All the World's a Stage: The European right to be forgotten revisited from a US perspective. *Journal of Intellectual Property Law & Practice*, 11(5). Oxford University Press, 360-371.

15. Nieuwesteeg, B., Faure, M. (2018). An analysis of the effectiveness of the EU data breach notification obligation. *Computer Law & Security Review*, 34(6). Elsevier, 1232-1246.

16. Oostveen, M. (2016). Identifiability and the applicability of data protection to big data. *International Data Privacy Law*, 6(4). Oxford University Press, 299-309.

17. 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). Oxford University Press, 1-20.

18. Politou, E., Michota, A., Alepis, E., Pocs, M., Patsakis, C. (2018). Backups and the right to be forgotten in the GDPR: An uneasy relationship. *Computer Law & Security Review*, 34(6). Elsevier, 1247-1257.

19. Romanosky, S. (2016). Examining the costs and causes of cyber incidents. *Journal of Cybersecurity*, 2(2). Oxford University Press, 121-135.

20. Romanosky, S., Ablon, L., Kuehn, A., Jones, T. (2019). Content analysis of cyber insurances polices: How do carriers price cyber risk? *Journal of Cybersecurity*, 5(1). Oxford University Press, 1-19.

21. Sartor, G. (2015). The right to be forgotten in the Draft Data Protection Regulation. *International Data Privacy Law*, 5(1). Oxford University Press, 64-72.

22. Tankard, C. (2016). What the GDPR means for business. *Network Security*, 2016(6). Elsevier, 5-8.

23. Tikkinen-Piri, C., Rohunen, A., Markkula, J. (2018). EU General Data Protection Regulation: Changes and implications for personal data collecting companies. *Computer Law & Security Review*, 34(1). Elsevier, 134-153.

24. Wolters, P.T.J. (2017). The security of personal data under the GDPR: A harmonized duty or a shared responsibility? *International Data Privacy Law*, 7(3). Oxford University Press, 165-178.

EU legislation

25. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). OJ L 119, 4.5.2016.

26. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. OJ L 281, 23.11.1995.

27. Charter of Fundamental Rights of the European Union (EU) 2012/C 326/02, OJ C 326, 26.10.2012.

Finnish legislation

28. Tietosuojalaki 5.12.2018/1050.

29. Työsopimuslaki 26.1.2001/55.

EU Court decisions

30. Judgment of 13 May 2014, Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, C-131/12, EU:C:2014:317.

Other sources

31. Andreasson, A., Riikonen, J., Ylipartanen, A. (2019). *Osaava tietosuojaastaava ja EU:n yleinen tietosuoja-asetus*. Helsinki, Finland: Tietosanoma.

32. Spindler, G., Schmechel, P. (2016). Personal Data and Encryption in the European General Data Protection Regulation. *JIPITEC*, 7(2), 163-177.

33. *Baden-Württemberg supervisory authority issues first German GDPR fine*. European Data Protection Board. Retrieved from https://edpb.europa.eu/news/national-news/2018/baden-wuerttemberg-supervisory-authority-issues-first-german-gdpr-fine_en, 11 May 2020.

34. *British Airways faces record £183m fine for data breach*. BBC News. Retrieved from https://www.bbc.com/news/business-48905907, 16 February 2020.

35. *Data Protection under GDPR*. Official website of the European Union. Retrieved from https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_en.htm, 21 April 2020.

36. *Factsheet on the "Right to be Forgotten" ruling (C-131/12)*. European Commission. Retrieved from https://www.inforights.im/media/1186/cl_eu_commission_factsheet_right_to_be-forgotten.pdf, 20 March 2020.

37. *Modernize IT Infrastructure in a Hybrid World*. Gartner. Retrieved from https://www.gartner.com/smarterwithgartner/modernize-it-infrastructure-in-a-hybrid-world, 11 May 2020.

38. *Personal data deletion*. European Commission. Retrieved from https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/dealing-citizens/do-we-always-have-delete-personal-data-if-person-asks_fi, 10 May 2020.

39. *Pseudonymised and anonymised data*. Office of the Data Protection Ombudsman. Retrieved from https://tietosuoja.fi/en/pseudonymised-and-anonymised-data, 26 April 2020.

40. *What is personal data?* Office of the Data Protection Ombudsman. Retrieved from https://tietosuoja.fi/en/what-is-personal-data, 2 March 2020.

APPENDICES

Appendix 1. Questionnaire

Industry of the corporation: _____

Size of the corporation: _____

QUESTIONS

1. The GDPR is a very topical subject at the moment, what thoughts does the regulation evoke in you as a corporation?
1. Regulation is a major change and affects the activities of the corporation significantly. How did the entry into force of the GDPR change your way of doing business?

Article 17 The right to erasure (the "right to be forgotten") is one of the major changes based on my research. It states that the data subject has the right to have the controller delete personal data concerning the data subject without undue delay, and the controller has an obligation to delete personal data without undue delay, unless, for instance, the controller has a legitimate reason to process personal data. At worst, personal information is scattered across many different places. This requires IT capabilities to ensure that personal information is not left unauthorised on various systems - such as log files, backups or printouts. The use of time and resources may also pose challenges in the event of a removal request if the corporation does not have a specific designated person to take care of the matter within a certain time frame.

1. What challenges does this cause in your corporation?
2. How do you think these challenges and the legal problems they bring can be solved or how have they been solved in your corporation?
3. What will happen in your corporation if the data subject approaches you on such a matter and wants his or her personal data to be removed from your systems? (What would you respond to the data subject? Is there a nominated person in your corporation to take care of the matter? Are there any legal obligations to keep the information in the register?)

Infringements may be subject to an administrative fine of up to EUR 20 000 000 or, in the case of a corporation, 4% of the total annual worldwide turnover for the preceding business year, whichever is the higher.

1. As a corporation, are you prepared for possible fines? What thoughts do these sums evoke in you as a corporation?

Something else you would like to share concerning these matters: _____

Appendix 2. Non-exclusive licence

Non-exclusive licence for reproduction and for granting public access to the graduation thesis[1]

I Linda Lehtiniemi

1. Give Tallinn University of Technology a permission (non-exclusive licence) to use free of charge my creation

Analysing the challenges of Article 17 of the EU General Data Protection Regulation for multinational corporations,

supervised by Jenna Uusitalo,

1.1. to reproduce with the purpose of keeping and publishing electronically, including for the purpose of supplementing the digital collection of TalTech library until the copyright expires;

1.2. to make available to the public through the web environment of Tallinn University of Technology, including through the digital collection of TalTech library until the copyright expires.

2. I am aware that the author also retains the rights provided in Section 1.

3. I confirm that by granting the non-exclusive licence no infringement is committed to the third persons' intellectual property rights or to the rights arising from the personal data protection act and other legislation.

---

[1] *The non-exclusive licence is not valid during the access restriction period with the exception of the right of the university to reproduce the graduation thesis only for the purposes of preservation.*