RIGA GRADUATE SCHOOL OF LAW

Problems of user's consent to the privacy policy

MASTER'S THESIS

AUTHOR: Ellina Logacheva (Sedleniece)
LL.M 2019/2020 year student
student number M019022

SUPERVISOR: *Dr M.R. Leiser*

(Visiting Professor)

DECLARATION OF HONOUR:
I declare that this thesis is my own work, and that all references to, or quotations from, the work of others are fully and correctly cited.

(Signed) …….

RIGA, 2020

ABSTRACT

The purpose of the thesis is to identify the problems of the acceptance of the privacy policies by users of the online services. The author proposes that there are two types of consent to the privacy policy which are given by the same act of acceptance of the provisions of the privacy policy. The first type of consent is consent to the processing of personal data. This consent shall be in compliance with provisions of the GDPR. The second consent is consent to the rest of the provisions of the privacy policy. This consent may create a binding agreement for the user. In order to prove this assumption, the provisions of the privacy policies of Google, Microsoft, Likedin, Facebook and Apple were analysed. The analysis has shown that the provisions of the privacy policies might be considered as violating the provisions of the GDPR. Also, provisions of the privacy policies are structured in a way to be able to create binding obligations for the user, or at least to create an illusion of the existence of such obligations.

SUMMARY

The purpose of the thesis "Problems of user's consent to the privacy policy" is to identify whether the acceptance of the provisions of the privacy policy as a whole document by the user form a valid consent thereof. The acceptance of the provisions of the privacy policy seems to be twofold. It might constitute the consent to processing of the personal data in accordance with the provisions of the General Data Protection Regulation and at the same time it provides for the consent of the user to the provisions of the privacy policy which might be of a contractual nature. The thesis aims to determine the problems of user's consent to the privacy policy through the analysis of the provisions of five the privacy policies, in particular Google, Microsoft, Likedin, Facebook and Apple.

The introduction of the thesis provides for the aim of the research. It briefly establishes the topicality of the research and the directions of the existing academic discussions of the problems of self-regulation of the online service providers by means of the privacy policies. It also defines the limitations of the research.

In the first chapter of the thesis the privacy policies are discussed from the point of view that the privacy policies represent a tool for self-regulation of the online service providers. The first subchapter of this chapter describes the preconditions for the privacy policies to become one of the main legal documents of non-legislative nature, which regulates data protection matters between the online service provider and the data subject. The second subchapter describes the privacy policies in the current practice. The third subchapter provides for the analysis of the existing problems of self-regulation by the privacy policies. The problem of reading and accessibility of the privacy policies, the problem of attitude, the problem of unification of consent and the problem of unclear nature of the privacy policies are examined in the subchapter.

The second chapter provides for a detailed analysis of the provisions of the privacy policies of Google, Microsoft, Likedin, Facebook and Apple. The analysis is based on the following questions:

- Is the privacy policy accessible?
- Does the privacy policy clearly state what personal data is being processed by the service provider?
- Does the privacy policy clearly state the purposes for processing of personal data?
- Does the privacy policy provide information of the period of storage of personal data?
- What is the procedure for the amendment of the privacy policy?

In order to answer these questions the provisions of the privacy policies are compared with the provisions of the General Data Protection Regulation, the European Data Protection Board Guidelines 05/2020 on Consent, Article 29 Data Protection Working Party Opinions and Guidelines, the case law and academic literature.

The third chapter represents the consolidated results of the analysis and describes the common flaws of the privacy policies which are identified by the analysis. This chapter provides for the consolidated answer on the questions, posed in the third chapter and also compares the results with the provisions of the General Data Protection Regulation, the European Data Protection Board Guidelines 05/2020 on Consent, Article 29 Data Protection Working Party Opinions and Guidelines, the case law and academic literature.

The final part of the thesis formulates the conclusions and gives recommendations for a possible future research.

TABLE OF CONTENTS

INTRODUCTION

The online environment is developing at a high pace every day. Currently, the online services have occupied many markets which before were presented mostly in offline environment. This tendency has become universal and is especially relevant during the lockdowns all over the world, which have been caused by the spreading of the SARS-CoV-2 virus. A lot of businesses, which were not presented online or had poorly developed online services, have focused their attention on the Internet as a marketplace for their products. Consumers also have refocused to the Internet. Therefore, the adequate level of protection of personal data in digital space has become more topical than ever.

Any interaction between the consumers and the online service providers are accompanied by the processing of personal data. Any actions of the consumers towards obtaining the online services, for example, the process of negotiations, the conclusion of the agreement in any form, any correspondence with the service provider, lead to the necessity to provide personal data. However, the processing of the personal data is regulated by the legislation, in particular by the General Data Protection Regulation, and there are legislative conditions for the processing to be lawful.[1] One of the conditions for the processing of the personal data to be lawful is the consent of the data subject.

In practice the online service providers tend to structure their processes of cooperation with the consumer in such a way to be able to obtain the consent of the consumer to the processing of personal data through the acceptance of the privacy policies. These practices are beneficial to the online service providers for several reasons. It requires less transactional costs, it is convenient and it is in line with the applicable legislation. However, the development of this practice has created the possibility for the online service providers to abuse their rights. The privacy policies have started to perform functions which they initially were not intended to perform. Instead of providing clear information on how the personal data is being processed, the privacy policies merely serve as a shield for the service providers from possible accusations in violation of the legislation on protection of the personal data.

Everyone who uses the Internet has accepted a privacy policy at least once in their lifetime. Therefore, it is justified to state that the privacy policies have occupied a dominant position among legal documents which regulate the relationship between the service provider and the data subject on the processing of data. Nevertheless, the privacy policies are not regulated by the legislation directly.

All the privacy policies ask the consumers to provide a consent to their provisions. The author proposes that there are two types of consent to the privacy policy. The first consent is the consent to the processing of personal data, which shall be given in accordance with the provisions of the General Data Protection Regulation. And the second consent is the consent to the rest of the provisions of the privacy

[1] Regulation (EU) No 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). Article 6. Available on https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679 accessed April 16, 2020

policy, which often includes conditions that are not relevant to the protection of the personal data. In order to prove the stated assumption, the research proposes the question:

Does the acceptance of the provisions of the privacy policy form a valid consent thereof?

To answer the research question, it is necessary to obtain a clear understanding on the current functions of the privacy policies and to provide an analysis of the provisions of the privacy policies. Therefore, the first part of the research is focused on the preconditions for the rise of the privacy policies. Then, the problems of the system of self-regulation of the service providers by the means of the privacy policies, *inter alia*, the problem of the accessibility, the problem of the attitude of the customer towards the privacy policy and the problem of the uncertain legal nature of the privacy policies are discussed. This part of the research is not limited by the territorial scope and serves as a foundation for the further deeper study of provisions of the privacy policies.

The second and the main part of the research is dedicated to a detailed analysis of provisions of the privacy policies of the dominant online companies with data power[2], which are Google, Apple, Microsoft, Facebook and Linkedin. The author defines such policies as influential privacy policies. These privacy policies are analyzed from the perspective that on the one hand the provisions of the privacy policies are drafted with the aim to establish the consent of the consumer to the processing of the personal data and consequently, this consent shall be freely given, specific, informed and unambiguous.[3] On the other hand, provisions of the privacy policies, *inter alia*, regulate a relationship the object of which is not connected to the processing of personal data. Thus, the consent of the consumer to those provisions of the privacy policies is not needed according to the legislation. Nevertheless, the consumer is asked to give the consent to all the provisions of the privacy policy by accepting the whole document. Therefore, the second type of consent may impose the contractual nature to the privacy policy.

The final part of the present research will aim to identify the common tendencies in drafting of influential privacy policies. These tendencies will be discussed from the perspective of the consent of the consumer to the privacy policy and the compliance with the current legislation.

The analysis of the content of the influential privacy policies is limited by the territorial scope, in particular by the territory of the European Union. The analysis is based on the provisions of the General Data Protection Regulation, the European Data Protection Board Guidelines 05/2020 on Consent, Article 29 Data Protection Working Party Opinions and Guidelines, the case law and academic literature.

---

[2] Orla Lynskey, "Grappling with "Data Power": Normative Nudges from Data Protection and Privacy", Theoretical inquiries in Law 20 (2019):p.201

[3] *Supra* note 1, Article 4 (11).

THE PRIVACY POLICIES AS AN INSTRUMENT OF SELF-REGULATION FOR THE ONLINE SERVICE PROVIDERS

1.1 The preconditions for the rise of the privacy policies

There are numerous ways to define privacy. Nonetheless, still every person understands this concept in an individual way. According to the Cambridge dictionary privacy is "someone's right to keep their personal matters and relationships secret".[4] However, in the era of the Internet, a concept of privacy has been significantly broadened and, in some cases, even lost its limits. "Before search engines, no one had any records of curiosity".[5] Currently, the records of online activities of the users are being considered as a profitable asset for the providers of online services. Often these records are estimated even higher than the revenue from the actual services that such providers perform.

"You have zero privacy anyway. Get over it".[6] This is the famous statement of the chairman of Sun Microsystems that illustrates the mainstream attitude of the online companies towards personal data of the users and their privacy. It is obvious, that to maintain normal relationships with each other the individuals need to share their personal information to others. The communications in the online environment have facilitated and eased the process of voluntary disclosure of the personal information by the users. For example, almost three-quarters of interviewed citizens of the European Union have said that in the modern society it is impossible not to disclose a greater amount of personal information than it was considered as normal to disclose before.[7] However, at the same time, to operate the relationships in an efficient way the personal information must be secured.[8] Regardless of the fact, that in recent years in various jurisdictions a stricter legislation on the protection of personal data of users has been adopted, the process of the commoditisation of personal data and privacy seems to be inevitable. It is justified to state that to some extent the existence of this process has been accepted by the society and has been indirectly supported by the legislator.[9]

For example, the online relationships in the European Union between the users and the service providers are based on the principle that "the right to the protection of personal data is not an absolute right".[10] Therefore, this leads to the conclusion that

---

[4] Cambridge Dictionary. Available on: https://dictionary.cambridge.org/dictionary/english/privacy accessed May 26, 2020

[5] Lawrence Lessig, *Code Ver 2.0.* (New York: Basic books, 2006) p. 204

[6] Scott McNealy. Available on: https://en.wikiquote.org/wiki/Scott_McNealy accessed May 26, 2020

[7] EU Open Data Portal. Special Eurobarometer 359: Attitudes on Data Protection and Electronic Identity in the European Union. p.23 Available on: https://data.europa.eu/euodp/en/data/dataset/S864_74_3_EBS359 accessed June 01, 2020

[8] Jeffrey T. Child, Shawn C. Starcher, "Fuzzy Facebook privacy boundaries: Exploring mediated lurking, vague-booking, and Facebook privacy management", *Computer in Human Behaviour* 54 (2016): p.484

[9] Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services. Available on: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32019L0770 Accessed 05.06.2020.

[10] *Supra* note 1, Recital 4.

the aim of the legislation shall be to maintain the balance between the right of a legal entity to gain profit and the right of a private person to protect its personal data.[11]

Obviously, the system of regulation of the online space differs from the system of regulation of the offline space. There are several reasons for that.

The first reason is that the online space expands on a high speed. Almost every day new kinds of online services are being developed. For example, in the recent past, it was hard to imagine that in year 2020 not just private companies but also a number of governments, including countries of the European Union, would offer to the users to install tracking mobile applications. The main function of such applications is to track people who are diagnosed with SARS-CoV-2 virus (COVID-19) and notify the user whether he or she have come into a contact with an infected person.[12]

The second reason seems to be that the Internet has a great variety of online actors. Apart from conventional state actors, the researchers distinguish several groups of non-state actors, such as "(1) business actors; (2) transnational multistate actors; (3) transnational private actors; and (4) civil society groups".[13] Even though for those actors it is impossible to create the legislation, they may have a strong impact on the policy makers.[14]

The factors stated above have created the conditions that have precluded the legislative bodies in different countries from adopting comprehensive, up to date and tailored legislation focused on the online services.[15] As a result, there is a pull of separate enactments that regulate the digital technologies from different perspectives.[16] However, the market, at least from the side of the consumer, has formed a demand for an addressed regulation and/or industry standards. In particular such regulation that would concentrate solely on the aspects of the online relationships between the user and a service provider in respect of personal data and privacy. The distinctive characteristic of these relationships is that their core subject matter is the process of exchanging personal data and privacy for free or almost free online services. The privacy policies have become the answer to the demand of the market. They have replaced the legislative regulation and have become the main source of self-regulation in the field.

---

[11] *Supra* note 1, Recital 4.

[12] MIT Technology review. Available on: https://www.technologyreview.com/2020/05/07/1000961/launching-mittr-covid-tracing-tracker/ accessed May 25, 2020

[13] Mark R. Leiser, Andrew D. Murray, "The role of non-state actors and institutions in the governance of new and emerging digital technologies", *The Oxford Handbook of Law, Regulation and Technology* (2016): p. 671.

[14] ibid.

[15] Amanda Grannis, "You didn't even notice: elements of effective online the privacy policies [notes]", *Fordham Urban Law Journal* 42 (2015): p. 1113

[16] European commission. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - Online Platforms and the Digital Single Market Opportunities and Challenges for Europe (COM(2016)288) p. 3 Available on: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52016DC0288 accessed 01.06.2020

The request from the consumers for the regulation of the privacy matters in the online environments has been formed already for a long time.

For example, in the United States of America in year 2000 the Federal Trade Commission in its report to the Congress has stated that seventy six percent of the consumers have concerns about how their personal data will be used in the Internet. The consequence of such concerns was that consumers have been reluctant to actively participate in the online commerce.[17] However, this issue is still relevant. According to the poll recently made by Amnesty international, the majority of participants in the poll, the consumers who use online services, have concerns about the way their personal data is being collected, processed, used and transferred by the online service providers. Also, it has been revealed that the consumers would like the government to adopt a stricter regulation for the protection of privacy and personal data in the field of online commerce.[18]

In Europe, harmonized legislation on the protection of personal data has started to evolve since 1950 on the level of the Council of Europe, when the European Convention on Human Rights (ECHR) was adopted. Provisions of Article 8 of the ECHR proclaim the right of the person to respect for the private and family life, home and correspondence.[19] The right of the protection of personal data represents part of the rights which are established by Article 8 of ECHR.[20] Another instrument on the level of the Council of Europe which protects rights of natural persons in relation to processing of personal data is the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data.[21] On the level of the European Union the right to data protection has been declared by Article 16 of the Treaty of the Functioning of the European Union[22] and has been recognized as a fundamental right by Article 8 of the Charter of Fundamental Rights of the European Union.[23] The regulation of data protection in the European Union has started with the Data

[17] Federal Trade Commission Privacy Online: Fair Information Practices in the Electronic Marketplace: A Federal Trade Commission Report to Congress. p.2. Available on https://www.ftc.gov/reports/privacy-online-fair-information-practices-electronic-marketplace-federal-trade-commission accessed 25.05.2020

[18] Amnesty international. Available on: https://www.amnesty.org/en/latest/news/2019/12/big-tech-privacy-poll-shows-people-worried/ Accessed May 19, 2020

[19] The Convention for the Protection of human Rights and Fundamental Freedoms (Rome, 4 Nov. 1950) article 8. Available on https://www.echr.coe.int/Documents/Convention_ENG.pdf Accessed June 8, 2020

[20] ECHR: Malone v. The United Kingdom, judgment of 02 August 1984, Series A no. 8691/79 Available on: https://hudoc.echr.coe.int/eng#{%22fulltext%22:[%228691/79%22],%22documentcollectionid2%22:[%22GRANDCHAMBER%22,%22CHAMBER%22],%22itemid%22:[%22001-57533%22]} Accessed June 8, 2020

[21] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Council of Europe, CETS No.108, 1981.

