FACULTY OF LAW
Lund University

Bajramović Sanjin

Issues of uniform application of General Data Protection Regulation

JAEM01 Master Thesis

European Business Law
15 higher education credits

Supervisor: Justin Pierce

Term: Spring 2017

TABLE OF CONTENTS

List of Abbreviations

CJEU	Court of Justice of European Union
DSM	Digital Single Market
EC	European Commission
EU	European Union
GDPR	General Data Protection Regulation
MS	Member State
TFEU	Treaty on Function of European Union

Abstract

As a respond to the development of Internet and Digital technologies, EU listed creation of Digital Single Market (hereinafter referred to as: "DSM") as a strategic goal. The development of DSM would contribute in securing competitiveness within the Union. Establishment of DSM inevitably raises an issue of data management in the EU and in order to successfully form DSM, EU needs to create a harmonious and uniformly applicable legal data protection framework. Data protection framework was created by adoption of Data Protection Directive in 1995[1] (hereinafter: "Directive 1995"). Directive 1995 was framed to the specific needs of the market that were matter of concern in 1995, but recent development had shown that Directive 1995 cannot answer nor resolve all the current issues. As a step in improving data protection framework, EU has adopted a GDPR[2]. In preamble of the GDPR it is emphasized that *"legal and practical certainty for natural persons, economic operators and public authorities should be enhanced".*[3] This thesis will evaluate capabilities of GDPR in achieving this aim. In addition, it is aiming to discover potential issues that may arise in the application of GDPR.

The thesis will be divided in two sections: The first section covers issue of GDPR regarding long list of derogations left at the competence of Member States. Due to the page constraints of the thesis, the focus will be only on those derogations that can significantly impede the objectives of GDPR. Additionally, in the first section author will talk about the different legal instrument used by EU in creation of data protection framework and difference between regulation and directive.

Second section of the paper will try to discover how uncertain it is going to be to enforce the rights provided by GDPR due to the possibilities of derogations mentioned in the first section of the paper. Focus will be on two practical issues, (a) the content data expressed by the users of social networks acting outside of the scope of household activities, and (b) enforcement of the right to be forgotten in national courts after Google Spain case.

[1] 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 [1995] OJ L-281/31

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

[3] Reg 2016/69 OJ L 119/2

The thesis concludes by drawing the conclusions from the section one and section two which evaluate the effect of the GDPR in creation of harmonious legal data protection framework across EU.

Introduction

One of EU's listed priorities is the establishment of DSM within the European Union[4]. DSM is defined as *"one in which the free movement of persons, services and capital is ensured and where the individuals and businesses can seamlessly access and exercise online activities under conditions of fair competition, and a high level of consumer and personal data protection, irrespective of their nationality or place of residence"*.[5] The purpose of DSM is to create an environment in which consumers and economic operators are going to be able to fully access to the goods and services without fear of infringement of any of their rights and in case of infringement of such rights, they will be able to fully enforce their rights. In order to successfully establish DSM, EC has identified three policy areas or "pillars" which require additional regulation: "Better access for consumers and businesses to online goods"[6], "The right environment for digital network and services"[7] and "Economy and Society"[8]. As a part of regulating mentioned specific pillars, EU identified the creation of European Union Data Protection Laws as area of significant importance. Brief background about the data protection laws will be discussed in the next paragraphs.

EU Data Protection laws were first adopted in 1995 as a response to the fast growing internet services at that time. Having in mind the difference in levels of protection of rights and freedoms of individuals, but most notably the right of privacy, and as this difference may create an obstacle to the free market[9] EU institutions, but more precisely The Council of the EU and European Parliament have adopted a Directive on the protection of individuals with

[4] 'Priorities' (European Commission - European Commission, 2017) <https://ec.europa.eu/commission/priorities_en> accessed 23 May 2017
[5] 'Digital Single Market' (Digital Single Market, 2017) <https://ec.europa.eu/digital-single-market/en/digital-single-market> accessed 23 May 2017
[6] 'Better Access For Consumers And Business To Online Goods' (Digital Single Market, 2017) <https://ec.europa.eu/digital-single-market/node/78515> accessed 23 May 2017
[7] 'Right Environment For Digital Networks And Services' (Digital Single Market, 2017) <https://ec.europa.eu/digital-single-market/node/78516> accessed 23 May 2017
[8] 'Economy & Society' (Digital Single Market, 2017) <https://ec.europa.eu/digital-single-market/node/78517> accessed 23 May 2017
[9] 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 [1995] OJ L-281/31

regard to the processing of personal data and on the free movement of such data[10] also referred to as "1995 Data Protection Directive". According to the Union law, more precisely Article 288 of TFEU, the institutions of EU, in exercise of their competences, are able to adopt regulations, directives, recommendations and opinions.[11] The legal instrument used to address the data protection issues is a "directive". As opposed to regulation, directives provide more discretion to the MS who are required to interpret and transpose the directives in the national law[12]. Due to the fact that MS needs to interpret directive, there is a high possibility of different interpretation which in the end leads to the fragmentation of data protection law among MS. This leads to the increase in the administrative compliance costs and costs of adjustment to different technical setting for each MS, resulting in increased financial burden on the individuals as well as economic operators acting in the field of data protection. For that reason choice of regulation as a legal instrument would be much more appropriate in creation of unified and harmonious legal framework as regulation is having a general application within the EU, it does not require interpretation and transposition to national laws and it is binding in its entirety and directly applicable in all MS[13]. For that reason, choice of a regulation as legal instrument is indication of the necessity to harmonize certain area, in this case data protection laws.

Due to the fast technological progress, Internet development, introduction of online business, the ability of consumers to acquire goods and services online, the 1995 Directive could not answer all the needs of the market. Development of Web 2.0 which in accordance with online Oxford dictionary is defined as *"the second stage of development of the Internet, characterized especially by the change from static web pages to dynamic or user-generated content and the growth of social media"*[14]. The creation of social networks has opened another possibility for individuals to expose themselves, new ways of sharing personal data through the social networks have become a part of everyday activities, moreover, the pace of technological change and globalization have changed the way the personal data is processed and acquired.[15] EU has noticed these issues and identified them in the preamble of white

[10] ibid
[11] Consolidated version of Treaty on functioning of European Union [2008] OJ C 326/171
[12] Consolidated version of Treaty on functioning of European Union [2008] OJ C 326/172
[13] Consolidated version of Treaty on functioning of European Union [2008] OJ C 326/171
[14] 'Web 2.0 - Definition Of Web 2.0 In English | Oxford Dictionaries' (Oxford Dictionaries | English, 2017) <https://en.oxforddictionaries.com/definition/Web_2.0> accessed 23 May 2017
[15] Communication from the Commission to the European Parliament, the Council, the European economic and social committee and the Committee of the regions - Safeguarding Privacy in a Connected World A European Data Protection Framework for the 21st Century – COM/2012/09 final – paragraph 1

paper "Safeguarding Privacy in a Connected World - A European Data Protection Framework for the 21st Century".[16] The EU intervened in regulating this area in order to protect their citizens. This created the incentive for European Commission to engage more in adjustment of their policies within DSM, more precisely adoption of new data protection law.