[22] Treaty on the Functioning of the European Union (Consolidated version 2012), OJ C 326, 26.10.2012. Available on: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012E/TXT Accessed June 8, 2020

[23] Charter of Fundamental Rights of the European Union [2012] OJ C326/391.

Protection Directive, which was implemented in 1995.[24] Finally, in 2016 the General Data Protection Regulation (GDPR) was adopted[25] and the legislation which governs the processing of personal data for the purposes of law enforcement.[26] However, despite the fact that the legislation of the European Union provides for the protection of personal data, only fourteen percent of the respondents have indicated that they believe that they are in control over the personal data which they have provided online. Thirty percent of the respondents have stated that they do not have any control over the personal data provided online.[27]

Therefore, at first, the privacy policies were implemented by the online service providers as an answer to the consumer request indicated above. In 1999 it was observed that consumer trust increases significantly for those websites which have adopted and posted a privacy policy.[28] Around the same time the big influential companies such as IBM, Microsoft, Disney's Go Network have stated that they are going to stop using for advertising purposes websites, which have not adopted a privacy policy.[29] Thus, the majority of the online companies voluntarily adopted the privacy policies. In 1998 the practice to have a privacy policy was implemented only by two percent of the online companies. Nevertheless, already in 2000 almost all websites have published their privacy policies.[30]

However, the stimulation of the consumers who have been concerned about their privacy to proceed to participate in the online commerce was not the only reason to implement the privacy policies. There was also a different reason for the companies to embrace the new practice. The online companies have had the aim to prevent possible excessive regulation from the side of the government. This aim has motivated the online companies to simultaneously start to regulate issues of processing of personal data of the user by terms of the privacy policies.[31]

> A political consensus on appropriate use of consumer information has arrived, and effective self-regulation (at the level of the individual company and of the

---

[24] 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. Available on: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A31995L0046 accessed May 27, 2020

[25] *supra* note 1.

[26] Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA. Available on: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016L0680 accessed June 08, 2020

[27] EU Open Data Portal. Special Eurobarometer 487a: The General Data Protection Regulation. p.34 Available on: https://ec.europa.eu/info/law/law-topic/data-protection/eu-data-protection-rules_en Accessed June 06, 2020

[28] Scott Killingsworth, "Minding your own business: The privacy policies in principle and in practice" *Journal of Intellectual Property Law* 1 (1999): p. 63.

[29] Killingsworth, *supra* note 28, p. 67

[30] *Supra* note 15, p. 1114

[31] Daniel Solove, Woodrow Hartzog "The FTC and the new common law of privacy", *Colombia law review* 114:583 (2014): p. 594

> Internet community as a whole) is probably the only way to head off federal privacy legislation, with its threat of inflexibility and bureaucratization. These companies know that the alternative to adopting the privacy policy is to have the government adopt one for them. The choice is not whether to volunteer for liability or to avoid it; the choice is whether to define one's own standard or to accept whatever standard the political process may define.[32]

Consequentially, the approach has been developed to regulate the collection, processing, usage and the transferring of personal data by the privacy policies which are voluntarily drafted and adopted by the online service providers. This approach has become harmonized and a common best practice for the online industry. The privacy policies have turned into an effective self-regulatory tool for the business.[33]

The governments also have accepted and even promoted the regime of self-regulation.[34] For example, the European Commission stated in year 2016 that "it will further encourage coordinated EU-wide self-regulatory efforts by online platforms".[35]

There is a reason for such high level of trust from the side of the legislator. The speed and the scale of the development of the digital technologies persuades the legislator to believe in the effectiveness of the self-regulatory practice of the online actors. It is hard to underestimate the role of the Internet in the modern economy. The European Commission has indicated that:

> We witness a new industrial revolution driven by digital data, computation and automation. Human activities, industrial processes and research all lead to data collection and processing on an unprecedented scale, spurring new products and services as well as new business processes and scientific methodologies.[36]

The excessive strict legislative regulation for the business activities of the online companies might slow down the speed of the development of a digital economy which is an important factor for the innovation.

However, with time the problem has emerged that "the privacy policy content appears to be shaped at least as much by market forces as by a self-regulatory regime based on external guidelines".[37] The private sector has started to abuse its carte

---

[32] Killingsworth, *supra* note 28, p. 68

[33] C. Jensen, C. Potts "The privacy policies as Decision-Making Tools: An Evaluation of Online Privacy Notices." CHI '04: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, April 2004, p. 471

[34] *Supra* note 15, p. 1111

[35] European commission. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - Online Platforms and the Digital Single Market Opportunities and Challenges for Europe (COM(2016)288) p. 9 Available on: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52016DC0288 accessed 01.06.2020

[36] European commission. Communication on data-driven economy. p.2 Available on: https://ec.europa.eu/digital-single-market/en/news/communication-data-driven-economy accessed 01.06.2020

[37] Florencia Marotta-Wurgler,"Self-regulation and competition in The privacy policies", *Journal of Legal studies* 45 (2016): pp. S13-S-40

blanche and has begun to use the self-regulatory regime mostly in its own favor. The reason for that is that a data driven economy implies that a huge amount of data, including personal data, must be processed. Naturally, the business does not want to restrict itself on how to process such data by the means of the privacy policies. Another reason is that it might be difficult to implement the limits of the data processing in the situation when the consumers do not mind giving it up their personal data.[38] On the other hand, the presumption of the self-regulatory effectiveness can be considered as true only when the fundamental rights of the users and, in particular, the right to the protection of personal data[39], are not depressed.[40]

1.2 The privacy policies in practice

The relationship between the online service provider and the user are usually regulated by several legal documents. These documents might have different titles but, commonly they are the terms of service, a user agreement, and the privacy policy. All these documents are connected to each other. The terms of service and the user agreement indicate the services that will be provided to the user. Also, they usually provide for a dispute resolution, establish rights and obligations and liability of the user and the service provider. The terms of service and the user agreement are contracts by nature and, although subject to discussions among scholars[41], they are generally binding for the parties. These contracts are concluded in the form of the standard terms, which means that the consumer accepts the whole contract. The conditions in the terms of service and the user agreement are identical for all the consumers and could not be negotiated from the side of the consumer. On the other hand, the legislator provides for the protection of the consumer by the means of special regulation for the standard terms.[42] It is common, that the terms of service and the user agreement have a reference to the privacy policy in their text as they do not directly regulate the issues of the processing of personal data.[43]

As it was discussed in the previous chapter but worth to mention, the privacy policies have been developed independently from the terms of service and the user agreement, as a response to certain conditions in the online commerce. The main aims

---

[38] Bernhard Debatin, Jennette P. Lovejoy, "Facebook and Online Privacy: Attitudes, Behaviors, and Unintended Consequences", *Journal of Computer-Mediated Communication 15 (2009):p.87.*

[39] Charter of Fundamental Rights of the European Union [2012] OJ C326/391, Article 8.

[40] European commission. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - Online Platforms and the Digital Single Market Opportunities and Challenges for Europe (COM(2016)288) p. 9 Available on: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52016DC0288 accessed 01.06.2020

[41] Marco Loos "Standard terms for the use of the Apple App Store and the Google Play Store" *Journal of European Consumer and Market Law* (2016), Volume 5, Issue 1 p.13

[42] Directive (EU) 2019/2161 of the European Parliament and of the Council of 27 November 2019 amending Council Directive 93/13/EEC and Directives 98/6/EC, 2005/29/EC and 2011/83/EU of the European Parliament and of the Council as regards the better enforcement and modernisation of Union consumer protection rules Available on:https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32019L2161Accessed 01.06.2020

[43] Facebook. Terms of service. Available on: https://www.facebook.com/legal/terms Accessed 01.06.2020

of the privacy policy are to concentrate on the issues of processing of personal data of the user and to provide the user with the information about the company's practices in respect to these issues. Thus, commonly, the privacy policy is a standalone document which is focused only on the privacy practices of the company.[44]

There are many ways of placing the privacy policy on the website, but typically it is located under a hyperlink at the bottom of a homepage of a website.[45] Generally, the privacy policies describe how the personal data of the user is being collected and according to what procedure it is being used, stored and transferred.

At first, when the privacy policies have begun to develop as a self-regulation instrument, the concept of the passive consent of the user to privacy practices of the online service provider have prevailed. Users could have provided the results of their choice on whether to consent on the processing of personal data most often in a form of an opt-out option[46]. This option suggests that there is a presumption that the user has accepted the privacy policy by default. In order to decline the processing of personal data the user had to additionally indicate that the consent has not been given. Most commonly the user had to do it by unticking a box. This practice has currently stopped as a result of the evolution of the legislation on data protection. According to section 11 of Article 4 of the GDPR, which regulates the processing of personal data in the European Union, only the opt-in option is permitted as a form of consent for data processing. The user must provide freely given, specific, informed and unambiguous consent to the processing of his or her personal data by a statement or by a clear affirmative action.[47]

One of the purposes of the GDPR is to protect "fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data".[48] In order to fulfil this purpose, the GDPR defines the circumstances under which the processing of personal data is lawful in Article 6. Also, it defines what information shall be provided to the user by the service provider in respect with the processing of personal data.[49] The consent of the user is one of the grounds for lawful processing of personal data.[50]

The GDPR, as well as other legislation of the European Union, does not define what a privacy policy is. Also, it does not directly establish the regime according to which the processing of personal data is regulated by the privacy policies. According to a literal interpretation of the provisions of the GDPR it is not mandatory for the online companies to have a privacy policy.

However, the Article 29 Working Party has recommended that every online company shall have a privacy policy published. Also, Article 29 Working Party has

---

[44] Solove, Hartzog, *supra* note 31, p. 595

[45] Solove, Hartzog, *supra* note 31, p. 592

[46] Eleni Kosta, "Construing the Meaning of "Opt-Out" - An Analysis of the European, U.K. and German Data Protection Legislation", *European Data protection Law Review* 1 (2015):pp. 16-31

[47] *supra* note 1, Article 4 (11), Recital 32. 0

[48] *supra* note 1, Article 1 (2).

[49] *supra* note 1, Article 13.

[50] *supra* note 1, Article 6(1)(a).

suggested that every collection of personal data by the service provider shall be accompanied with a link to the privacy policy.[51] As a result of the implementation of the mentioned provisions of the GDPR the online service providers have started to use the privacy policies as a tool that helps to comply with the requirements of the legislation. Therefore, currently the privacy policies are commonly used for obtaining and documenting the consent of the user to the processing of its personal data. Also, the privacy policies are used as an instrument to provide to the user all the information required by the legislation, for example by Articles 13 and 14 of the GDPR. For online service providers the privacy policy has become a very convenient legal instrument because it facilitates the compliance with the legislation and at the same time makes such compliance faster, easier, and free from extra expenses. The reason for that is the absence of statutory need for the service provider to obtain the consent based on separate document from each user. To fulfil the legal requirements, it is enough for the online service provider to draft and to adopt the privacy policy with a certain type of provisions. These provisions usually establish that the consent for the processing of the personal information of the user is deemed to be explicit when the user accepts the policy. As a result, despite the primarily purpose to perform the informational function for the user, the privacy policies have become the document with a user as a party thereof. Currently, all the privacy policies of the online companies ask the user to accept their provisions.

1.3 Problems of self-regulation by the privacy policies

The described model of regulation of privacy and personal data processing has been extensively criticised by the scholars.[52] The analysis of the model shows that it requires active self-management from the consumer and devotion to the principles of self-regulation from the service provider for the model to work effectively. Thus, there are several reasons for criticism.

1.3.1 The problem of reading and accessibility of the privacy policies

The first problem is easy to identify. It is known that users generally do not read and even tend to ignore the privacy policies. There is no significant evidence that users do read the privacy policies, although the companies commonly advise to read the privacy policy.[53] Usually, the user shall scroll down to the bottom of the text of the privacy policy to accept its provisions. However, there are no mechanisms in place for the service provider to check whether the user has read the policy.

Typically, the privacy policies are considerably long documents and consist of at least several pages. Therefore, it is reasonable to state that it might take a significant amount of time for the users to read the privacy policies. For example, according to the results of one research it would take two hundred and one hours per

---

[51] Article 29 Working Party Guidelines on Transparency under Regulation 2016/679 as of 29 November 2017. p. 8 Available on: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051 accessed June 06, 2020

[52] C. Jensen, C. Potts "The privacy policies as Decision-Making Tools: An Evaluation of Online Privacy Notices." CH.I '04: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, April 2004, p. 471-478.

[53] Google privacy policy. Available on: https://policies.google.com/terms?fg=1 Accessed 27.05.2020

year for an average consumer in the United States of America to read the online privacy policies for the websites that he or she occasionally visits. If the user decides to spend this amount of time for reading the privacy policies, it will cost him or her $3,534 per year.[54] The same research has concluded that if all the consumers of online services in the United States of America read the privacy policies it will cost approximately $781 billion per year for the economy.[55] Moreover, a lot of the online service providers change the provisions of their privacy policies from time to time. Thus, the user is compelled to read the privacy policy of one legal entity for several times. Furthermore, the scholars have indicated "the problem of scale"[56], which implies that there are too many privacy policies to read as every website has its own version of the privacy policy. Also, apart from the privacy policy there are other legal documents on every website, such as the user agreement and the terms of service, which the user has to read and accept to be able to receive the services. Therefore, a conclusion could be made that there is a possibility for a person to read the privacy policies of several companies. However, in order to do it the user has to have a skill of self-management. But when the scale increases the self-management does not work appropriately.[57] Consequently:

> Even if every entity provided people with an easy and clear way to manage their privacy, there are simply too many entities that collect, use, and disclose people's data for the rational person to handle.[58]

This problem has also been identified by Lessig in a straightforward and simple way as he suggested that "no one has the time or patience to read through cumbersome documents describing obscure rules for controlling data".[59]

The results of a recent research made by the European Consumer Organization support the position that there are too many privacy policies for the consumer to read. The analyses of fourteen privacy policies of popular online services has revealed that these policies together have a significant amount of words to read, approximately 80.000 words.[60] The European Consumer Organization states that the reviewed privacy policies represent only a part of the policies that the average consumer needs to read online.