As a response to the issues listed above, which were confirmed by the EC in white paper "Safeguarding Privacy in a Connected World A European Data Protection Framework for the 21st Century"[17], Council of European Union, European Commission and European Parliament adopted **'**Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)'[18]. In accordance with the Article 94 of GDPR, the 1995 Directive will be repealed as of 25th of May 2018.[19] The new GDPR will become a single law that is applicable in all MS of EU. The national laws of MS that are currently effective will be non applicable, due to primacy of EU law over the national law.**[20]** The predominant aims of new GDPR are to 'strengthen fundamental citizens' rights and facilitate business by simplifying rules for companies in Digital Single Market'**[21]**. Secondly, in accordance with the assessment provided by the European Commission, new GDPR 'as a single law should do away with the current fragmentation and costly administrative burdens, leading to savings for businesses of around €2.3 billion a year'[22]. The most significant difference in terms of legislation of data protection is the change in the legal instrument, EU legislators decided to use regulation as a form of the legislation instrument. The difference between regulation and directive has been indicated in previous paragraph. The fact that EU decided to use regulation as a legal instrument is an indicator of the need to harmonize data protection framework. Choice of Regulations as a legal instrument is capable of creating unified and harmonious legal framework for the business and companies operating in the European Union, which was, as previously stated, one of the aims and objectives of Data Protection reform.

[16] Communication from the Commission to the European Parliament, the Council, the European economic and social committee and the Committee of the regions - Safeguarding Privacy in a Connected World A European Data Protection Framework for the 21st Century – COM/2012/09 final
[17] ibid
[18] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L 119/1
[19] Reg 2016/679 OJ L 119/86
[20] Case C-6/64, *Falminio Costa v. ENEL* [1964] page 594.
[21] 'Reform Of EU Data Protection Rules - European Commission' (Ec.europa.eu, 2017) <http://ec.europa.eu/justice/data-protection/reform/index_en.htm> accessed 12 May 2017.
[22] Ibid

The question that arises and that will be discussed in the thesis is whether the change of the legal instrument from directive to regulation is sufficient to bring about the desired harmonisation? Is the GDPR clear enough to achieve this aim?

Section one

Introduction

Initially, the new GDPR in general has a long list of derogations from its provisions, which jeopardizes the unanimous and harmonious application of the GDPR. Derogations are defined, in accordance with online Oxford dictionary, as *"exemptions from or relaxation of a rule of law".*[23] The existence of derogations in the legislation is leaving a MS to be exempted from certain provision or section of law and it is usually under condition of protection of certain principles of EU law, generally the protection of fundamental rights and principle of proportionality. This means that even MS who derogate from certain rules are allowed to do so under requirement of respect of principles of proportionality and protection of fundamental rights. The issue with the derogation is that they create different rules in different MS which eventually develops non-harmonious legal framework which results in additional financial costs for Controllers[24] of personal data, as they must adjust to the different set of rules in different Member States. Due to the space constraint the entire regulation cannot be considered in detail, for that reason the thesis will cover Article 6 (2) which relates to lawfulness of data processing, more precisely lawfulness of processing of personal data published by users of social networks who are acting outside of the household activity. Moreover, the thesis will cover Article 23 which restricts Data Subject[25] rights and how the derogations create issues in uniform application of right to be forgotten[26] defined by Article 17 of GDPR. The thesis will take into consideration the application of right to be forgotten in national courts of MS as illustration of different application of Google Spain[27] case, due to its vague and ambiguous terms.

[23] 'Derogation - Definition Of Derogation In English | Oxford Dictionaries' (Oxford Dictionaries | English, 2017) <https://en.oxforddictionaries.com/definition/derogation> accessed 23 May 2017
[24] Reg 2016/679 OJ L 119/33
[25] ibid
[26] Reg 2016/679 OJ L 119/43
[27] Case C-131/12 *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos(AEPD) and Mario Costeja González* [2014] ECLI:EU:C:2014:317

1. Derogations from lawful data processing

Article 6 (2) of GDPR entitles a MS to "maintain" and "introduce" more detailed requirements to ensure "fair" and "lawful" processing of personal data, with regards to Article 6 (1) sub-sections (c) to (e)[28]. The issue in this section is the fact that Article 6 (1) (d) applies when *"processing is necessary to protect vital interest of data subject or of another natural person."*[29] Term "vital interest" is not defined by the GDPR and it is a very broad, ambiguous and generally applicable term. This may represent a serious issue for the data Controllers[30]. Term such as "vital interest" creates additional uncertainty in terms of interpretation of the law, which results in undermining one of the fundamental principles of EU – legal certainty. When harmonising certain legal fields, EU may choose different approaches, for example, EU may opt for exhaustive harmonisation[31], minimum harmonisation[32] and optional harmonisation[33]. Exhaustive (maximum) harmonisation means that EU is setting the standards and does not allow MS to go over these standards. This approach is useful for avoidance of "gold-plating"[34] where the EU is trying to avoid over-regulating certain area which leads to creation of unnecessary administrative compliance burden. On the other hand, minimum harmonisation approach tends to set the lowest standards and creates an obligation for a MS not to go below but allows MS to impose higher standards. In the Recital 10 of the 1995 Directive it stated that *"...the approximation of those laws must not result in any lessening of the protection they afford but must, on the contrary, seek to ensure a high level of protection in the Community;".*[35] It is reasonable to assume that Recital 10 implies that EU used minimum harmonization approach for regulation of data protection law. The issue of minimum harmonization approach lies in the ability of MS to impose higher standards of protection than those provided by the directive. The similar issue was in the application of Right to be forgotten where the CJEU left for the national courts to strike fair balance between, on the one hand, freedom of expression and right of privacy and protection of personal data, on the other.[36] This led to the imposition of different levels of

[28] Reg 2016/679 OJ L 119/36
[29] ibid
[30] See supra note 27
[31] Catherine Bernard, *The Substantive Law Of The EU* (5th edn, Oxford University press 2016) pg. 582
[32] Ibid – pg. 586
[33] Ibid
[34] 'Glossary - European Commission' (Ec.europa.eu, 2017) <http://ec.europa.eu/smart regulation/guidelines/ug_chap8_en.htm> accessed 23 May 2017
[35] Dir 95/46/EC OJ L 281/32
[36] Case C-131/12 *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González* [2014], ECLI:EU:C:2014:317 – paragraph 81

protection to the freedom of expression, and consequently different application and interpretation of right to be forgotten by national courts of MS.

The thesis did not go into evaluation of specific national legislation that derived out of the 1995 Directive, but it went through the analysis of the application of Article 12 (b) of the 1995 Directive which was legal ground for creation of "Right to be forgotten" in the Google Spain[37] case. The analysis will include interpretation of national courts while striking a balance between freedom of expression, on one hand, and rights of privacy and protection of personal data, on the other. This analysis will be used as an example to illustrate issue with the use of vague and undefined terms such as one in the Article 6 (2) "vital interest".

2. Derogations of data subject rights

The rights of data subjects are provided for in Chapter 3 of GDPR[38]. This paper will only cover the right to be forgotten which is provided by Article 17 of the GDPR which states that Data Subjects[39] shall have right of erasure (Right to be forgotten)[40]. It is important to indicate that current Right to be forgotten originated from CJEU's judgment in Google Spain[41] case, where the CJEU said that *'operator of a search engine is obliged to remove from the list of results displayed following a search made on the basis of a person's name links to web pages, published by third parties and containing information relating to that person*'[42]. The previous provision was reframed and set in Article 17 of GDPR but the issue that may arise in the interpretation of RTBF was provided by Article 23 of GDPR which provides a restriction on Data Subject Rights and states that *'...Member State law to which the data controller or processor is subject may restrict by way of a legislative measure the scope of the obligations and rights provided for in Articles 12 to 22...*'. Different laws of MS might create a different application of the Data Subject Rights provided by General Data Protection Regulation. This issue will be discussed more in depth in Section two of this paper.

[37] See supra note 27
[38] Reg 2016/679 OJ L 119/39
[39] See supra note 25
[40] Reg 2016/679 OJ L 119/43
[41] See supra note 27
[42] Case C-131/12 *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos(AEPD) and Mario Costeja González* [2014] ECLI:EU:C:2014:317 - paragraph 88

Conclusion of section one

To conclude, above-mentioned derogations are only some of the derogations provided by provisions of General Data Protection Regulation, in depth reading of it can reveal even more places where the competence to regulate was left on the Member State. Therefore the question that arises here is why did the legislator opt for a regulation as a legal instrument when in its very content it had created some type of a hybrid regulation-directive? Moreover, regulating data protection in the EU might result to the creation of additional financial burden or implications on the controllers due to the broad use of derogations. This section will be concluded with the following paragraph "*However, the large number of derogations and their potential broad scope is likely to result in many international companies having to continue to deal with national data protection law variations across numerous Member States to ensure compliance with the varying EU data protection requirements."*[43]

Section Two

Introduction

This section discusses the practical problems which may arise in application of GDPR concentrating on two issues, (a) issue of lawfulness of the content data expressed by the users of social networks acting outside of the scope of household activities, and (b) enforcement of the right to be forgotten in national courts after Google Spain[44] case. The first issue will be evaluated from the point of view of users of social networks being data controllers. Second issue will be explored from the point of view of French and Dutch courts implementing right to be forgotten after Google Spain[45], more precisely striking balance between freedom of expression, on one hand and right of privacy and protection of personal data, on the other and whether the issues in different application of right to be forgotten can be solved by newly framed Article 17 in relation to Article 23 of GDPR?

[43] William Long and Francesca Blythe, 'Member States' Derogations Undermine The GDPR' (Privacy laws& business United Kingdom report 2016)
[44] See supra note 27.
[45] ibid.

1. Content data expressed by the users of social networks acting outside the scope of household activities

The development of Web 2.0, which is defined by online Oxford dictionary as *"the second stage of development of the Internet, characterized especially by the change from static web pages to dynamic or user-generated content and the growth of social media"*[46] has created additional problems for the citizens and legal entities in EU[47]. The question that first arises is what happens if content generated by user is a personal data? Does that mean that users become data controllers? Article 2(2)(c) of GDPR answers the first question by defining material scope of regulation and stating that *"This Regulation does not apply to the processing of personal data: ... (c) by a natural person in the course of a purely personal or household activity;"*[48] Then the question remains what does the term "household activity" means? The Court gave criteria in *Lindquist*[49] case where it stated *"That exception must therefore be interpreted as relating only to activities which are carried out in the course of private or family life of individuals, which is clearly not the case with the processing of personal data consisting in publication on the internet so that those data are made accessible to an indefinite number of people*[50]*".* So the Court said that publications to the indefinite number of people are not in the course of private or family life of individuals, therefore not under the household activity exemption. Does that mean that any post on social network that is labelled "Public[51]" is a post that is shared to indefinite number of people? If yes, then even the user of social network can be classified as data controller in the sense of GDPR. For the purpose of applicable law Data Controller is taken to mean *'...the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data..."* Data Controllers as such are required by GDPR to certain set of obligations when processing personal data, specifically and for purpose of the thesis, Article 6 of GDPR – "Lawfulness of processing"[52] and Article 17 of GDPR "Right of erasure/right to be forgotten". These issues are further elaborated in the thesis.

[46] See supra note 23
[47] See Introduction paragraph 3
[48] Reg 2016/679 OJ L 119/32
[49] Case C-101/1 *Lindquist* [2003] ECLI:EU:C:2003:596
[50] Ibid paragraph 47
[51] 'What Is Public Information? | Facebook Help Centre | Facebook' (Facebook.com, 2017) <https://www.facebook.com/help/203805466323736> accessed 16 May 2017
[52] Reg 2016/679 OJ L 119/36

a) Lawfulness of processing of personal data under consent

Principles of processing personal data are defined by Article 5 of GDPR and first principle requires personal data to be *'processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency')".*[53] The principle of lawfulness is further elaborated in Article 6 of GDPR.[54] In order to fulfil this obligation, user of social network acting as a data controller needs to acquire consents of every data subject that is subject of his public social network post. In order for user of social network acting as a data controller to fulfil this obligation there must be a technical requirement set by social network service provider, which requires every public post to fulfil "consent" criteria. Additionally, if GDPR is applicable to the users of social networks as data controllers acting outside the scope of household activities then the latter shall enforce the rights of data subjects provided by GDRP. Right to erasure specified by Article 17 (1) (b) of GDPR entitles a data subject to have personal data removed/erased if it has withdrawn its consent for such processing[55]. This means that social user shall remove the personal data regarding another data subject if it does not have its consent. As this may be a burden on users of social networks as data controllers, this is also a burden on social network service providers. In order to create environment capable of lawful processing of data subjects personal data by users of social networks, social network service providers shall include "approval requirement". Approval requirement can be used for processing of pictures containing more than one person. For example, Facebook has already implemented and is using a "face recognition technology"[56], so it can be used to identify number of the persons on the picture and to require number of consents equal to the number of the persons recognized by the face recognition technology. The personal data that is subject of "approval requirement" can be under "pending" status as long as it does not fulfill the criteria. The next paragraph is exploring further the issues of lawfulness of processing personal data, specifically lawfulness of protection necessary for the protection of "vital interest".