According to the outcomes of a Special Eurobarometer survey, which was made in year 2019, only thirteen percent of the respondents stated that they read the privacy policies. It is less then was indicated in year 2015. 66 percent of the

---

[54] A.M. McDonald, L.F. Cranor "The cost of reading the privacy policies" *I/S: A Journal of Law and Policy for the Information Society* 4 (2008): p. 565

[55] *Ibid.*

[56] Daniel Solove "Privacy self-management and the consent dilemma" *Harvard Law Review* 126 (2013): p.1889

[57] *Ibid.*

[58] Solove, *supra* note 56, p.1888

[59] Lessig, *supra* note 5, p. 204

[60] The European Consumer Organization. Study report. "CLAUDETTE meets GDPR". Available on: http://www.beuc.eu/search?keys=claudette&field_reference_value=&field_creation_date_value%5Bmin%5D%5Bdate%5D=&field_creation_date_value%5Bmax%5D%5Bdate%5D= Accessed June 06, 2020

respondents stated that the reason why they do not read the privacy policies is the excessive length of the privacy policies. And at least one out of ten respondents in the European Union thinks that it is not important to read the privacy policies.[61] The indicated results show that the willingness of the consumers to read the privacy policies has not increased and even has declined. These results also show that after the GDPR came into force the attitude of users towards private policies has changed in a negative direction.

The fact that it has become a standard behavior for the user to accept the privacy policy without reading, creates a legal paradox. On the one hand the user by affirmative action clearly indicates that he or she has read the policy when clicking on the "I agree" button. This action seems to constitute a valid consent under section 11 of Article 4 of the GDPR. On the other hand, if the consumer has not actually read the policy the question arises whether the consent to processing personal is informed and, therefore, valid.[62] Additional issue that might need more research is the problem to present the evidence that the user has not read the policy. The challenge occurs in the situation when a person in the past by affirmative action clearly has agreed on the provisions but then has acknowledged that he or she has not read the provisions of the privacy policy. It seems that the user will have the burden of proof in such case. Still it is unclear how would the user be able to prove that he or she has not read the policy.

Therefore, the problem of the users not reading the privacy policies has as least two negative effects. First is that consent of the user to processing personal data loses one of its quality and *de facto* stopes being informed. However, *de jure* consent is informed[63] as the user accepted the terms and conditions of the policy. Thus, the users might deprive themselves from the rights which the GDPR has granted to them.

The second aspect of the problem is the accessibility of the privacy policies. It has been observed in the literature that one of the main conditions for the privacy policy to be read by consumers is that the privacy policy is accessible. The level of quality of the content of the privacy policy does not make any difference unless the privacy policy is easy to find:

> Accessibility is key to usability. Unless policies are easily found and readily available to end users the quality of the policy doesn't really matter. When we talk about the accessibility of the privacy policies, we are really interested in two things: First, how easy is it for users to find the policy? This is a function of where the link to the policy is placed, and how visible it is to users.

---

[61] EU Open Data Portal. Special Eurobarometer 487a: The General Data Protection Regulation. Available on: https://ec.europa.eu/info/law/law-topic/data-protection/eu-data-protection-rules_en Accessed June 06, 2020

[62] *supra* note 1, Article 4(11).

[63] In this example for the mental experiment to be clearer, it is presumed that provisions of the privacy policy constitute informed consent and that the information is provided in accordance to provisions of GDPR. However, the user has not read the policy.

> Second, how easy is it to get a complete picture of the policy? This is a function of how long and how many pages the policy is spread across.[64]

The Article 29 Working Party has recommended that the online service provider shall place link that leads to the privacy policy on every page of the website. This link shall be noticeable, and the title of the link shall be the same on every page. The service provider may not have several different titles for the privacy policy in order not to confuse the consumer.[65] In the same recommendations the Article 29 Working Party defines that the practice to place the link in the position that makes the link less visible could not be considered as compliant with the requirements for accessibility. Also, it could not be considered as the best practice to color the link in less visible colors.[66]

However, the results of the analysis of the content of the privacy policies which are stated in the chapter 4 of the thesis has shown, that service providers do not pay enough attention to the accessibility of the privacy policies.

1.3.2 The problem of attitude

The second reason for the criticism of the present model of regulation is the problem of the existing tendency for the people to easily give up their personal data in exchange for access to the services. Moreover, for example, six out of ten respondents in the European Union are convinced that in order to obtain the online services the user shall disclose personal information to the service provider.[67] It has been indicated that the users "generally overestimate the value of some platforms' services, while underestimating the value of the personal data they divulge in return".[68]

The present model of self-regulation implies that the user has to read and understand the privacy policy before he or she could make an informative decision whether to enter into relationship with the service provider or not. Consequently, the user must make an assessment of possible harm that could be made to him or her on the very early stage of engagement with the service provider.[69] However, people often deny that extensive processing of their personal data might lead to negative consequences. Instead of taking steps on protection of personal data they address this problem with the nothing to hide argument. The essence of this argument was described by Solove. According to Solove people argue that it is normal to give up personal data because they have nothing to hide and, therefore, it is not interesting for

---

[64] C. Jensen, C. Potts "The privacy policies as Decision-Making Tools: An Evaluation of Online Privacy Notices." CHI '04: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, April 2004, p. 473

[65] Article 29 Working Party *Guidelines on Transparency under Regulation 2016/679* p. 8 Available on: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051 accessed June 06, 2020

[66] *Ibid.*

[67] EU Open Data Portal. Special Eurobarometer 359: Attitudes on Data Protection and Electronic Identity in the European Union. p.27 Available on: https://data.europa.eu/euodp/en/data/dataset/S864_74_3_EBS359 accessed June 01, 2020

[68] Viktoria Robertson "Excessive data collection: Privacy considerations and abuse of dominance in the era of big data" *Common Market Law Review* 57 (2020): p. 175.

[69] Solove, *supra* note 56, p.1891.

the government or other actors to trace them.[70] The problem of this argument is that people think that the main idea behind the concept of privacy is to hide negative facts about themselves.[71] It is difficult for people to take a pre-emptive action when they do not truly understand the negative effect of the absence of such actions. The results of the recent poll have shown that 77 percent of respondents in the European Union purchase goods or services on the Internet. 39 percent out of them buy on the Internet on a regular basis.[72] The Internet offers to the consumer to have a relationship with the supplier on a high speed. It does not take a lot of time and/or formalities to buy sneakers online. From the perspective of the consumer one of the main advantages of online commerce is that the Internet has eliminated all extra collateral activities which the consumer had to make in the offline environment. Therefore, the speed of the transactions has increased. It would be naive to expect from the consumer to decrease the speed of life, which is offered by the Internet, in order to read and understand the privacy policies. This statement is especially true in the conditions when no tangible losses for the consumer might be determined in advance. Therefore, the average user would rather believe that as long as he or she does not have things to hide, it would be justified to accept the privacy policy without the time-consuming assessment of the possible consequences.

On the other hand, the consequences for abuse of personal data usually have a cumulative nature and it is hard for an average user to assess them sufficiently on the early state of the cooperation with the service provider.[73]

Hence, the described attitudes among the users towards the necessity to read and understand the privacy policies rise the question whether the consent to accept the provisions of the privacy policy may be deemed as informed according to the provision of the GDPR. It seems to be reasonable to state that unless the user truly understands the consequences of the processing of personal data the consent may not be deemed as informed. However, there is no legal obligation for the service provider to explain these consequences to the user in terms of losses that user might have.

1.3.3 Unification of consent to the privacy policies

Another problem that emerges from the previously discussed problems is also connected to the level of quality of the consent of the user to the privacy policy. According to the GDPR consent of the user for the processing of the personal information shall be freely given, specific, informed and unambiguous.[74] Typically, the privacy policies are structured to be accepted or to be rejected by the user as a whole document. However, it would be logical to assume that in order to follow the requirements of the legislation the consent, which is obtained from the user, might not

---

[70] *Ibid.*

[71] Daniel Solove, "I've got nothing to hide and other misunderstandings of privacy", *San Diego Law Review* (2007) p. 764.

[72] EU Open Data Portal. Special Eurobarometer 487a: The General Data Protection Regulation.p.6 Available on: https://ec.europa.eu/info/law/law-topic/data-protection/eu-data-protection-rules_en Accessed June 06, 2020

[73] Solove, *supra* note 56, p.1893.

[74] *supra* note 1, Article 4 (11).

be identical for different persons. The observation of the procedure of how the consent is obtained by the service providers gives reasons to conclude that the consent is not personalised. The reason why the online service providers do not obtain personalised consents is obvious. "High-quality consent imposes many transaction costs that are difficult for companies to manage, particularly in high volume, distance transactions".[75] At the first sight it seems unrealistic to demand from the online service providers to obtain a personalised consent. This might entail, for example, that the service providers will have to negotiate with every user and to store all the documentation on the negotiation and its results. Nevertheless, in situation when the online business actors state that they need to process personal data in order to provide personalized services to the user[76], it is unclear why the consent to the processing of personal data shall be generic. If the services themselves, which are provided to billions of users, can be personalised and tailored[77], then it will be logically to assume that it is technically possible to obtain personalised consent to the processing of personal data.

Article 7 of the GDPR *inter alia*, regulates the consent, which is given in a form of acceptance of the provisions of the privacy policy. This Article states that:

> If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language.[78]

Therefore, the GDPR does not oblige the service providers to obtain personalised unique consent from every data subject. The Regulation is also silent on the question whether identical consents, obtained by one service provider, might form the valid consent. However, in practice some of the privacy policies, provisions of which *inter alia* provide that the acceptance of the privacy policy constitute the consent to the processing of personal data, are accepted by billions of users.[79] It would be wrong to state that each of these users provide the same amount and type of personal data to the service provider and for the same purposes of processing. The relationships between each user and the service provider are different at least because some of the services are personalised. Therefore, it would be reasonable to expect that these relationships are regulated according to different conditions and may not be regulated by one standard document. Thus, it seems to be justified to conclude that the consent which is presented in a form of acceptance of provisions of the privacy policy might not be deemed as of high-quality as long this consent is not personalised.

1.3.4 The problem of the unclear nature of the privacy policies

One more problem of the present model of self-regulation leads to the discussion about the nature of the privacy policies. It has been debated in the scientific circles whether provisions of the privacy policy are binding upon the user or in other words,

---

[75] Cris Hoofnagle "Designing for consent" *Journal of European Consumer and Market Law* 7 (2018): p.163

[76] For example, Google Account. Data and personalisation.

[77] Ariel Ezrachi, Viktoria H.S.E. Robertson, "Competition, Market Power and Third-Party Tracking", *World Competition* 42 (2019): p.6

[78] *supra* note 1, Article 7 (2).

[79] See chapter 3.

whether provisions of the privacy policies create obligations for the user.[80] The analysis of the problem leads to the assumption that the privacy policy creates corresponding obligations for the parties of the policy and therefore, that the privacy policy is of a contractual nature.[81]

In order to assess this assumption, it is necessary to establish functions of the privacy policies. The privacy policies are the self-regulatory tool of the online service providers. The initial function of the privacy policies is to increase user's knowledge about practices of online companies in respect to the processing of personal data. Yet, during the process of evolution of the privacy policies several additional functions have emerged. These functions have been identified, *inter alia*, by Article 29 Working Party.[82] The first function is to establish obligations of service providers on how personal data shall be processed by them. The second function is to bind companies with the terms and conditions of the privacy policies which establish such obligations. The third function is to clearly inform users about the rights that they have when their personal data is being processed. And the fourth, more general function, is to replace the possible strict legislation, which would regulate the business, with the regime of effective self-regulation.

However, it was observed that many the privacy policies have provisions that aim to establish obligations for the consumers towards service providers and as a consequence to bind consumers with such obligations. This conclusion is made according to the analysis of the drafting techniques of service providers which tend to use "the language of contract and assent"[83] in the privacy policies.

There are examples of the described drafting techniques. For instance, the clauses that regulate the procedure on how the privacy policy is amended. Typically, the user must accept the clause which states that service provider may amend the privacy policy from time to time on its own discretion.[84] Consent to these provisions might be considered as an acceptance to the offer[85] and therefore, might create bilateral contractual relationship. Similar consequences might be created by clauses which provide for the user's preliminary consent to the future possibility for the change of the owner of the service provider. These clauses might be considered as of contractual nature. Typically, the discussed clause in the privacy policy also declares that the relationship with a new owner shall be regulated by the provisions of the privacy policy that has been concluded with the previous owner. If the consent that is asked by the service provider from the user is given, the discussed clause basically transforms into a contract. This logic might lead to the conclusion that there is a possibility to enforce the clause according to the principle of *pacta sunt servanda.*

---

[80] S.van Gulik, J. Hulstijn, "Ensuring Data Protection by Private Law Contract Monitoring: A Legal and Value-Based Approach", *European Review of Private Law* 5 (2018): pp.637.

[81] Solove, Hartzog, *supra* note 31, p. 595

[82] Article 29 Working Party Guidelines on Transparency under Regulation 2016/679 p. 8 Available on: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051 accessed June 06, 2020.

[83] Allyson Haynes, "Online the privacy policies: Contracting away control over personal information?" *Penn State Law Review*, 111 (2007): p. 596.

[84] For example, Facebook data policy. Available on: https://www.facebook.com/privacy/explanation/ Accessed 27.05.2020.

[85] Killingsworth, *supra* note 28, p. 35.

Accordingly, some scholars conclude that the privacy policies are contracts by nature: "the website's promise and the user's use of the site and submission of personal data are each sufficient consideration to support a contractual obligation".[86] Consequently, the plausible result of such conclusion might be that the provisions of the privacy policy are enforceable in the court of law. The user and the service provider might have rights to "sue and seek all available remedies for breach of the privacy policy".[87]

On the other hand, rights and interests of users in relation to the processing of their personal data are guaranteed and protected by public legislation. Therefore, there is an opinion among scholars that consent to the processing of personal data and "contractual agreements are generally considered not to come into close contact"[88] and that the privacy policies are not of contractual nature. It is indicated in the literature that there have been several attempts to litigate on the basis of breach of contract, which resulted out of violations of the provisions of the privacy policy in the United States of America. These attempts have not been successful.[89] For example, the litigation have been lost mostly because the claimant has not been able to prove damages, which are the imperative element for an action for breach of contracts according to New York law.[90] However, even in jurisdictions where damages are not the imperative element in order to establish the breach of the contract, there would be no sense for the user to apply to the court without possibility to remedies. Therefore, indeed, it seems to be challenging, for example, for the user to be able to calculate and to prove in court damages that might occur due to the violation of the provisions of the privacy policy that establish the period for information retention. It appears that it would be difficult for the user to prove that storage of personal information for the longer period than it has been promised in the privacy policy itself has led to any kind of loses or harm. As well as it would be challenging to the service provider to establish damages, which might occur due to violations of the privacy policy by the user. Moreover, the privacy policies typically do not provide for contractual liability of the parties, for example, in a form of contractual penalties. Also, it worth noting that the privacy policies by definition are meant to be user centric.[91] Thus, at least from the theoretical point of view, there could be no balance between the parties in the privacy policies.

Another argument against the theory that the privacy policies are contracts is that there are no provisions on monetary consideration in the privacy policies. While

---

[86] Killingsworth, *supra* note 28, p. 35.

[87] Ibid.

[88] K. Pormeister, "Informed consent to sensitive personal data processing for the performance of digital consumer contracts on the example of "23andMe", *Journal of European consumer and Market Law* 6 (2017): p.17.

[89] Solove, Hartzog, *supra* note 31, p. 596.

[90] In re JetBlue Airways Corp. Privacy Litigation, 379 F. Supp. 2d 299 (E.D.N.Y 2005) District Court, E.D. New York.