[53] Reg 2016/679 OJ L 119/35
[54] See supra note 52.
[55] Reg 2016/679 OJ L 119/44
[56] 'How Does Facebook Suggest Tags? | Facebook Help Centre | Facebook' (Facebook.com, 2017) <https://www.facebook.com/help/122175507864081?helpref=faq_content> accessed 11 May 2017.

b) Lawfulness of processing for protection of "vital interest"

"Lawfulness of processing" is defined by Article 6 (1) of GDPR and it states that *'processing shall be lawful only if and to the extent that at least one of the following applies:"*[57] and in paragraph (d) it states that "*(d) processing is necessary in order to protect the vital interests of the data subject or of another natural person".*[58] This paragraph has been a subject of discussion in Section one of the thesis from the perspective of being subject of derogation by the Member States under Article 6 (2) of GDPR. Requirement under Article 6 (1) (d) can be subject of additional technical adjustments on behalf of social network service provider. For example, if public post published by user of social network acting as a data controller outside the scope of household activity does not fulfil consent criteria, then social network service provider shall allow an option to check whether it is in the "vital interest" of "another natural person" to publish the post. This is very costly burden on the social network service provider, especially due to the fact that Article 6 (1) (d) is subject of derogations and thus it is highly probable that it will be different among Member States. Potential issue that may arise out of protection of "vital interest" is that social network service providers will be acting as a body who is obliged to determine whether publication of certain Data subject's[59] personal data is in "protection of vital interest" of either "data subject" or "another natural person"[60]. Having an obligation on social service provider to act as body determining "protection of vital interest" is problematic from the perspective of human resources qualified for such decision. The problem of different interpretation of the term "vital interest" can create non-harmonious application of the GDPR. This can be a very costly burden on the social network services providers, but even more for the users of social network acting as data controllers outside of the household activity, as it is unreasonable to expect that every user posses necessary knowledge for performance of such task. Additional obligation for the data controllers is requirement to inform data subjects about recipients of the personal data[61]. This obligation will be shortly elaborated in next paragraph with aim of illustrating irrationality of imposition of such obligation on users of social network as data controllers.

[57] Reg 2016/679 OJ L 119/36
[58] ibid
[59] See supra note 25.
[60] See supra note 57.
[61] Reg 2016/679 OJ L 119/40

c) Information to be provided where personal data are collected from the data subject

Article 13 (1) of GDPR requires controllers to provide certain information to the data subject whose data they are processing[62]. For the purpose of this section, we are going to talk about requirement under Article 13 (1) (e) which states that controller needs to inform data subject about *"(e) the recipients or categories of recipients of the personal data, if any"*[63]. Examination of this obligation from the perspective of user of social network acting as a data controller highlights the issue that it remains difficult and an unreasonable burden to require the data subject to be informed about the specific recipients of their personal data, as it can be anyone. The only idea that comes to author's mind is to deliver a general message to data subject which states that publication is "Public" and can be seen by anyone. In the author's opinion purpose of obligation imposed by Article 13 (1) of GDPR is to inform data subject about physical/legal entities that are processing their personal data and if this obligation will be fulfilled by stating that it can be seen by "anyone" than the very substance of the right is being jeopardized. Next paragraph will be exploring the obligation of data controllers to respect the rights of data subjects provided by GDPR, specifically right to be forgotten.

d) Right to be forgotten under GDPR

Right to be forgotten as provided by Article 17 of GDPR entitles data subject to erase personal data that is: "*(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; (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)"*[64]. Having the obligation on the burden of user of social network acting as a controller is highly impracticable, for the same reason as it is impracticable to impose an obligation to interpret the term "vital interest"

[62] Ibid
[63] Reg 2016/679 OJ L 119/41
[64] Reg 2016/679 OJ L 119/43

(lack of human resources capable of performing such task). This thesis will illustrate how difficult it is for the national courts to strike a balance between freedom of expression, on one hand and right of privacy and protection of personal data on the other, so having the same obligation on the user of social network seems irrational. The discussion about right to be forgotten and its application at national court's level will be in the second part of section two of this paper. The subject of discussion will be obligation of national courts to strike a balance between freedom of expression and right of privacy and protection of personal data. Difficulties of such task are related to the vagueness, ambiguousness and lack of clarity in performance of such task, which is the same potential issue with application of above-mentioned articles of GDPR.

The question that remains to be answered is whether social users acting as data controllers outside the scope of household activity are going to be data controllers in the sense of GDPR?

One of the possible solutions for the issue of differentiation between user of social network acting as a controller was addressed in the paper written by Brendan Van Alsenoy & Joris Ballet & Aleksandra Kuczerawy & Jos Dumortier – "Social networks and web 2.0: are users also bound by data protection regulations?", where authors of the paper introduced a notion of decision making power to the controllers. They are suggesting that "*an entity must exercise at least some level of decision-making power with regards to both the purposes and means of a particular processing operation."*[65] They are differentiating between purposes and means of processing, identifying user of social network as the one that exercises the decision-making power over the purpose as every person has autonomy in choice of purpose for which they are publishing certain data and on the other hand technical means where the user does not enjoy free choice, so this portion of decision-making power lies on the social network service provider[66]. This approach was written in the context of 1995 Data Protection Directive but as it seems it was disregarded by legislators when they were adopting new GDPR even though in my opinion it would perfectly fit and resolve the issues explained and listed above.