[91] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - Online Platforms and the Digital Single Market Opportunities and Challenges for Europe (COM(2016)288) p. 4 Available on: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52016DC0288 accessed 01.06.2020

online companies provide services to the user, the user provides personal data in response, according to provisions of the privacy policies. Yet, among the scholars the question remains whether personal data shall be treated as a sufficient consideration.[92]

The legislation of the European Union directly does not regulate the relationship which commoditise personal data. Though, the Directive 2019/770 appeals to this topic. The Recital 24 of Directive proclaims that "the protection of personal data is a fundamental right and that therefore personal data cannot be considered as a commodity".[93] However, in the same Recital the Directive admits that there is a steady practice in the market where a company provides digital services for the user for free in exchange for the personal data. The Directive does not encourage but at the same time does not prohibit such practice. Therefore, according to the legislation personal data can constitute contractual consideration.

Still, it seems that for the personal data in order to constitute sufficient counter-performance several conditions have to be fulfilled. First, it shall be stated directly in the provisions of the agreement that personal data is a consideration for the services. On the other hand, the service provider often obtains personal data even before parties enter into the contract, for example, during negotiations or preparatory work. Therefore, the personal data alone, without consent of the user, might not be valuable for the service provider. Consequently, the second condition for the personal data to constitute sufficient consideration might be the existence of the consent of data subject for the processing the data. Therefore, data subject might have an obligation under the contract to provide personal data and to give an explicit consent to the processing of personal data.[94] However, data subject has the right to withdraw the consent on his or her own discretion according to legislation.[95] This conclusion could be also supported by the provisions of the Recital 67 of Directive 2019/770:

> Where the digital content or digital service is not supplied in exchange for a price but personal data are provided by the consumer, the consumer should be entitled to terminate the contract also in cases where the lack of conformity is minor, since the remedy of price reduction is not available to the consumer.[96]

Thus, the consideration in a form of personal data with the consent to the processing of personal data would not guarantee the stability of the contractual relationship to the service provider.

Finally, if to accept the assumption that the privacy policy is of a contractual nature, it remains unclear, what kind of contract it might be.[97] As it was mentioned before the services that online companies provide are usually regulated by separate agreements with the user, namely terms of service and/or user agreement. Therefore,

---

[92] C. Langhanke, M. Schmidt-Kessel "Consumer Data as Consideration" *Journal of European Consumer and Market Law* 4 (2015): p. 218

[93] *supra* note 9, Recital 24.

[94] C. Langhanke, M. Schmidt-Kessel "Consumer Data as Consideration" Journal of European Consumer and Market Law (2015), Volume 4, Issue 6, p. 223

[95] *supra* note 1, Article 7 (3).

[96] *supra* note 9, Recital 67.

[97] Zohar Efroni "Gaps and opportunities: the rudimentary protection for "data-paying consumers" under new EU consumer protection law" *Common Market Law Review* 57 (2020): p. 800

the privacy policy might have the same object of contract as terms of service and/or user agreement. Then, it would seem reasonable to merge the privacy policy with the terms of services as they have the same object of contract. Consequently, there would be no logic for the privacy policy to exist in a form of a separate document. Provisions of the privacy policy would be implemented as clauses of terms of services or user agreement. However, the consent of the user for the processing of personal data is not regulated by provisions of contract law as it is regulated by public law. And in the case when provisions of national contract law lead to any inconsistency with the provisions of the GDPR, provisions of the later shall prevail:

> This rule represents the general understanding that neither contract law in general nor specific consumer protection provisions, can derogate from the level of protection persons enjoy under data protection and privacy law.[98]

Therefore, service providers need the privacy policy to be drafted in a form of separate document to secure themselves in cases when the processing of personal data is based on consent. Thus, it appears unreasonable for the service provider to merge provisions of the privacy policy into other agreements. In this case service providers will have to obtain a separate consent from the user for the processing of personal data.

In conclusion it shall be noted that the problems which are associated with self-regulation by means of the privacy policies in their core have the issue of questionable consent of the user. It has become common practice that the privacy policies are accepted by users without being read and/or understood. This practice is facilitated by service providers as they do not make attempts to slow the user and to check whether the user at least has read the privacy policy. The typical the privacy policy comprises provisions required by the law in a form of considerably long and often obscure legal document with unclear nature. For service providers the privacy policy is merely the tool for the compliance with legislation on protection of personal data. Therefore, it has become a standard to focus the provisions of the privacy policies on the consent of the user to processing personal data instead of aiming to insure the clear understanding of privacy practices of the company.

[98] Efroni, *supra* note 97, p. 806

THE INFLUENTIAL THE PRIVACY POLICIES AND USER'S CONSENT

In order to answer the research question, it is important to analyze the provisions of the privacy policies which have prevalent position in the online market. As it was mentioned before the privacy policy is an instrument of self-regulation. The regime of self-regulation implies that there are standards, which are accepted by the actors in the industry. For the purposes of the analysis several the privacy policies were examined. These policies can be defined as "influential the privacy policies". By "influential the privacy policies" in this analysis are meant the privacy policies which are drafted and adopted by transnational private actors.[99] These policies might be viewed as setting the standard for the content of the privacy policies of the online companies. There are reasons for that. Such transnational private actors as Google, Facebook, LinkedIn, Apple, Microsoft represent non-state actors that have the ability to regulate behavior of others and therefore, exercise quasi-regulatory functions when governments in the same conditions are not able to do so.[100] Furthermore, they have the necessary capacity to establish standards of the industry. They have internal dedicated legal staff, they are transnational, therefore, their policies are applicable in different jurisdictions, they are willing to comply with the legislation, they have good reputation across the industry and they process a lot of personal data. Also, such companies occupy a dominant position in a certain sphere of online commerce.[101] For example, Google has a dominant position as a search engine, Facebook is a leader among social networks and LinkedIn, which belongs to Microsoft group of companies, has a dominant position as a professional social network.

Moreover, Lynskey refers to such transnational private actors as to companies with data power and also gatekeepers.[102] He states that the processing of personal data by companies with data powers might influence rights of data subjects in a negative way even more, than these rights might be influenced by the same actions of governments.[103]

For example, in relation to online platforms it was observed in a literature that they:

> have a direct impact on the rights to privacy and data protection as a result of their role in setting privacy and data use conditions for all applications using their software.[104]

Consequently, the analysis of these the privacy policies shall reveal the trends of the industry in relation to the content of the privacy policies.

---

[99] *supra* note 13, p. 671.

[100] Orla Lynskey, "Grappling with "Data Power": Normative Nudges from Data Protection and Privacy" *Theoretical inquiries in Law* 20 (2019):p.201

[101] *supra* note 13, p. 675.

[102] Lynskey, *supra* note 100, p.201

[103] *Ibid.*

[104] Orla Lynskey, "Regulating "Platform power" LSE Law, Society and Economy Working Papers 1/2017 p.13 Available on: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2921021 accessed 09 June, 2020

In order to receive services according to provisions of influential the privacy policies user has to accept the privacy policies,[105] consequently, it is justified to assume that the user has to give two types of consent by this accept. The first type of consent is consent to provisions of the privacy policy, acceptance of which does not constitute consent to the processing of personal data. For example, provisions that regulate succession of the privacy policy in case of any of corporate action in respect to service provider or consent to the processing of data, which does not constitute personal data under the GDPR.

The second type of consent in the privacy policy is consent to the processing of personal data, which according to the provision of section 11 of Article 4 of GDPR shall be freely given, specific, informed and unambiguous.

The analysis will be focused on both types of consent, which when combined, form the general consent to accept the provisions of the privacy policy. Therefore, the main questions for the analysis shall be:

1) Is the privacy policy accessible?

2) Does the privacy policy clearly state what personal data is being processed by the service provider?

3) Does the privacy policy clearly state the purposes for processing of personal data?

4) Does the privacy policy provide for the period of storage of personal data?

5) What is the procedure for the amendment of the privacy policy?

For the purposes of answering the questions indicated above, provisions of influential the privacy policies are compared with the provisions of the GDPR. Also, the comparison is based on the recommendations that have been given by the European Data Protection Board, Article 29 Working Party and on the case law.

1.4 Google the privacy policy

According to Alphabet Inc. Annual Report, in 2019 “Google's core products and platforms, such as Android, Chrome, Gmail, Google Drive, Google Maps, Google Play, Search, and YouTube each have over one billion monthly active users”.[106] These numbers give the reasonable ground for the assumption that Google the privacy policy has been accepted by users more than dozen billion times. Moreover, amendments to Google the privacy policy have been accepted by users at least ones a year.[107] Even among legislative acts there are not many documents in the world that regulate legal relationships for such number of natural persons. Therefore, Google the

---

[105] For example, see Google privacy policy. Available on: https://policies.google.com/privacy?fg=1accessed 27.05.2020

[106] Alphabet Inc. Annual Report p.5 Available on: https://abc.xyz/investor/static/pdf/20200204_alphabet_10K.pdf?cache=cdd6dbf Accessed 29.05.2020

[107] Google privacy policy. Available on: https://policies.google.com/privacy?fg=1 Accessed 07.06.2020

privacy policy might be considered as an influential document that makes trends for drafting of the privacy policies by other actors in the industry.

Google the privacy policy is located in the right bottom corner of the main page of Google website along with six other sections.[108] It can be stated that the policy is considerably easy to find.

There are fifteen chapters in Google the privacy policy. In PDF format it has thirty pages of text with clickable links included in the provisions of the policy. These clickable links contain definitions for terms which are used in Google the privacy policy. Thus, the actual length of the policy is more than thirty pages. This approach might not be in compliance with the recommendations of Article 29 Working Party Guidelines on transparency that the information shall be presented efficiently "in order to avoid information fatigue".[109]

The main text is divided into relatively short chapters and subchapters. Google the privacy policy sets up the aim to itself to "explain things as clearly as possible".[110] In order to achieve that aim the main text is written in simple language and does not have heavy legal terms or definitions. This approach is in compliance with the recommendations of the European Data Protection Board Guidelines 05/2020 on consent, which requires to use language "understandable for the average person and not only for lawyers".[111]

In its first statement Google the privacy policy accepts that Google processes personal data of its clients. Also, the policy makes a promise to put the user in control of how his or her information is being used by Google.[112] Further it gives a definition of personal data that Google collects and stores. However, the policy defines personal data through the term "personal information". According to Google the privacy policy personal information is:

> information that you provide to us which personally identifies you, such as your name, email address, or billing information, or other data that can be reasonably linked to such information by Google, such as information we associate with your Google Account.[113]

On the other hand, the legislation of the European Union provides for a different definition of personal data, which is:

---

[108] Google. Available on: https://www.google.com/Accessed 27.05.2020

[109] Article 29 Working Party *Guidelines on Transparency under Regulation 2016/679* paragraph 8 Available on: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051 accessed June 06, 2020

[110] Google privacy policy. Available on: https://policies.google.com/privacy?fg=1Accessed 27.05.2020

[111] The European Data Protection Board. Guidelines 05/2020 on consent under Regulation 2016/679 of, paragraph 67. Available on: https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_en accessed 06.06.2020

[112] Google privacy policy. Available on: https://policies.google.com/privacy/key-terms#toc-terms-personal-info Accessed 27.05.2020

[113] Google privacy policy. Available on: https://policies.google.com/privacy?fg=1Accessed 27.05.2020

> personal data means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. [114]

Although, from the first impression definitions seem to be very similar, they are not. Both definitions describe "personal information" and "personal data" as information with the ability to identify a natural person. Also, both definitions do not provide for an exhaustive list of what shall be considered as "personal information" or "personal data". However, the detailed comparison of the definitions shows that the definition of "private information" in Google the privacy policy is substantially narrower than the definition of "personal data" in the GDPR.

The literal interpretation of the first part of the definition of personal information in Google the privacy policy might lead to the conclusion that personal information shall be only the information which is provided to Google by the user. This statement seems to be misleading. It might create the false idea for the user that personal data can be obtained by Google only directly from the user. Furthermore, the wrong conclusion could be made that if personal data have not been obtained directly from the user by Google, or have not been *provided* by the user to Google, it is not treated by Google as "personal information" anymore. However, the GDPR regulates cases where "personal data have not been obtained from the data subject".[115] Apart from that, further in the end of the chapter "Information we collect as you use our services" it is stated that Google collects information about its users from the third parties.[116]

The words "personally identifies you" could also be interpreted as the narrower concept than "any information relating to an identified or identifiable natural person"[117] provided by the GDPR. According to Cambridge dictionary word "personally" has several meanings, which include "used when you give your opinion"[118] and "affecting you and not anyone else".[119] Therefore, by using word "personally" before word "identifies" Google the privacy policy gives an additional connotation to the definition as a whole. This connotation might create a limiting impression that personal data shall be such information, based on which an opinion about a person can be formed or which directly identifies a person. However, in accordance with the provisions of the GDPR personal data is any information that

---

[114] *supra* note 1, Article 4 (1).
[115] *supra* note 1, Article 14.
[116] Google privacy policy. Available on: https://policies.google.com/privacy?fg=1Accessed 27.05.2020
[117] *supra* note 1, Article 4 (1).
[118] Cambridge Dictionary Available on: https://dictionary.cambridge.org/dictionary/english/personally accessed May 27, 2020
[119] *Ibid.*

directly or indirectly identifies a person.[120] This conclusion might be supported by the case law of the Court of Justice of the European Union, which stated, that:

> The use of the expression 'any information' in the definition of the concept of 'personal data', within Article 2(a) of Directive 95/46, reflects the aim of the EU legislature to assign a wide scope to that concept, which is not restricted to information that is sensitive or private, but potentially encompasses all kinds of information, not only objective but also subjective, in the form of opinions and assessments, provided that it 'relates' to the data subject.[121]

Furthermore, the definition in Google the privacy policy establishes that personal information is not limited by the definition itself. However, it is also stated that personal information could be "other data that can be reasonably linked to such information by Google".[122] This statement limits the perception of the concept of personal data for the user. According to the Recital 26 of the GDPR[123] and the case law of the Court of Justice of the European Union it is not required for the information to be controlled by a single legal entity to be considered as "personal data".[124] Google could obtain from the user or from the third party information which alone does not constitute personal data. However, in order to constitute personal data it is enough for the information to have the ability to identify a person when combined with another information.[125] Also, from the point of view of the Court of Justice of the European Union it is not important which legal entity would do the "linking" for the determination whether the information constitutes the personal data.[126] Therefore, it seems reasonable if words "by Google" would be excluded from the definition of personal information provided by Google the privacy policy.

Another example of misleading usage of the definition of personal information could be found in the chapter "Things you create or provide to us".[127] The clickable term "personal information" is used there as one of examples of information which could be provided to Google by the user. In the same chapter phone number, payment information, email, photos and videos, docs and spreadsheets, comments are listed as information that might be provided additionally to provided "personal information".[128] Thus, the interpretation of the chapter as a whole might lead the user to a false conclusion that term "personal information" which is given by Google the

---

[120] *supra* note 1, Article 4 (1).

[121] The Court of Justice of the European Union: Judgement of 20 December 2017, *Nowak*, C-434/16, EU:C:2017:994, paragraph 34.

[122] Google privacy policy. Available on: https://policies.google.com/privacy?fg=1 Accessed 27.05.2020

[123] *supra* note 1, Recital 26.

[124] The Court of Justice of the European Union: Judgement of 19 October 2016, *Breyer*, C-582/14, EU:C:2016:779, paragraph 43.