[65]Brendan Van Alsenoy and others, 'Social Networks And Web 2.0: Are Users Also Bound By Data Protection Regulations?' (2009) 2 Identity in the Information Society.
[66] Ibid paragraph 2

2. Google Spain case and its application in national courts of Netherlands and France

a) Google Spain SL and Google Inc. v Agencia Española de Protección de Datos[67]

Facts

Mr. Costeja filed a complaint at Agencia Española de Protección de Datos (AEPD) against La Vanguardia, Google Spain and Google Inc. The complaint was based on the fact that when user types the name of Mr. Costeja in the Google search engine, the search results include two pages of La Vanguardia newspapers with articles about Mr. Costeja connected to his recovery of social security debts[68]. By the above-mentioned complaint Mr. Costeja requested from La Vanguardia to remove articles or to adjust them in such manner not to show any of his personal data and additionally he requested Google to remove or conceal the personal data from the search results. Mr. Costeja based his request on the fact that personal data are no longer relevant[69]. The complaint was upheld against Google but was rejected against La Vanguardia, and for that reason Google brought an action against APED.[70]

Ruling of Google Spain case

The Court in its ruling concluded that Google, as a search engine, is a controller of personal data within the meaning of 1995 Data Protective Directive[71] and as such *"in order to comply with the rights laid down in those provisions and in so far as the conditions laid down by those provisions are in fact satisfied, the operator of a search engine is obliged to remove from the list of results displayed following a search made on the basis of a person's name links to web pages, published by third parties and containing information relating to that person, also in a case where that name or information is not erased beforehand or simultaneously from those web pages, and even, as the case may be, when its publication in itself on those pages is lawful.[72]"* Google Spain created an avalanche of comments and articles from scholars about relation between Freedom of privacy and Protection of personal

[67] Case C-131/12 *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González* [2014], ECLI:EU:C:2014:317
[68] ibid paragraph 14
[69] Case C-131/12 *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González* [2014], ECLI:EU:C:2014:317, paragraph 15
[70] Ibid paragraphs 16, 17 and 18
[71] Ibid paragraph 41
[72] Ibid paragraph 88

data with Freedom of Expression within the EU, especially because of paragraph 99 where the Court said that *"As the data subject may, in the light of his fundamental rights under Articles 7 and 8 of the Charter, request that the information in question no longer be made available to the general public on account of its inclusion in such a list of results, those rights override, as a rule, not only the economic interest of the operator of the search engine but also the interest of the general public in having access to that information upon a search relating to the data subject's name"*[73]

Freedom of privacy and Protection of Personal data are both listed in Charter of fundamental rights of European Union (hereinafter: "the Charter"), more precisely in Article 7 and Article 8, respectively[74]. The Charter has equal legal value as the Treaty on function of European Union and Treaty on European Union[75]. Additionally, the Charter also provides in Article 11 Freedom of expression and information[76], which consists of the *"freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers".* In author's opinion, provision 99 of the Google Case judgment[77] is the one that creates the most problems for national courts. CJEU has given a greater legal value to the protection of Article 7 and 8 of the Charter compared to economic rights of operators and general interest in access to information. This provision serves as an indicator for balancing between rights of freedom of expression and right to privacy and protection of personal data. In author's opinion and as it may be seen from the national court cases, the courts of MS have disregarded provision 99 and they have given a greater significance to the freedom of expression instead of supporting Article 7 and 8 of the Charter as it was stated in the ruling of Google Spain case.[78] CJEU has additionally confused national courts with the provision 81 of the ruling where they stated that "*...Whilst it is true that the data subject's rights protected by those articles also override, as a general rule, that interest of internet users, that balance may however depend, in specific cases, on the nature of the information in question and its sensitivity for the data subject's private life and on the interest of the public in having that information, an interest which may vary, in particular, according to the role played by the data subject in public life."*[79] In this provision, CJEU has acknowledged the

[73] Case C-131/12 *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González* [2014], ECLI:EU:C:2014:317, paragraph 99
[74] Charter of Fundamental Rights of European Union [2000] C 364/10
[75] Consolidated version on Treaty of European Union [2012] C 326/19
[76] Charter of Fundamental Rights of European Union [2000] C 364/11
[77] See supra note 73.
[78] See supra note 27.
[79] See supra note 36.

provision 99[80], but this had created a possibility for the national courts to disregard it on the grounds of protection of freedom of expression. In the author's opinion this provision is slightly contradicting the provision 99[81] as the latter strengthens rights of data subjects, more precisely their rights provided by Article 7 and 8 of the Charter, but then the provision, 81 states that "nature of the information" shall be taken in consideration especially if the data subject is playing the role in "public life". Both of these terms are vague, they lack clarity and thus create a possibility of non-harmonious application of the ruling. Precisely this is going to be discussed in the next sub-section of the thesis where author explores application of the Google Spain ruling in the cases before national courts of France and the Netherlands.

b) Application of Google Spain ruling in national courts of the Netherlands and France

With all of that being said, duty to respect the Charter, duty to respect Google Spain ruling[82], national courts have faced difficulties in interpretation and application of right to be forgotten. The most difficult issue is successfully assessing and striking fair balance between the Freedom of privacy and Right to protect personal data with Freedom of expression, due to the lack of clarity of provisions of Google Spain case.[83] It should be kept in mind, the obligation of *"judicial authorities of the Member States, which are responsible for ensuring that Community law is applied and respected in the national legal system"*.[84] Also, it should be noted that the exclusive competence for the interpretation of the acts of EU institutions is left to the CJEU, under the Article 267 of TFEU.[85] National courts of MS must be careful not to interfere with the exclusive competence of the CJEU by giving a different interpretation to the acts of EU institutions. The next following paragraphs will discuss the application of Google Spain ruling in the context of national courts of the Netherlands and France.

The Netherlands

Arthur van M. v. Google Netherlands and Google Inc[86]

[80] See supra note 73.
[81] ibid
[82] See supra note 27.
[83] ibid
[84] Case C-2/88 J. J. Zwartveld and Others [1990] I-3372
[85] Consolidated version on Treaty of function of European Union [2012] OJ C 326/164
[86] European Court of Human Rights judgments on the right to freedom of expression - Bulletin LVIII: THE 'RIGHT TO BE FORGOTTEN' - 24 May 2015, pg 1

In 2012 Dutch TV broadcasted hidden camera footage where a man, Arthur van M, was discussing with an assassin how to best kill competitors[87]. Dutch TV did not refer to full name of the person but referred only to the full first name and first letter of his last name[88]. The footage was later used as evidence in criminal case to convict Arthur van M and he was sentenced to 6 years imprisonment[89]. Additionally, his story was inspiration for Angel Engelbertink who wrote and published a book about it with the main character, who commissioned assassination, being called Arthur van M. Later on, Arthur van M requested Google to delist some of links displayed when searcher types his name[90]. Google refused to delist links which eventually resulted in Arthur van M starting a procedure at District Court of Amsterdam where he invoked the Google Spain case but District Court rejected his arguments, so he appealed to the Court of Appeals of Amsterdam.[91]

Court of Appeals of Amsterdam started its reasoning by pointing out the fact that Arthur van M was prosecuted for the serious offence and confirms that he is convicted in the first instance court.[92] Also, it emphasized the fact that public is already showing the interest in his case since the articles are being published[93]. The Court of Appeals also states that articles in search results are only displaying Arthur van M's initials but not his full name[94]. So, users who search under his full name cannot claim with certainty that this is him, unless they know other information about him which will identify him personally[95]. Arthur van M argued that searchers can use a book written with the character who is named same as him to relate it to him, but the Court of Appeals disagreed and stated that book is a mix of fiction and facts and in book there was actual assassination commissioned by main character which is different than in real life and for that reason public cannot relate to him[96]. The Court of Appeals of Amsterdam rejected all the claims stated by Arthur van M and he lost the case.