[125] The Court of Justice of the European Union: Judgement of 19 October 2016, *Breyer*, C-582/14, EU:C:2016:779, paragraph 37.

[126] The Court of Justice of the European Union: Judgement of 19 October 2016, *Breyer*, C-582/14, EU:C:2016:779, paragraph 48.

[127] Google privacy policy. Available on: https://policies.google.com/privacy?fg=1Accessed 27.05.2020

[128] *Ibid.*

privacy policy excludes phone number, payment information, email, photos and videos, docs and spreadsheets, comments.[129] This false conclusion might have a negative effect on the rights of data subject which are given by the legislation. The user might not understand that he or she has rights towards the information that seems to be excluded from the term "personal information" by Google the privacy policy.

Further, the analysis shows that the usage of the definition of personal information provided in the privacy policy is inconsistent. In several chapters instead of the term "personal information" Google uses words "information that personally identifies you" or "your data".[130] Such inconsistence could seem not important. However, it might suggest that the consent to the privacy policy which is given by the user is not informed. The user might conclude that he or she does not have rights in respect to the information which is not indicated as "personal information" in the policy. Therefore, it is not clear from the policy what information Google consider as personal data. The conclusion could be made that Google the privacy policy does not clearly state what personal data is processed by Google.

The policy establishes the list of purposes for processing of personal data. Among the list there are such purposes as development of new services or protection of Google, its users and the public.[131] These purposes might not be in compliance with the principle of data minimization, which is proclaimed by the GDPR.[132] It seems that the development of new services might require more personal data than it is required for the provision of existing services. The way the purposes are formulated does not provide for the possibility of any limitation.

The provisions of the policy on data retention periods are vague and unclear. It is stated in the policy that the retention period depends on user's settings. Therefore, for the unregistered user it is impossible to fully understand how long the retention period is.

Finally, Google reserves a right to change its privacy policy anytime. It is indicated that Google "will not reduce your rights under this The privacy policy without your explicit consent".[133] The interpretation of this statement might lead to a justified conclusion that Google the privacy policy can be changed by Google unilaterally without explicit consent of the user if on Google's absolute discretion the changes do not reduce user's rights. Also, the language of the statement mentioned above implies that Google is the only party that has a right to assess whether the changes of provisions of the policy affect rights of the user. Moreover, Google is the only party that has a right to initiate any changes to the policy. The policy does not provide for the possibility to negotiate the changes, even though the user and Google have already established certain relationship based on the initial conditions of the

---

[129] *Ibid.*

[130] *Ibid.*

[131] Google privacy policy. Chapter "we use data to build better services". Available on: https://policies.google.com/privacy?fg=1Accessed 27.05.2020

[132] *supra* note 1, Article 5 (1)(c).

[133] Google privacy policy. Available on: https://policies.google.com/privacy?fg=1Accessed 27.05.2020

privacy policy. The only choice which is left for the user if he or she does not agree with proposed changes is to delete user's account and not to use service anymore. [134] In the procedure which Google uses for the privacy reminder it is indicated that if person decides to delete the account, there is no possibility to have an access to the certain content on Google play or You Tube anymore.[135] The statement is applicable to purchases of movies or rentals for which the date of termination of the contract haven't come yet. The statement also includes services by subscription, for example Google Play Music and applications that have been bought by the user on Google Play.[136]

Thus, the described consequences of deletion of user's account could influence the decision whether to accept proposed changes to Google the privacy policy or to delete an account. According to the GDPR consent shall not be considered as freely given if the data subject does not have true or free choice or there is no possibility for the data subject to refuse or withdraw consent without disadvantage.[137] In circumstances stated above the user might give his or her consent to changes to the privacy policy only because he or she might lose or might think that it is possible to lose money when deleting an account.[138] Therefore, the conclusion could be made that Google's procedure for adoption of new versions of the privacy policy violates user's right to freely given consent which is granted by the GDPR.

In conclusion it should be noted that Google the privacy policy is drafted with an obvious purpose to convince the user that Google's approach to privacy is focused primarily on the user's rights. On the other hand, Google the privacy policy is a document which is drafted in a form of unilateral statement and provides the user with an illusion of consensual relationship.

The analysis of the provisions of the policy shows that the definition of personal information is vague and misleading. It is important to indicate that the discussed definition is a key definition for the user to understand what personal data is being collected by Google and what rights does the user have in respect to such information. However, the given definition is used only in the first part of the document and is not used in the second part. Consequently, the policy lacks the coherence because of the inconsistence in usage of its main term. It is not definitively clear from the text of the policy which personal data is collected by Google. Also, purposes of the processing of personal data are not limited and vague. The acceptance of the provisions of the policy forms the condition for the data subjects to use the services. The policy guarantees that changes to the policy will not derogate from the rights of the user which are initially granted by the policy. However, there is no right for the user to negotiate the conditions of the new versions of the privacy policy that

---

[134] Google Account help. Available on https://support.google.com/accounts/answer/6227261?hl=en Accessed 27.05.2020

[135] *Ibid.*

[136] *Ibid.*

[137] *supra* note 1, Recitals 42, 43.

[138] The European Data Protection Board. Guidelines 05/2020 on consent under Regulation 2016/679 of, paragraph 24. Available on: https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_en accessed 06.06.2020

are adopted by Google. Also, there is no right for the user to accept separate parts or clauses of the Google privacy policy and no right to initiate any changes to the accepted privacy policy. Therefore, the promise to put user in control, that Google the privacy policy makes in its first heading[139] seems to be simply untrue.

1.5 Facebook data policy

According to Facebook Report to investors on the first quarter of 2020 results, there are 2,60 billion monthly active users and 1,73 billion daily active users on Facebook as of March 31, 2020.[140] This statistics put Facebook in a position of the most popular online social network platform in the world. To consume services that Facebook provide, users must accept its data policy.

Facebook data policy is a separate document which focuses exclusively on the information that is collected by Facebook from and/or about the user. Facebook has located its data policy in the bottom of the main webpage. However, the clickable link "Privacy", that leads to the text of the policy, is placed among other twenty-eight links.[141] The link is not easy to find. It seems that the policy has been placed with a purpose not to draw additional attention of the potential user to it. Facebook data policy consists of eleven chapters, which is approximately fourteen pages of text.

The first chapter is dedicated to the information collected by Facebook about the user. The Facebook data policy in contrast with Google the privacy policy does not provide for the definition of personal data. Instead of the special term it uses words "your data" and "information about you" when listing the information that is being collected by Facebook.[142] Consequently, Facebook in its data policy does not make a clear direct statement that it collects personal data in the meaning of provisions of the GDPR.

For example, in the subsection "Network and connections" of the section "Device information" of the chapter "What kinds of information do we collect?" it is stated in the same sentence that Facebook collects:

> information such as the name of your mobile operator or ISP, language, time zone, mobile phone number, IP address, connection speed and, in some cases, information about other devices that are nearby or on your network, so we can do things like help you stream a video from your phone to your TV .[143]

From the perspective of the average user it is hard to imagine that information about time zone and connection speed might constitute personal data because it is not obvious that these pieces of information might somehow identify data subject.

---

[139] Google privacy policy. Available on: https://policies.google.com/privacy?fg=1Accessed 27.05.2020

[140] Facebook Investor Relations. Available on: https://investor.fb.com/investor-news/press-release-details/2020/Facebook-Reports-First-Quarter-2020-Results/default.aspx Accessed 27.05.2020

[141] Facebook. Available on: https://www.facebook.com/ Accessed 27.05.2020

[142] Facebook data policy. Available on: https://www.facebook.com/privacy/explanation/ Accessed 27.05.2020

[143] *Ibid.*

However, it is generally known that the user may be identified, for example, by IP address. Moreover, according to the interpretation of provisions of the Directive 95/46[144] that has been given by the Court of Justice of the European Union, IP address may constitute personal data because it "allows users to be precisely identified".[145] Therefore, Facebook puts categories of information, the processing of which might create different legal consequences for the user in the same row and in the same sentence. Thus, by the way the presented clause is structured it might create the wrong impression for the user, that IP address cannot be used for identification purposes.

Moreover, the chapter which provides for the controversial clause does not indicate in its heading, which is "What kinds of information do we collect?", that among other kinds of information the chapter regulates the collection of personal data. This might lead to the situation that the user just skips and does not read the chapter as he or she might consider it to be irrelevant to the processing of personal data.

Also, the revised clause of the data policy reveals practice of Facebook to collect information about other devices, which are located closely to the device of the user. It is unclear from the statement on what basis the information from the device, which is located closely to the device of the user, is being processed by Facebook. This statement might constitute violations of the provisions of section 1 of Article 6 of the GDPR. In this situation the user of the later device might not be a user of Facebook. Therefore, he or she have not given consent to processing of personal data and processing of personal data is not necessary for the performance of a contract. Other grounds for lawful processing also seem to be not applicable in this case.[146]

Another concern towards Facebook data policy is that it does not explain the user which information, collected by Facebook, creates legal rights for the user and which does not.[147] As a result of such approach in drafting of provisions of the privacy policy the user might not be able to obtain unambiguous concise understanding of rights that he or she has under the privacy policy. Facebook data policy aims to provide the user with examples and typical cases to illustrate how and when it collects personal data. However, the policy describes Facebook privacy practices in an abstract way. Therefore, Facebook data policy does not clearly state what personal data is processed by Facebook. This practice of Facebook does not seem to be in compliance with provisions of section 1 of article 12 of the GDPR and with the recommendations of Article 29 Working Party Guidelines on transparency.[148]

Facebook data policy defines the purposes for which personal data is being processed. However, the purposes are stated in the non-exhaustive way. It might be concluded that according to the policy the list of purposes gives Facebook right to

---

[144] *supra* note 24.

[145] The Court of Justice of the European Union: Judgement of 19 October 2016, *Breyer*, C-582/14, EU:C:2016:779, paragraph 33.

[146] *supra* note, 1 Article 6 (1).

[147] Facebook data policy. Available on: https://www.facebook.com/privacy/explanation/ Accessed 27.05.2020

[148] Article 29 Working Party Guidelines on Transparency under Regulation 2016/679 as of 29 November 2017. Paragraph 6. Available on: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051 accessed June 06, 2020.

process personal data for any purpose without obtaining additional consent from the user. This approach might violate the provisions of the GDPR on the principle of purpose limitation, according to which purposes of processing of personal data shall be specific, explicit, and legitimate.[149]

The chapter "New owner" declares that personal data of the user could be transferred to the new owner of a product.[150] By accepting the data policy the user give his or her consent to this possible future transaction. However, terms and conditions of such transactions are unknown to the user at the moment of consent. This might lead to a conclusion the acceptance of provisions of Facebook data policy creates a future obligation for the user to enter into contractual relationship with random legal entity. Moreover, the decision whether the user enters into such contractual relationship or not and on what conditions is made by Facebook on its own discretion.

Facebook data policy informs the user about the retention period. However, it is stated in the policy that the retention period is identified on the basis of "case-by-case determination".[151] Therefore, the policy does not provide the user with the certain information on the retention period. From the content of the provisions of the privacy policy the user cannot make an assessment whether the retention period is acceptable.

Finally, the policy establishes that the changes to the data policy shall be made by Facebook unilaterally. Facebook declares that "We'll notify you before we make changes to this policy and give you the opportunity to review the revised policy before you choose to continue using our Products".[152] The interpretation of this clause leads to the conclusion that there is no possibility left for the user to edit proposed changes, negotiate, or accept them partially. The policy does not establish any limitation for possible changes. The user, who refuses to accept proposed changes to the privacy policy, must stop using services of Facebook. The approach, when the user is left with take-it-or-leave-it option might be referred to as exploitative abuse.[153] In described situation the user does not have an actual choice. The only opportunity for the user is to accept that his or her data might be processed by Facebook according to the conditions that are unilaterally offered by Facebook.[154]

An important issue here is that for the user it might be impossible to delete Facebook account from the social and psychological point of view. The reason for that is a unique position of Facebook on the market of social online networks. Facebook offers to the user the opportunity to be connected by his account with friends, family and acquaintances, to share content and to communicate. The motto of

---

[149] *supra* note 1, Article 5 (1)(b).

[150] Facebook data policy. Available on: https://www.facebook.com/privacy/explanation/ Accessed 27.05.2020

[151] *Ibid.*

[152] *Ibid.*

[153] Martin Moore, Damian Tambini, *"Digital Dominance: the Power of Google, Amazon, Facebook and Apple"* (Oxford:Oxford University Press, 2018) p.89

[154] *Ibid.*

the company is "Connect with friends and the world around you on Facebook".[155] The average user of Facebook has approximately one hundred fifty five friends on Facebook.[156] Because of the big amount of the active users Facebook has obtained the network effect. In academic literature the network effect of social online platforms has been discussed and described as "the direct network effects might be experienced in the context of a social networking service where the more individuals avail themselves of the service the more utility that service is to others".[157] The federal Cartel Office in Germany (Bundeskartellamt) in its Decision as of 06 February 2020 has indicated that the bigger the network is the lesser users are being left for its competitors and eventually users shift to the larger network.[158] Further, Bundeskartellamt has stated, that as a result of indirect and direct network effects combined together, the probability that users will leave the network is very low. Leaving the network will lead to the loss of the contacts for users because the possibility that their contacts will leave the network is also very low.[159] Bundeskartellamt has pointed out that the existence of Facebook account might have a significant impact on life of users:

> In view of the role played by the social network as the online reflection of their social environment and activities, users often cannot even refrain from using the network as this would isolate them from their contacts and the exchange of information.[160]

Therefore, the situation in which the user must delete his or her account because of the rejection to accept the new version of the privacy policy could be unimaginable to the user, especially when "goods and services are given away "freely" in exchange for personal data".[161] It also has been discussed in the academic literature that:

> If the platforms at the heart of the digital economy were entirely committed to monetization and efficiency, they would offer consumers more options. A user might be offered the opportunity to pay, say, twice the discounted present value of the data he was expected to generate for the platform. In return, he is assured that his data is unavailable for the platform's use. But such a seemingly Pareto-optimal arrangement is not on offer, and its invisibility suggests why imbalances in power, rather than efficiency or consent, ought to be the normative focus of antitrust and privacy law.[162]

---

[155] Facebook. Available on: https://www.facebook.com/ Accessed 27.05.2020

[156] The Telegraph. Available on: https://www.telegraph.co.uk/news/science/science-news/12108412/Facebook-users-have-155-friends-but-would-trust-just-four-in-a-crisis.html Accessed 27.05.2020

[157] Lynskey, *supra* note 100, p.213.

[158] Bundeskartellamt Decision (B6-22/16), 6 February 2019. paragraph 424 Available on: https://www.bundeskartellamt.de/SharedDocs/Entscheidung/EN/Entscheidungen/Missbrauchsaufsicht/2019/B6-22-16.html accessed 10.06.2020

[159] Bundeskartellamt Decision (B6-22/16), 6 February 2019. paragraph 448 Available on: https://www.bundeskartellamt.de/SharedDocs/Entscheidung/EN/Entscheidungen/Missbrauchsaufsicht/2019/B6-22-16.html accessed 10.06.2020

[160] *Ibid.*

[161] Blume P. "Data protection in the private sector" *Scandinavian studies in Law* 47 (2004): p. 306

[162] Frank Pasquale "Privacy, antitrust, and power" *Geo. Mason L.Rev*. 20 (2013) p.1023

Due to provisions of section 4 of Article 7 of the GDPR in order to make an assessment whether consent is freely given it shall be determined if provision of services is conditional on consent of data subject to the processing of personal data. Recital 43 of the GDPR clarifies that a clear imbalance between the user and service provider indicates that consent shall not be deemed as freely given. According to the Decision of Bundeskartellamt Facebook occupies dominant, quasi-monopolistic position on the market, "with a user share more than 90 percent"[163] in Germany and this position creates clear imbalance between the user and Facebook.[164]

Thus, the consent given by the user to proposed changes of data policy by default could be considered as conditional and not freely given.[165]

The analysis of Facebook data policy shows that the provisions of the policy about what personal data of the user is being processed by Facebook are vague. The policy seems to be written in a plain language because of extensive usage of words like "you", "us", "your data". However, the policy does not provide the user with clear understanding of his or her rights towards each piece of collected personal data. Some provisions of the policy have characteristics of separate additional contract, for example, the provisions about the change of the ownership of a product. However, the policy does not explain what legal consequences for the user may occur after accepting such provisions. Furthermore, Facebook data policy the same as Google the privacy policy does not let the user to participate in the process of drafting of changes to the privacy policy. It is impossible for the user instead of accepting the edited version of the policy to proceed using services under the version of the policy that was initially accepted. Also, there is no possibility for the user to propose changes to the privacy policy. The conclusion could be made that although the privacy policy has elements of a contract the user is not treated by Facebook as an equal party to the agreement. Principles of individual autonomy and freedom of contract are not followed by Facebook data policy. By accepting the privacy policy, the user most likely does not have a will to enter into a contract and does not understand that he or she might create contractual obligations for themselves. Therefore, it would be justified to make an assumption that provisions of the policy, which are structured as a contract, would not be enforceable from the perspective of contract law. However, the presence of such clauses in the policy might confuse the user. As a result, Facebook the privacy policy does not fulfill its main function – to inform the user about privacy practices of Facebook.

1.6 Microsoft Privacy Statement

According to Microsoft Annual Report 2019, Office 365 Commercial has 180 million users, Outlook apps on iOS and Android have more than one hundred million users.[166]

---

[163] Bundeskartellamt Decision (B6-22/16), 6 February 2019. Paragraph 646 Available on: https://www.bundeskartellamt.de/SharedDocs/Entscheidung/EN/Entscheidungen/Missbrauchsaufsicht/2019/B6-22-16.html accessed 10.06.2020

[164] *Ibid.*

[165] Bundeskartellamt Decision (B6-22/16), 6 February 2019. Paragraph 5 Available on: https://www.bundeskartellamt.de/SharedDocs/Entscheidung/EN/Entscheidungen/Missbrauchsaufsicht/2019/B6-22-16.html accessed 10.06.2020

Microsoft privacy statement is a separate document which has been located in the bottom of the home webpage.[167] The policy has thirteen chapters and approximately nine pages of text. Microsoft privacy statement uses term "personal data" for the description of the information that is collected from the user and processing of which is regulated by the policy.[168] However, the policy does not give the definition of personal data and does not clearly provide what personal data is collected by Microsoft.[169]

The policy divides personal data in two categories. Personal data that is needed for the performance of the services and optional personal data, which is not needed for the performance of the services but the collection of which may improve the services. Also, the policy clearly defines the consequences that occur if the user does not want to provide mandatory or optional personal data.[170]

Microsoft directly states that "not all personal data processed by Microsoft can be accessed or controlled via the tools"[171] that are listed in the policy. Therefore, Microsoft clarifies that the user has a right to address to Microsoft his or her concerns about all categories of personal data that is being collected. Microsoft declares that more than 28 million people had exercised their rights in respect to personal data that is processed by Microsoft in the period between May 2018 and October 2019.[172]

It is interesting that Microsoft put a clause in its privacy statement that establishes the hierarchy between the privacy statement and contracts, concluded by Microsoft with its users. The discussed clause provides that in case of any discrepancies between provisions of privacy statement and terms of contract concluded between a client and *Microsoft for Enterprise and Developer Products, terms and conditions of such contract shall prevail.*[173] This clause does not apply directly to personal data of natural persons because clients of *Microsoft for Enterprise and Developer Products are legal entities. Nevertheless,* it shows the general attitude of Microsoft towards the privacy statement. The conclusion could be made that privacy statement is not viewed by Microsoft purely as a declaration of the company which binds only Microsoft. It seems that Microsoft attempts to give to its the privacy policy character of a bilateral agreement.

---

166 Microsoft Annual Report 2019 Available on: https://www.microsoft.com/investor/reports/ar19/index.html Accessed 29.05.2020

167 Microsoft. Available on: https://www.microsoft.com/en-gb Accessed 29.05.2020

168 Microsoft privacy statement. Available on https://privacy.microsoft.com/en-gb/privacystatement Accessed 29.05.2020

169 The European Data Protection Board. Guidelines 05/2020 on consent under Regulation 2016/679 of, paragraph 64. Available on: https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_en accessed 06.06.2020

170 Microsoft privacy statement. Chapter "Personal data we collect". Available on: https://privacy.microsoft.com/en-gb/privacystatementAccessed 29.05.2020

171 Microsoft privacy statement. Chapter "How to access and control your personal data". Available on: Accessed https://privacy.microsoft.com/en-gb/privacystatement29.05.2020

172 Microsoft privacy report. Available on: https://privacy.microsoft.com/en-US/privacy-report Accessed 29.05.2020

173 Microsoft privacy statement. Chapter "Enterprise and developer products". Available on: https://privacy.microsoft.com/en-gb/privacystatement accessed 29.05.2020

However, as it was previously discussed in Chapter 2.2.4 thereof the processing of personal data in the European Union is regulated by the GDPR and not by the provisions of contract law. Section 2 of Article 7 of the GDPR states that "if the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matter".[174] Therefore, the inclusion in the privacy policy clause of contractual nature might confuse the user and be not in compliance with the indicated provisions of the GDPR.

On the other hand, the statement is silent about how it is being updated and whether there are any limitations in respect to such updating.

Also, the statement does not provide any information for the retention period, which is not in compliance with Article 13 (2) (a) of the GDPR.

In the chapter "How we use personal data" Microsoft lists such purposes as "to improve and develop our products". The indication of the purpose of processing of personal data is not in compliance with provisions of Article 5 (1) (b) of the GDPR, which stated that the purpose of processing shall be specific according to the principle of purpose limitation. Such practice is also described as poor by paragraph 12 of Guidelines on transparency of 29 Article Working Party.

The analysis of the provisions of Microsoft privacy statement shows that its provisions are not much elaborated. It seems to be justified to state that the reason for that appears to be the business model of Microsoft. For Microsoft it is not vital to process as much different types of personal information as it is processed by Google and Facebook. For example, Microsoft states that it does not use "emails, chat, files or other personal content to target ads to you".[175]

However, the approach to divide collected personal data to *required* and *optional* is in compliance with provisions of the GDPR.[176] The provisions of the policy that describe the consequences for the user if he or her refuses to provide required or optional personal information seem to create transparent practice. The GDPR prescribes that in order to determine whether the consent is freely given, it should be considered whether the performance of a contract "is conditional on consent to the processing of personal data that is not necessary for the performance of that contract".[177] Therefore, mentioned above practices of Microsoft are in compliance with the legislation. Such practices offer the actual possibility to the user to make a free and informed decision on what personal data to provide to Microsoft in different situations.

1.7 Apple The privacy policy

[174] *supra* note 1, Article 7 (2).
[175] Privacy at Microsoft. Available on https://privacy.microsoft.com/en-gb/privacystatement Accessed 29.05.2020
[176] *supra* note 1, Article 5(1) (c).
[177] *supra* note 1, Article 7 (4).

Apple products include iPhone, iPad, Mac, Apple Watch, Apple TV, five software platforms: iOS, iPadOS, macOS, watchOS, and tvOS, and services such as the App Store, Apple Music, Apple Pay, and iCloud.[178] Apple the privacy policy establishes legal relationships with great amount of users. This assertion means that Apple the privacy policy is a legal instrument that has global influence on how personal data of natural person is being processed and how the information on privacy practices of companies is provided to users.

It is not easy to find Apple the privacy policy. It takes at least three steps if the user is specially looking for it. The user must scroll down to the very bottom of Apple's home webpage, which is rather long.[179] There, the user can find a clickable link "Privacy" amongst other fifty clickable links. Then the user gets to the page dedicated to privacy where Apple promotes its level of protection of the user. On this page the clickable link which leads to the privacy policy can be found. It could be reasonably assumed that the user has to be dedicated to the idea to read Apple the privacy policy to find it and not be distracted with other clickable links, which are presented in the way to draw maximum attention. The described approach might be not in compliance with the recommendations of Article 29 Working Party, which are given in Guidelines on Transparency.[180] According to paragraph 11 of the Guidelines "The "easily accessible" element means that the data subject should not have to seek out the information".[181]

The privacy policy is a separate document. The approximate length of the policy is ten pages.

Apple the privacy policy provides for its own definition of personal data. The definition is "Personal information is data that can be used to identify or contact a single person".[182] This definition does not seem to be misleading and is in consistence with the definition of personal data which is given by the GDPR.[183]

Further, the privacy policy divides information that Apple collects into two groups: personal information and non-personal information.[184] Non-personal information is defined as "data in a form that does not, *on its own*, permit direct association with any specific individual".[185] However, the analysis of this definition gives the reasonable ground to assume that if the data is combined, Apple would obtain the ability

---

[178] Apple Investor Relations. Available on: https://www.apple.com/newsroom/2020/04/apple-reports-second-quarter-results/ accessed May 30, 2020

[179] Apple. Available on: https://www.apple.com/ Accessed 29.05.2020

[180] Article 29 Working Party Guidelines on Transparency under Regulation 2016/679 as of 29 November 2017. Available on: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051 accessed June 06, 2020.

[181] Article 29 Working Party Guidelines on Transparency under Regulation 2016/679 as of 29 November 2017 paragraph 11. Available on: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051 accessed June 06, 2020.

[182] Apple The privacy policy. Available on https://www.apple.com/legal/privacy/en-ww/ Accessed 29.05.2020.

[183] *supra* note 1, Article 4 (1).

[184] Apple The privacy policy Chapter "Collection and Use of Non-Personal Information. Available on https://www.apple.com/legal/privacy/en-ww/ Accessed 29.05.2020

[185] *Ibid.*

to identify data subject.[186] Then Apple states that the company and its affiliates have right to collect, use, transfer, and disclose non-personal information on their own discretion and provides for non-exhaustive list with examples of such information.[187] Further, the declaration is made that in the situation when Apple combines non-personal information and personal information, the result will be considered as personal information.[188] Yet, the described process seems to be not in compliance with the GDPR and the case law of the Court of Justice of the European Union. According to the case law of the Court of Justice of the European Union it is not necessary for the isolated piece of information to have the ability to identify the person.[189] It is enough for this piece of information to create a possibility that when combined with other information the result could lead to the identification of a person.[190]

Therefore, two conclusions could be made based on the analysis of the chapter on non-personal information of Apple the privacy policy.

The first conclusion is that the definition of non-personal information, provided in the privacy policy might be considered as misleading. The information, which alone does not identify data subject, still could be personal data.[191] Thus, Apple and its affiliates do not have right to collect, use, transfer and disclose such information on their own discretion without consent of the user or without other conditions which are established by the GDPR, these actions might be considered as unlawful.[192] On the other hand, by accepting the privacy policy the user consents to the definition and to the consequences for which the definition provides. This raises the question whether the consent of the user to the provisions of the privacy policy which are not in compliance with the case law and, consequently with the provisions of the GDPR, be considered as valid.[193] Also, the legal problem could be identified as whether the consent to the discussed clause of the privacy policy creates legal rights and obligations for the parties, or the clause shall be treated as automatically invalid for the reason that it misleads the user. According to provisions of Article 7 of the GDPR the consent to the processing of personal data may be given as a part of declaration which also regulates different issues. However, if any part of such

---

[186] The European Consumer Organization. Study report. "CLAUDETTE meets GDPR". p.49 Available on: http://www.beuc.eu/search?keys=claudette&field_reference_value=&field_creation_date_value%5Bmin%5D%5Bdate%5D=&field_creation_date_value%5Bmax%5D%5Bdate%5D= accessed June 06, 2020

[187] Apple The privacy policy Chapter "Collection and Use of Non-Personal Information. Available on https://www.apple.com/legal/privacy/en-ww/ Accessed 29.05.2020

[188] *Ibid.*

[189] The Court of Justice of the European Union: Judgement of 24 November 2011, *Scarlet Extended*, C-70/10, EU:C:2011:771, paragraph 51

[190] The Court of Justice of the European Union: Judgement of 19 October 2016, *Breyer*, C-582/14, EU:C:2016:779, paragraph 33.

[191] The Court of Justice of the European Union: Judgement of 19 October 2016, *Breyer*, C-582/14, EU:C:2016:779, paragraph 33.

[192] *supra* note 1, Article 6.

[193] *supra* note 1, Article 4 (11).

declaration violates provisions of Regulation this part automatically becomes non-binding.[194]

The second conclusion is that the promise of Apple the privacy policy to treat non-personal information as personal data in a case if non-personal information is combined with personal information is also might be considered as misleading. By this promise the privacy policy makes an attempt to narrow the object of rights of the user in relation to the information that is being collected by Apple. Several pieces of non-personal information, which are combined, could create personal data.[195] Consequently, those pieces of information shall be treated as personal data even if they are not combined with information that is considered as personal by Apple. The existence of possibility to combine several pieces of data with such a result that may lead to identification of a person is enough for those pieces of data to separately constitute personal data.[196] The provisions of Recital 26 of the GDPR support this conclusion.[197]

Therefore, the conclusion could be made that Apple the privacy policy does not unambiguously state what personal data is processed by Apple. Instead of identifying personal data that is being processed, Apple the privacy policy introduces the definition of non-personal information which might confuse the user. The list of personal data that is collected by Apple provided in the policy is not exhaustive. Thus, this clause might be interpreted in a way that when the user accepts the privacy policy, he or she accepts the general clause that Apple may collect any personal information about the user. However, the European Data Protection Board in Guidelines 05/2020 on consent has stated that the information shall be provided to the user on "what (type of data) data will be collected". [198] Also, such approach is not in compliance with the principle of purpose limitation, which is established by Article 5 (1) (b) of the GDPR.

Further, the privacy policy states that Apple "will not be able to respond to any queries you may have"[199] in the case if the person refuses to provide personal information that Apple have requested. This statement raises some questions. For example, it is uncertain whether the statement refers to the situation of initial request of personal information when the data subject is not yet a user of Apple's services or also to the situation when Apple requires additional personal data from the user. In both situation such statement might constitute a violation of provisions of Article 13 (1) of the GDPR, which prescribes "at any time when personal data are obtained" [200]

---

[194] *supra* note 1, Article 7 (2).

[195] The Court of Justice of the European Union: Judgement of 19 October 2016, *Breyer*, C-582/14, EU:C:2016:779, paragraph 33.