When balancing between personal data protection right and freedom of expression, Court of Appeals of Amsterdam put more emphasize in the protection of freedom of expression. The decision of Court of Appeals is setting a low threshold for the public interest

[87] 1 Eur. Data Prot. L. Rev. 118 2015
[88] ibid
[89] Ibid
[90] ibid
[91] ibid
[92] ibid
[93] ibid
[94] Ibid
[95] ibid
[96] Ibid

requirement, as any person who commits a serious criminal offence can be seen as a person of public interest, the one only needs to be written about in the news. This is contrary to the standard set by the Google Spain ruling, more precisely standard set in the provision 99 where the CJEU states that *"that the interference with his fundamental rights is justified by the preponderant interest of the general public in having, on account of its inclusion in the list of results, access to the information in question".*[97] The standard set in provision 99 of Google Spain ruling is that there has to be "preponderant" interest of general public, so the question is whether the mere publication of article in the media can constitute "preponderant interest of general public"? For the purpose of comparison and definition of term "preponderant", thesis will explore the similar standard from civil case law. "Preponderance of evidence" standard in a civil law cases means that *"more than 50% of evidences points to something".*[98] Mere publication in the media thus cannot create a "preponderant interest of general public". For example, the article can be published in the newspapers or internet portal that nobody reads, does that mean that "preponderant interest of general public" exists? On the other hand, one can argue that this low public interest standard is in accordance with Article 29 Working party[99], where they stated in its „Guidelines on the implementation of the Court of Justice of the European Union judgment on "Google Spain and Inc v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González" C-131/12", that when assessing delisting request DPA[100] shall take into account whether the data is related to criminal offence, the seriousness of offence and time of the event[101]. It is also important to clarify that Article 29 Working Party issued a "guidance" which under EU law are not binding, but purely advisory[102]. The existence of Article 29 Working Group additionally bolsters non-harmonious interpretation, due to advisory non-binding character of its guidance. National courts of MS sometimes chose to follow their guidance and sometimes they do not. The issue of the preponderant standards illustrates different approach in the balancing between rights of personal data and freedom of expression and for that reason we

[97] See supra note 69.
[98] 'Preponderance Of The Evidence' (LII / Legal Information Institute, 2017) <https://www.law.cornell.edu/wex/preponderance_of_the_evidence> accessed 5 May 2017
[99] Dir 95/46/EC OJ L 281/48
[100] Reg 2016/679 OJ L 119/65
[101] Article 29 Working Party - „Guidelines on the implementation of the Court of Justice of the European Union judgment on "Google Spain and inc v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González" C-131/12" 14EN 225 adopted on 26 November 2014, pg 20
[102] Article 1 (1) of Rules of procedure of Working party on the protection of individuals with regard to the processing of personal data – adopted 15th of February 2010

can conclude that national courts of the Netherlands are interpreting and applying Google Spain[103] case differently.

Ewald van Hamersveld v. Google Inc.[104]

KPMG partner engaged in contract to build a house, after the house was finished he was not satisfied how it was done and refused to pay fee for additional works and late payments in amount of 200 000 EUR.[105] The consequence of this refusal was change of locks in the house so KPMG Partner could not enter it. Eventually, he had to sleep in containers installed next to the house.[106] The contractor and KPMP partner brought dispute before Dutch Arbitration Board for Building Industry and eventually settled on a fee in amount 60 000 EUR.[107] The additional issue arose when Dutch newspapers "De Telegraf" published newspapers with front-page stating "KPMG Top Executive Camps in Container".[108] KPMG partner invoked the right to be forgotten and requested Google to de-list "De Telegraf" articles which are displayed upon search of his name.[109] Google refused to de-list stating that *"the webpages contained information that is relevant, of public interest, and not out-dated".*[110] Consequently, KPMG partner initiated a proceeding against Google at District Court of Amsterdam asking the court to order Google to either de-list the web pages or to place these web pages on the bottom of the search results.[111] He was claiming that it was harmful for his career as client usually search for him and they eventually end up reading about „container story".[112] Additionally, KPMG partner was claiming that this information is purely within its private life and for that reason shall not be as of general public interest.[113]

The District Court of Amsterdam rejected the arguments made by KPMG partner. Reasoning of the court was more concentrated on the lawfulness of the search results instead of lawfulness of the content.[114] Additionally, in its reasoning the court is emphasizing the correctness and accuracy of the information provided in the news and states for that reason it

[103] See supra note 27
[104] European Court of Human Rights judgments on the right to freedom of expression - Bulletin LVIII: THE 'RIGHT TO BE FORGOTTEN' - 24 May 2015, pg 1
[105] 1 Eur. Data Prot. L. Rev. 119 2015
[106] ibid
[107] 1 Eur. Data Prot. L. Rev. 120 2015
[108] ibid
[109] Ibid
[110] ibid
[111] ibid
[112] ibid
[113] 1 Eur. Data Prot. L. Rev. 120 2015
[114] 1 Eur. Data Prot. L. Rev. 121 2015

should not be erased.[115] Moreover, the court is basing "relevance" of the information provided in article on the fact that media decided that the news is "newsworthy".[116] The mere fact that media decided to publish news cannot be taken as evidence that the same news are in the interest of public. There would be no request for erasure if the article was not published in the first place. Such low threshold is jeopardizing the very essence of the right to be forgotten, since according to the District Court of Amsterdam, every published article is "newsworthy", and therefore it shall not be erased. Moreover, this is contrary to the Article 29 Working Party Guidance on the application of Google Spain reasoning. Article 29 Working Party recognizes the private life of public figures:

> *„But as a rule of thumb, if applicants are public figures, and the information in question does not constitute genuinely private information, there will be a stronger argument against de-listing search results relating to them"[117] [emphasis added]*

The question that arises is why the Court of Amsterdam did not uphold the right of privacy of a KPMG partner who is not even a public figure while having in mind the obligation provided by the Article 7 of the Charter on Right of private and family life?[118] Even if we assume that the KPMG partner was public figure, the information contained in the published article is from his private life and in accordance with the Guidance[119] Google should have erased it. Also, the courts justification based on the lawfulness of the information is contrary to the Google Spain[120] ruling, since in the paragraph 88, the CJEU explicitly states that *"the operator of a search engine is obliged to remove from the list of results displayed following a search made on the basis of a person's name links to web pages ... and even, as the case may be, when its publication in itself on those pages is lawful."*[121]

When it comes to the Netherlands, we can see from the cases above that the Courts of the Netherlands are applying Google Spain ruling differently. The question that arises next is how can GDPR improve and unify the application? Apparently, all the arguments provided by the Courts of Netherlands can be read in the light of derogation provided by Article 23 of

[115] Ibid
[116] ibid
[117] Article 29 Working Party - „Guidelines on the implementation of the Court of Justice of the European Union judgment on "Google Spain and inc v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González" c-131/12" adopted on 26 November 2014, pg 14
[118] Charter of Fundamental rights of European Union [2000] OJ C 364/19
[119] See supra note 117.
[120] See supra note 27.
[121] Case C-131/12 *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González* [2014], ECLI:EU:C:2014:317, paragraph 88

GDPR, more precisely, Article 23 (1) (i) „the protection of the data subject or the rights and freedoms of others".[122] Protection of freedom of expression and right to receive information can be legitimate derogation under Article 23 (1) (i). The different interpretation of Google Spain ruling in national courts of the Netherlands results from the use of vague and ambiguous terms, such as "preponderant".. This issue should have been tackled by GDPR in order to ensure unified application. The GDPR had to be as precise as possible without leaving any room for interpretation.

After exploring the interpretation of national courts of the Netherlands, thesis will now discuss application of Google Spain ruling at the national courts of France.

France

Marie - France M. v. Google France and Google Inc.[123]

The case concerned an applicant who requested from Google to de-list web pages containing information about applicant's commitment of fraud from 2006.[124] The applicant requested to be delisted from Google search results displayed upon the search on basis of its name.[125] Google rejected the request on the grounds that it was in the interest of the public.[126] After the second link appeared in the Google search results the applicant decided to bring Google to the proceeding before regional court (Tribunal de Grande Instance - TGI).[127]

TGI noted, in its reasoning, the fact that *„the applicant did not bring a case against the editor of the article did not deprive her of the right to request de-referencing directly from the search engine operator."*[128] TGI granted a affirmative judgment for the applicant and ordered Google to remove the web pages containing information about the fraud from the search results based on applicant's name on the grounds that the article were published more than 8 years ago.[129] This case shows that the national courts of France are willing to suppress the freedom of expression on the grounds of the relevance and time of publication. As indicated

[122] Reg 2016/679 OJ L 119/47
[123] European Court of Human Rights judgments on the right to freedom of expression - Bulletin LVIII: THE 'RIGHT TO BE FORGOTTEN' - 24 May 2015
[124] 'France : The Right To Be Forgotten: First Decision Delivered In Application Of CJEU Jurisprudence' (Merlin.obs.coe.int, 2017) <http://merlin.obs.coe.int/iris/2015/4/article8.en.html> accessed 18 May 2017
[125] ibid
[126] Ibid
[127] Ibid
[128] Ibid
[129] ibid

in the Article 29 Working Party Guidance[130], the time of publication plays significant role when balancing between protection of personal data and freedom of expression.

Franck J. v. Google France and Google Inc [131]

The case concerned applicant's request to delist news reports from Google search results, based on the name of applicant, which contain information about legal proceedings for harassment at work.[132] The case was brought under urgent procedure before Toulouse Regional Court.[133] The judgment in legal proceedings for harassment was delivered at court of first instance and it was accessible to public and also the facts about the case were from 2011, which the court found to be still recent.[134] The Toulouse Regional Court also noted the fact that even though the appeal was still pending it does not necessarily mean that court of first instance made a mistake and for that reason Toulouse Regional Court decided that *„right of the public to be informed about a current legal case outweighed an individual's 'right to be forgotten' and rejected the request for removal".*[135]

In this section we can see that national courts of France are interpreting the Google Spain ruling differently than the Netherlands national courts. National courts of France are following a Guidance published by Article 29 Working Party[136]. On the other hand, the Netherlands national courts are, in author's opinion, ruling contrary to the Article 29 Working Party Guidelines on application of Google Spain ruling[137] as in the case of *Ewald van Hamersveld v. Google Inc* they are ignoring the fact that the individual concerned was acting within its private life. This is not only disregarding the Guidance[138], but the Charter too. As a reminder, GDPR is supposed to create a harmonious legal framework within EU, so we shall now examine what provisions within GDPR are going to address specific issue of application of Right to be forgotten? More precisely, we need to examine whether there are

[130] Article 29 Working Party - „Guidelines on the implementation of the Court of Justice of the European Union judgment on "Google Spain and inc v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González" c-131/12" adopted on 26 November 2014, pg 18
[131] European Court of Human Rights judgments on the right to freedom of expression - Bulletin LVIII: THE 'RIGHT TO BE FORGOTTEN' - 24 May 2015, pg 1
[132] European Court of Human Rights judgments on the right to freedom of expression - Bulletin LVIII: THE 'RIGHT TO BE FORGOTTEN' - 24 May 2015, pg 3
[133] ibid
[134] ibid
[135] ibid
[136] Article 29 Working Party - „Guidelines on the implementation of the Court of Justice of the European Union judgment on "Google Spain and inc v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González" c-131/12" adopted on 26 November 2014
[137] ibid
[138] ibid

any provisions which deal with rules applicable when it comes to the striking a balance between rights in question. In the Article 23 of GDPR which is regulating restrictions of Data Subject rights provided by Articles 12 to Articles 22, Union or Member State law which is limiting the data subject right "*needs to respect the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguard."*[139] Respect of fundamental rights is already well established by the Charter and a restriction of fundamental rights is already limited by Article 52 of the Charter to the proportionality principle[140]. In the author's opinion the national courts of MS should have reached different judgement, especially in the case of KPMG partner as Respect of private and family life is recognized by the Article 7 of the Charter.[141]

Conclusion of section two

From the analysis Section two of the thesis, we can see that the existence of vague and ambiguous terms such as those explained and explored in section one of the thesis are going to create a non-harmonious application of the GDPR. We have seen through the examples of the application of Google Spain[142] ruling that courts show tendency to interpret vague and ambiguous terms and differently. The example of national courts interpreting Google Spain[143] ruling are proving the listed issues with GDPR. On the one hand, we can see that national courts of some Member states are applying Google Spain[144] ruling in accordance with the Guidance[145] and some MS are not, which is perfect example of existence of non-harmonious interpretation. Unfortunately, GDPR did not create any specific obligations to tackle this issue.