[196] The Court of Justice of the European Union: Judgement of 19 October 2016, *Breyer*, C-582/14, EU:C:2016:779, paragraph 41-45.

[197] *supra* note 1, Recital 26.

[198] The European Data Protection Board. Guidelines 05/2020 on consent under Regulation 2016/679 of, paragraph 64. Available on: https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_en accessed 06.06.2020

[199] Apple The privacy policy. Chapter "Collection and Use of Personal Information" Available on https://www.apple.com/legal/privacy/en-ww/ Accessed 29.05.2020

[200] *supra* note 1, Article 13 (1).

to provide a certain information to the data subject. Therefore, in a case when data subject has concerns and asks question, for example, about the purpose of the processing, before providing the personal data, it seems reasonable to expect that the party which requested personal data would answer such question. This conclusion is supported by the provisions of paragraph 10 of the Guidelines on Transparency of Article 29 Working Party, which state that:

> A central consideration of the principle of transparency outlined in these provisions is that the data subject should be able to determine in advance what the scope and consequences of the processing entails and that they should not be taken by surprise at a later point about the ways in which their personal data has been used.[201]

Apple the privacy policy does not provide the information about what is the time limit for storage of personal information. Instead of that, is states that Apple retains personal information according to the principle that consists of two elements. The first element is that personal data is collected exclusively for the purposes which are indicated in the policy. And the second element is that personal information is being retained for the period of time which shall not be longer than is needed to achieve the purposes of collection[202]. Due to provisions of the GDPR if it is not possible to indicate the period for which the storage of personal data applies Apple shall disclose the criteria to define such period.[203] It appears that the criteria that established in Apple the privacy policy is not transparent. For example, according to the policy one of Apple's purposes for collection of personal data is facilitating the creation, development and improvement of services, products, content and advertising.[204] This statement could lead to the conclusion that it is impossible to identify the period for which personal data is being stored by Apple. It is very unlikely that Apple would stop the development of its products, for example, company's Annual Report for 2019 states that Apple is dedicated to the expansion of its market opportunities in respect to electronic devices.[205] Therefore, the assumption could be made that according to the provisions of Apple the privacy policy the user has consented for his or her personal data to be stored by Apple by unlimited period of time. However, this is not provided by terms of the policy directly. Consequently, conditions of the privacy policy could be considered as misleading. On the other hand, the acceptance of these conditions by the user could be also perceived as consent because the policy directly lists the

---

[201] Article 29 Working Party Guidelines on Transparency under Regulation 2016/679 as of 29 November 2017. Available on: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051 accessed June 06, 2020.

[202] Apple The privacy policy. Chapter "Integrity and Retention of Personal Information" Available on https://www.apple.com/legal/privacy/en-ww/ Accessed 29.05.2020

[203] *supra* note 1, Article 13 (2)(a).

[204] Apple The privacy policy. Chapter "How we use personal information" Available on https://www.apple.com/legal/privacy/en-ww/ Accessed 29.05.2020

[205] Apple Investor Relations. Annual Reports on Form 10-K. Available on: https://www.apple.com/newsroom/2020/04/apple-reports-second-quarter-results/ accessed May 30, 2020

purposes of collection of the personal information.[206] Thus, it is unclear, whether parties have any rights and obligations in respect to provisions of the privacy policy on the term of retention of personal information. It is also unclear, whether the consent of the user to the provisions of the privacy policy as a whole has constituted the consent to one separate provision which appears to be not transparent and even misleading. Nevertheless, the described approach might be not in compliance with the recommendations of Article 29 Working Party, according which state that:

> The storage period (or criteria to determine it) may be dictated by factors such as statutory requirements or industry guidelines but should be phrased in a way that allows the data subject to assess, on the basis of his or her own situation, what the retention period will be for specific data/ purposes. It is not sufficient for the data controller to generically state that personal data will be kept as long as necessary for the legitimate purposes of the processing.[207]

Finally, the provisions on how Apple the privacy policy shall be amended are not elaborated and not clear. It is stated directly that Apple is the only party to the privacy policy with the right to amend the policy. Moreover, it is stated that the policy shall be changed occasionally. Apple promises to notify the user only when the privacy policy is going to be altered in a substantial manner. There is no indication in the policy on any limitations in respect to amendments to the policy. However, the possibility for the user to opt-out from certain separate provisions is not regulated by the policy. Also, the policy is silent about whether the user has a right to propose changes to the policy or negotiate at least certain conditions of the policy. However, it is stated that Apple might consider changes to the privacy policy in case if the user files a reasonable complaint.[208]

Apple the privacy policy does not introduce the division of personal information that is being collected on the required information an optional information. From the user's perspective it is not oblivious whether he or she has a right under the policy to refuse to provide part of the personal information that Apple has inquired.

1.8 Linkedin privacy policy

Linkedin presents itself as the "world's largest professional network".[209] According to the information on its website Linkedin has approximately 690 million users in the world. To get access to the services that Linkedin provides users must accept the provisions of Linkedin privacy policy.

---

[206] Apple The privacy policy. Chapter "How we use personal information" Available on https://www.apple.com/legal/privacy/en-ww/ Accessed 29.05.2020

[207] Article 29 Working Party Guidelines on Transparency under Regulation 2016/679 as of 29 November 2017 p.38. Available on: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051 accessed June 06, 2020.

[208] Apple The privacy policy. Available on https://www.apple.com/legal/privacy/en-ww/ Accessed 29.05.2020

[209] About Linkedin. Available on: https://about.linkedin.com/ accessed June 02, 2020

The hyperlink to Linkedin privacy policy is placed in the very bottom of the homepage of the website.[210] It is not hidden but also is not placed to draw attention of the user.

Linkedin privacy policy is comparatively long as it consists of sixteen pages. It also has hyperlink with definitions inside the main text of the policy.

Linkedin privacy policy does not provide for a specific definition of personal data. In the first chapter, which is called "Data we collect" the policy states that in order to create an account the user shall give to Linkedin *inter alia* name, email address, mobile number, billing information.[211] However, the policy does not directly state that the information required to create an account is personal data in accordance to legislation. Yet, further, the policy uses term personal data and makes examples of such data, which do not include the name, mobile number, email address or billing information.[212] However, such information is acknowledged as personal data by the case law of the Court of Justice of the European Union, because such information "represents information relating to an identified or identifiable natural person".[213]

Therefore, from the first chapter the privacy policy misleads the user because it might be not clear for the user whether the information required to create an account constitute personal data and whether the user has any rights in respect of that data.

The policy is structured in a way to notify the user about the data that is being collected by Linkedin. However, it does not clearly explain to the user which data is required and which is optional. Although there are separate clauses in the policy on the possibility for the user to refuse to opt-in for the collection of some types of personal data these clauses are not organized for user convenience.[214]

The chapter of the policy which is dedicated to the description of how personal data is being used by Linkedin is vague and does not provide the consumer with a comprehensive understanding of the issue. The policy establishes that the way Linkedin uses personal information of its consumers depends on what functions of services are used by the consumer and on the choices that were made by the consumer in the settings while using services.[215] In other words, it puts on the user the responsibility on how personal information is being used by Linkedin. The indicated approach might be considered as noncompliance with the provisions of section 1 of

---

[210] Linkedin. Available on: https://www.linkedin.com/ accessed June 02, 2020

[211] Linkedin. The privacy policy. Subchapter "Data you provide to us". Available on: https://www.linkedin.com/legal/privacy-policy?trk=homepage-basic_footer-privacy-policy accessed June 02, 2020

[212] Linkedin. The privacy policy. "Posting and uploading". Available on: https://www.linkedin.com/legal/privacy-policy?trk=homepage-basic_footer-privacy-policy accessed June 02, 2020

[213] The Court of Justice of the European Union: Judgement of 16 December 2008, *Huber*, C-524/06 EU:C:2008:724, paragraphs 31 and 43

[214] Linkedin. The privacy policy. Chapter "Your device and location". Available on: https://www.linkedin.com/legal/privacy-policy?trk=homepage-basic_footer-privacy-policy accessed June 02, 2020

[215] Linkedin. The privacy policy. Chapter "How we use your data". Available on: https://www.linkedin.com/legal/privacy-policy?trk=homepage-basic_footer-privacy-policy accessed June 02, 2020

Article 5 of the GDPR. These provisions establish the principles of purpose limitation and data minimization.[216] According to the principle of data minimisation, the processing of personal data shall be limited "to what is necessary in relation to the purposes for which they are processed".[217] However, in this case it seems that Linkedin makes an attempt not to limit data processing to the purposes of processing but to leave the decision on any limitation of the processing of personal data to the user. Also, Linkedin does not provide for a possibility to the person who is not registered as a user of the platform to familiarize himself or herself with the settings. Therefore, there is no opportunity to understand what options are given in the settings in order for the consumer to make an informative decision on whether to register as a user or not. The described approach could be considered as noncompliant with the definition of consent that is given by the GDPR which provides that consent shall be informed.[218]

It is stated in the private policy that Linkedin stores personal data of the user for the period of time while the user keeps being register with the platform. Also, there are exemptions from that rule. For example, the policy states that Linkedin retains personal data of the user even after the user deletes its account on the platform if to the full discretion of Linkedin it is required in order to fulfill law enforcement requests.[219] On the other hand, it is not indicated whether such law enforcement request shall exist by the time when user decides to delete the account, or it can be a possible future law enforcement request. Also, the policy does not elaborate on the precise indication of which personal data is stored by Linkedin less or more than during user's registration. Therefore, in violation to the provisions of the GDPR, Linkedin does not disclose all the criteria that indicate the period of storage of personal data.[220]

Finally, Linkedin privacy policy declares that changes to the policy may be made by Linkedin unilaterally. There is no possibility for a user to propose changes to the policy, negotiate or accept separate clauses of the privacy policy. Also, there is no limitation provided on how Linkedin the privacy policy may be amended.

Accordingly, in conclusion it worth noting that Linkedin privacy policy does not aim to help the user to obtain a clear understanding on what personal data is being processed by Linkedin. It would be justified to state that Linkedin privacy policy focuses more on the issues of regulation of horizontal relationships the subject of which is disclosure and sharing of personal information between platform's users. Linkedin does not identify exact list of personal information that it processes but only gives a general statement that it does process personal data. Furthermore, provisions of Linkedin privacy policy explicitly declare that the choice on how personal information is used by Linkedin is delegated to the user. However, the policy also

---

[216] *supra* note 1, Article 5(1) (b,c).

[217] *supra* note 1, Article 5(1)(c).

[218] *supra* note 1, Article 4 (11).

[219] Linkedin. The privacy policy. Chapter "Account closure". Available on: https://www.linkedin.com/legal/privacy-policy?trk=homepage-basic_footer-privacy-policy accessed June 02, 2020

[220] *supra* note 1, Article 13 (2)(a).

states that personal data is needed for provision of the services, *inter alia*, the development of the services.[221] Therefore, it is obvious that the user does not have complete control over the usage of his or her personal data. The user does not have the possibility to influence the decisions that are made by Linkedin on the development of its services. Consequently, the indicated above statement of Linkedin that user has the capability to make an actual choice on how Linkedin uses his or her personal data seems to be overexaggerated because the user does not have the capacity to make such choice.

[221] Linkedin. The privacy policy. Chapter "How we use your data". Available on: https://www.linkedin.com/legal/privacy-policy?trk=homepage-basic_footer-privacy-policy accessed June 02, 2020

COMMON FLAWS OF INFLUENTIAL THE PRIVACY POLICIES

In the previous chapter five influential the privacy policies have been analyzed in the light of consent that user gives when accepts provisions of these the privacy policies. The analysis has revealed flaws that are common for the revised policies. According to the results of the analysis several conclusions could be made.

The first conclusion is that the privacy policies are long documents, which are not easy to read and understand. Even though policies aim to use simple not legal language, the excessive length of these documents and complex structure does not make them easier to understand and might confuse the reader. Microsoft has the shortest the privacy policy among analyzed with nine pages, Google has the longest with thirty pages and clickable links with additional definitions inside the main text. This does not comply with the provisions of the Guidelines 05/2020 on consent under Regulation 2016/679 of the European Data Protection Board, which state that "controllers cannot use long the privacy policies that are difficult to understand".[222]

Also, not all reviewed the privacy policies are easy to find. Moreover, among analyzed the privacy policies none were placed in a way to intentionally draw attention of the user to them. Some of analyzed policies were placed in a more visible position than others. However, it is obvious that service providers do not have intention to focus the potential user on their privacy policies. Some of the features, that were indicated in the privacy policies as possibilities to control personal data which user provides, were not accessible for not registered user.[223] Therefore, the potential user has no chance to check whether he or she is comfortable with the whole system to which the privacy policy refers. The Guidelines 05/2020 on consent under Regulation 2016/679 of the European Data Protection Board (The Guidelines 05/2020) states that the information shall be provided to the potential user before the consent is given. This order is necessary for the user to be able to understand what the consent is given for. Otherwise, the consent shall be invalid as "user control becomes illusory".[224]

Therefore, the practice which establishes that data subject has to register in order to be acquainted with the detailed procedures of processing of personal data may be not in compliance with the provisions of Article 5 of the GDPR as violating the requirement for transparency.[225]

Therefore, all analyzed the privacy policies do not pass the test of accessibility.

---

[222] The European Data Protection Board. Guidelines 05/2020 on consent under Regulation 2016/679 of, paragraph 67. Available on: https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_en accessed 06.06.2020

[223] *Supra* Chapter 3.5.

[224] The European Data Protection Board. Guidelines 05/2020 on consent under Regulation 2016/679 of, paragraph 62. Available on: https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_en accessed 06.06.2020

[225] *Ibid.*

The second conclusion is that all of the reviewed the privacy policies do not aim to form the clear understanding for the user about what personal information is processed by service providers. All reviewed the privacy policies do not provide for the exhaustive list of personal data that is collected and processed by service providers. It could be explained by the fact that the GDPR also does not define the exhaustive the list of personal information.[226] However, the reason why the GDPR does not limit the definition of personal data is obvious. The purpose is to leave the possibility for the broader interpretation of what information can be personal data as the concept of personal data is not static and develops along with the technology. On the other hand, the reason for the privacy policies not to define the exhaustive list of personal data, which is being processed under the provisions of these the privacy policies, seems to be different. Such approach restricts the understanding of the user of what personal data is being processed. It leaves the user with the impression that service provider does not processes extensive amount of personal data. *De jure* the provisions of the privacy policies could be interpreted in a way that the user has consented to the processing of all of his or her personal data. However, such approach might be considered as the violation of the principle of purpose limitation and the principle of data minimization, which are established by Article 5 (1) (b) (c) of the GDPR. *De facto* the user might not understand that the consent is given to the processing of all of his or her personal data as it is not indicated directly in the privacy policies. This violates provisions of Article 6 (1) (a) of the GDPR, which state that consent shall be given for specific purposes. Due to paragraph 56 of the Guidelines 05/2020 the requirements of the GDPR for specific consent and purpose limitation serve as a protection against "the gradual widening or blurring of purposes for which data is processed".[227] Also, as the privacy policies do not clearly state what personal data is being processed by the service provider, consent of the user to the processing of personal data cannot be deemed as informed.[228]

Further, the review policies do not provide for clear and specific purposes for processing of personal data. It seems to be justified to conclude that the indication of such purposes as "development of our products" or "research purposes" cannot be deemed as specific and therefore, violates provisions of Article 6 (1) (a) of the GDPR. According to Article 29 Working party opinion 3/2013 on purpose limitation:

> a purpose that is vague or general, such as for instance 'improving users' experience', 'marketing purposes', 'IT-security purposes' or 'future research' will - without more detail - usually not meet the criteria of being 'specific'.[229]

Also, the privacy policies do not provide for "separate opt-in for each purpose".[230]

---

[226] *supra* note 1, Article 4 (1).