[139] Reg 2016/679 OJ L 119/46
[140] Charter on protection of fundamental rights in European Union [2000] OJ C 364/21
[141] Ibid OJ C 364/10
[142] See supra note 27.
[143] ibid
[144] ibid
[145] Article 29 Working Party - „Guidelines on the implementation of the Court of Justice of the European Union judgment on "Google Spain and inc v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González" C-131/12" adopted on 26 November 2014

Conclusion

This paper has explored the issues that GDPR may encounter while trying to achieve what it aims. As indicated already in the beginning of the paper, the aim of new GDPR is to create a harmonious legal framework which is going to be cost efficient. The content of GDPR is providing for long list of derogations where the competence to regulate area of data protection is shifted to the member states and thus GDPR creates legal diversity. Legal diversity is going to put additional financial on individuals and undertakings acting in the field of data protection.

Derogations are also placed on the rights of data subjects which eventually lead to the creation of non-harmonious legal framework. Moreover, the rights of data subjects are subject to the interpretation of supervisory authorities and national courts of respective MS and the paper has shown the willingness of national courts to interpret and apply the reasoning of the CJEU differently. There are no indications within GDPR itself of principles that are going to be used in terms of striking balance between rights. This void is basis for different approaches and different application of data subject rights, especially right to be forgotten.

The lack of provisions regulating users of social networks acting outside of household activity and uncertainty whether they can be understood as a data controllers under GDPR is creating additional void for interpretation. There is a possibility that Article 29 Working Party is going to adopt guidelines which will define more precisely approach of GDPR to this very specific issue, but we still have an issue of non-binding effect of such guidelines. In any case, it is reasonable to assume that this issue will be shifted to social network service providers, but this will create additional financial burden, which proves that new GDPR is not going to create cost efficiency within the social networks market.

Primary sources:

- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC
- 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 [1995] OJ 2 281/01

Published articles and textbooks

- Bernard C, The Substantive Law Of The EU (5th edn, Oxford University press 2016)
- Brendan Van Alsenoy and others, 'Social Networks And Web 2.0: Are Users Also Bound By Data Protection Regulations?' (2009) 2 Identity in the Information Society.
- William Long and Francesca Blythe, 'Member States' Derogations Undermine The GDPR' (Privacy laws& business United Kingdom report 2016)
- Article 29 Working Party - „Guidelines on the implementation of the Court of Justice of the European Union judgment on "Google Spain and inc v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González" C-131/12" adopted on 26 November 2014

Online sources:

- 'Priorities' (European Commission - European Commission, 2017) <https://ec.europa.eu/commission/priorities_en> accessed 23 May 2017
- 'Better Access For Consumers And Business To Online Goods' (Digital Single Market, 2017) <https://ec.europa.eu/digital-single-market/node/78515> accessed 23 May 2017
- 'Digital Single Market' (Digital Single Market, 2017) <https://ec.europa.eu/digital-single-market/en/digital-single-market> accessed 23 May 2017
- 'Right Environment For Digital Networks And Services' (Digital Single Market, 2017) <https://ec.europa.eu/digital-single-market/node/78516> accessed 23 May 2017
- 'Economy & Society' (Digital Single Market, 2017) <https://ec.europa.eu/digital-single-market/node/78517> accessed 23 May 2017
- 'Web 2.0 - Definition Of Web 2.0 In English | Oxford Dictionaries' (Oxford Dictionaries | English, 2017) <https://en.oxforddictionaries.com/definition/Web_2.0> accessed 23 May 2017
- 'Reform Of EU Data Protection Rules - European Commission' (Ec.europa.eu, 2017) <http://ec.europa.eu/justice/data-protection/reform/index_en.htm> accessed 12 May 2017
- 'Reform Of EU Data Protection Rules - European Commission' (Ec.europa.eu, 2017) <http://ec.europa.eu/justice/data-protection/reform/index_en.htm> accessed 12 May 2017

- 'Derogation - Definition Of Derogation In English | Oxford Dictionaries' (Oxford Dictionaries | English, 2017) <https://en.oxforddictionaries.com/definition/derogation> accessed 23 May 2017
- 'Glossary - European Commission' (Ec.europa.eu, 2017) <http://ec.europa.eu/smart-regulation/guidelines/ug_chap8_en.htm> accessed 23 May 2017
- 'What Is Public Information? | Facebook Help Centre | Facebook' (Facebook.com, 2017) <https://www.facebook.com/help/203805466323736> accessed 16 May 2017
- 'How Does Facebook Suggest Tags? | Facebook Help Centre | Facebook' (Facebook.com, 2017) <https://www.facebook.com/help/122175507864081?helpref=faq_content> accessed 11 May 2017.
- 'France : The Right To Be Forgotten: First Decision Delivered In Application Of CJEU Jurisprudence' (Merlin.obs.coe.int, 2017) <http://merlin.obs.coe.int/iris/2015/4/article8.en.html> accessed 18 May 2017

Table of cases:

- Case C-131/12 *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González* [2014], ECLI:EU:C:2014:317
- Franck J. v. Google France and Google Inc., TGI de Toulouse (urgent procedure), 21 January 2015
- Marie-France M. v. Google France and Google Inc., TGI de Paris (urgent procedure), 24 November and 19 December 2014
- Ewald van Hamersveld v. Google Inc., Amsterdam Court, 13 February 2015
- Arthur van M. v. Google Netherlands and Google Inc., Amsterdam Court of Appeals, 31 March 2015
- Case C-2/88 J. J. Zwartveld and Others [1990] I-3372
- Case C-101/1 *Lindquist* [2003] ECLI:EU:C:2003:596
- Case C-6/64, *Falminio Costa v. ENEL* [1964]

The thesis is dedicated to my family and friends without whom author would not be able to complete it. For that reason author finds convenient to mention them by their names Fehrija, Fadil, Jasmin, Evin, Nico, Maria, Kelly, Armina and Nina. Additionally, the thesis is dedicated to all employees of the company NSoft d.o.o. Mostar, but especially to those who made this journey possible, Igor, Stjepko and Marina.