[227] The European Data Protection Board. Guidelines 05/2020 on consent under Regulation 2016/679 of, paragraph 56. Available on: https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_en accessed 06.06.2020

[228] The European Data Protection Board. Guidelines 05/2020 on consent under Regulation 2016/679 of, paragraph 64. Available on: https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_en accessed 06.06.2020

[229] Article 29 Working Party Opinion on Purpose limitation 3/2013 Available on: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm#maincontentSec5 p.16 accessed June 06, 2020

The fourth conclusion is that the privacy policies do not provide for the certain period of storage of the personal data.[231] The privacy policies tend to include the storage criteria in their provisions instead of the indication of the certain period of data retention. The criteria are formulated in a way that does not allow for the user to make an assessment of the retention period.[232]

Finally, the procedure of amendment of the privacy policies does not put the user in control of personal data. The user does not have an actual choice on whether to accept or to refuse the proposed amendments. The only choice the user has is to accept the amendments or to stop using the online services. However, this situation creates imbalance of power[233] and therefore, consent cannot be deemed as freely given.[234]

---

[230] The European Data Protection Board. Guidelines 05/2020 on consent under Regulation 2016/679 of, paragraph 60. Available on: https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_en accessed 06.06.2020

[231] *supra* note 1, Article 13 (2)(a).

[232] Article 29 Working Party *Guidelines on Transparency under Regulation 2016/679* p. 38 Available on: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051 accessed June 06, 2020

[233] *supra* note 1, Recital 43.

[234] The European Data Protection Board. Guidelines 05/2020 on consent under Regulation 2016/679 of, paragraph 24. Available on: https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_en accessed 06.06.2020

CONCLUSION

The purpose of the thesis was to identify the existing problems of user's consent to the privacy policies.

The author of the thesis has made an assumption that the current nature of consent of the user to the privacy policies is twofold. Typically, according the procedure that is offered by the online service provider, the user has to accept the privacy policy as a whole document by clicking "I agree" button. However, the provisions of the privacy policy include statements, consent to which might form consent to the processing of personal data in accordance with the provisions of the GDPR.

Therefore, on the one hand, by accepting the privacy policy, the user gives consent to the processing of his or her personal data by a clear affirmative action.[235] This consent shall be in compliance with the requirements of Article 4 (11) of the GDPR. On the other hand, the privacy policy provides for other provisions, consent to which is out of the scope of the GDPR. However, when the user consents to such other provisions by clicking "I agree" button, it might form the acceptance of the offer and thus create binding contractual relationship between the user and the service provider. Nevertheless, the user might not intend to create such binding contractual relationship.

On order to reach the indicted purpose and to check the proposed assumption the research question was posed:

Does the acceptance of provisions of the privacy policy form the valid consent thereof?

In order to answer this question, the nature of the privacy policy was analyzed. The divergent opinions in the academic literature about the legal nature of the privacy policies were revised and discussed. In author's opinion the privacy policies are not of the contractual nature and, therefore, do not create binding obligations for the user. On the one hand, the privacy policies are not directly regulated by the legislation. However, on the other hand, the privacy policies usually include provisions which are regulated by public law for example, provisions on consent of the user to the processing of personal data. These provisions shall not be regulated by contract law.[236] Unless, service providers exclude such provisions from the content of the privacy policies, it cannot be justified to state that the privacy policies might obtain contractual nature by the fact that the user accepts its provisions. Thus, the conclusion shall be made that the second type of the consent of the user to the privacy policy does not create binding obligations for the user.

However, the nature of the consent of the user to provisions of the privacy policies which are outside the scope of the GDPR remains unclear and might be a topic for future deeper research.

---

[235] *supra* note 1, Article 4 (11).

[236] Efroni, *supra* note 97, p. 806

For the purposes of the justification of the previous conclusion the main part of the thesis was devoted to the analysis of the privacy policies of five companies with data power[237], which are Google, Facebook, Linkedin, Microsoft and Apple. These companies were choses as they represent the tendency of the industry in the area of the processing of the persona data. The analysis was based on the questions, which aim to test the validity of the first type of the user's consent to the privacy policies. This consent shall be given in accordance with the provisions of the GDPR and, therefore, shall be freely given, specific, informed and unambiguous.

However, the analysis has revealed that the revised the privacy policies are not in compliance with the provisions of the GDPR. The content of policies is vague, the provisions of the policies do not clearly state what personal data is going to be processed by the online service provider, they do not provide for specific purposes[238] of the processing of personal data. Thus, the consent shall not be deemed as specific. The procedure of acceptance and amendment of the privacy policy puts user in a position, where the provision of the services is conditional on consent of the user. Yet, the user has no possibility to make an assessment whether all personal data, which is collected from the user, is necessary for the performance of the services. Also, it was indicated in the research that there is an obvious imbalance of power between the user and analysed service providers.[239] Thus, the consent shall not be deemed as freely given. The provisions of revised the privacy policies are structured in a way that the user cannot make an informative decision on whether to give consent on the processing of personal data before the actual engagement with the service provider. The privacy policies refer to features which describe how user can control his or her personal data. However, the significant part of such features can be observed only by the registered user. Thus, the consent shall not be deemed as informed.

Consequently, in author's opinion the provisions of revised the privacy policies do not provide for the valid consent of the user on the processing of personal data. The conclusion could be made that personal data of billions of users is being processed on the basis of invalid consent and, therefore, such processing is not lawful.[240]

According to the results of the present research another conclusion could be made. In author's opinion the regime of self-regulation by means of the privacy policies, provisions of which aim to create consent of the user to the processing of personal data in order to comply with the provisions of the GDPR, does not work properly. The online service providers abuse their rights and do not intend to obtain valid consent from the user. On the other hand, Article 29 Working Party in Guidelines on transparency has stated in paragraph 11 that the online service provider

---

[237] Lynskey, *supra* note 2, p.201

[238] *supra* note 1, Article 5 (1) (b).

[239] Bundeskartellamt Decision (B6-22/16), 6 February 2019. Paragraph 646 Available on: https://www.bundeskartellamt.de/SharedDocs/Entscheidung/EN/Entscheidungen/Missbrauchsaufsicht/2019/B6-22-16.html accessed 10.06.2020

[240] *supra* note 1, Article 6 (1) (a).

shall have the privacy policy. The European Data Protection Board has endorsed these guidelines.[241]

Therefore, the present system of the regulation of the privacy policies and their content needs further deeper research. The aim of such research might be to establish possible directions of new more efficient and effective regulation of the privacy policies in situations where their provisions provide for the consent of the user to the processing of personal data.

BIBLIOGRAPHY

1.9 Primary sources

1.9.1 Legislation

1. The Convention for the Protection of human Rights and Fundamental Freedoms (Rome, 4 November 1950). Article 8. Available on https://www.echr.coe.int/Documents/Convention_ENG.pdf Accessed June 8, 2020.
2. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Council of Europe, CETS No.108, 1981.
3. Treaty on the Functioning of the European Union (Consolidated version 2012), OJ C 326, 26.10.2012. Available on: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012E/TXT Accessed June 8, 2020.
4. Charter of Fundamental Rights of the European Union [2012] OJ C326/391.
5. Regulation (EU)2016/679 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)". Available on: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679 Accessed April 16, 2020.
6. Directive 95/46/EC 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". Available on:https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A31995L0046 Accessed May 27, 2020.
7. Directive 2002/58/EC of 12 July 2002 "Concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)" Available on: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32002L0058 Accessed May 27, 2020.
8. Directive (EU) 2016/680 of 27 April 2016 "On the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA". Available on: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016L0680 accessed June 08, 2020.
9. Directive 2009/136/EC of 25 November 2009 "Amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation bet ween national authorities responsible for the enforcement of consumer protection laws" Available on: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32009L0136 Accessed May 27, 2020.

[241] The European Data Protection Board. GDPR:Guidelines, Recommendations, Best Practices. Available on https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_en accessed June 12, 2020

10. Directive 2005/29/EC of 11 May 2005 "Concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council ('Unfair Commercial Practices Directive')" Available on: https://eur-lex.europa.eu/eli/dir/2005/29/oj/en accessed June 02, 2020.
11. Directive (EU) 2019/2161 of 27 November 2019 "Amending Council Directive 93/13/EEC and Directives 98/6/EC, 2005/29/EC and 2011/83/EU of the European Parliament and of the Council as regards the better enforcement and modernisation of Union consumer protection rules" Available on:https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32019L2161 Accessed 01.06.2020.
12. Directive (EU) 2019/770 of 20 May 2019 "On certain aspects concerning contracts for the supply of digital content and digital services" Available on: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32019L0770 Accessed 05.06.2020.

1.9.2 Case law

13. ECHR: Malone v. The United Kingdom, judgment of 02 August 1984, Series A no. 8691/79 Available on: https://hudoc.echr.coe.int/eng#{%22fulltext%22:[%228691/79%22],%22documentcollectionid2%22:[%22GRANDCHAMBER%22,%22CHAMBER%22],%22itemid%22:[%22001-57533%22]}Accessed June 8, 2020.
14. The Court of Justice of the European Union: Judgement of 19 October 2016, *Breyer*, C-582/14, EU:C:2016:779.
15. The Court of Justice of the European Union: Judgement of 24 November 2011, *Scarlet Extended*, C-70/10, EU:C:2011:771.
16. The Court of Justice of the European Union: Judgement of 16 December 2008, *Huber*, C-524/06 EU:C:2008:724.
17. The Court of Justice of the European Union: Judgement of 20 December 2017, *Nowak*, C-434/16, EU:C:2017:994.
18. In re JetBlue Airways Corp. Privacy Litigation, 379 F. Supp. 2d 299 (E.D.N.Y 2005) District Court, E.D. New York.
19. Bundeskartellamt Decision (B6-22/16), 6 February 2019 Available on: https://www.bundeskartellamt.de/SharedDocs/Entscheidung/EN/Entscheidungen/Missbrauchsaufsicht/2019/B6-22-16.html accessed 10.06.2020.
20. The Court of Justice of the European Union: Opinion of Advocate General of 19 December 2018, *Fashion ID GmbH & Co. KG* , C-40/17, EU:C:2018:1039.

1.10 Secondary sources

1.10.1 Journal Articles

21. Blume Peter "Data protection in the private sector" *Scandinavian studies in Law* (2004), vol.47, pp. 297-318.
22. Child Jeffrey T., Starcher Shawn C. "Fuzzy Facebook privacy boundaries: Exploring mediated lurking, vague-booking, and Facebook privacy management" *Computer in Human Behavior* (2016) 54, pp.483-490.
23. Ciocchetti Corey A. "E-Commerce and Information Privacy: The privacy policies as Personal Information Protectors" *American Business Law Journal* 44 (2007):pp.55-126.

24. Debatin Bernhard, Lovejoy Jennette P., "Facebook and Online Privacy: Attitudes, Behaviors, and Unintended Consequences", *Journal of Computer-Mediated Communication 15 (2009): pp.83-108.*
25. Efroni Zohar "Gaps and opportunities: the rudimentary protection for "data-paying consumers" under new EU consumer protection law" *Common Market Law Review* 57 (2020):pp. 799-830.
26. Ezrachi Ariel, Robertson Viktoria H.S.E, "Competition, Market Power and Third-Party Tracking", *World Competition* 42 (2019): pp.5-19.
27. Grannis Amanda "You didn't even notice: elements of effective online the privacy policies [notes]." *Fordham Urban Law Journal*, (2015), vol. 42, issue 5, pp. 1109-1170.
28. Gulik Stephanie, Hulstijn Joris " Ensuring Data Protection by Private Law Contract Monitoring: A Legal and Value-Based Approach" *European Review of Private Law* (2018), 5, pp.635-660.
29. Happ Chistian, Melzer Andre, Steffgen Georges "Trick with treat – Reciprocity increases the willingness to communicate personal data" *Computer in Human Behavior, (2016),* vol.61, pp. 372-377.
30. Haynes Allyson, "Online the privacy policies: Contracting away control over personal information?", *Penn State Law Review*, 111 (2007): pp. 587-624.
31. Helberger Natalie, Borgesius Frederik Z., Reyna Augustin "The perfect match? A closer look at the relationship between EU consumer law and data protection law" *Common market Law Review* 54 (2017): 1427-1466.
32. Hoofnagle Chris "Designing for consent" *Journal of European Consumer and Market Law* 7 (2018):pp.162-171.
33. Kosta Eleni, "Construing the Meaning of "Opt-Out" - An Analysis of the European, U.K. and German Data Protection Legislation", *European Data protection Law Review* 1 (2015): pp. 16-31
34. Langhanke Carmen, Schmidt-Kessel Martin "Consumer Data as Consideration" *Journal of European Consumer and Market Law* 4 (2015): pp. 218-223
35. Lynskey, Orla, "Grappling with "Data Power": Normative Nudges from Data Protection and Privacy" *Theoretical inquiries in Law* 20 (2019): pp.189-220.
36. Leiser Mark, Murray Andrew. "The role of non-state actors and institutions in the governance of new and emerging digital technologies." *The Oxford Handbook of Law, Regulation and Technology (2016):* pp. 670-701.
37. Loos Marco "Standard terms for the use of the Apple App Store and the Google Play Store" *Journal of European Consumer and Market Law* 5 (2016): pp.10-15.
38. McDonald Aleecia, Cranor Lorrie "The cost of reading the privacy policies*" I/S: A Journal of Law and Policy for the Information Society* 4 (2008): pp.543-568.
39. Marotta-Wurgler Florencia "Self-regulation and competition in The privacy policies." *Journal of Legal studies* 45 (2016): pp. 13-40.
40. Killingsworth Scott "Minding your own business: The privacy policies in principle and in practice" *Journal of Intellectual Property Law*, 7 (1999): pp. 57-97.
41. Pasquale Frank "Privacy, antitrust, and power" *Geo. Mason L.Rev*. 20 (2013) pp.1009-1024.
42. Pormeister Kart "Informed consent to sensitive personal data processing for the performance of digital consumer contracts on the example of "23andMe" *Journal of European consumer and Market Law* 6 (2017): pp.17-23.
43. Przepiorka Aneta, Blachnio Agata "Time perspective in Internet and Facebook addiction" *Computers in Human Behavior* 60 (2016): pp.13-18.
44. Robertson Viktoria "Excessive data collection: Privacy considerations and abuse of dominance in the era of big data" *Common Market Law Review* 57 (2020): pp. 161-190.
45. J. Senechal "The Diversity of the Services provided by Online Platforms and the Specificity of the Counter-performance of these Services — A double Challenge for European and National Contract Law" *Journal of European Consumer and Market Law* 5 (2016): pp.39-44.
46. Solove Daniel, Hartzog Woodrow "The FTC and the new common law of privacy" *Colombia law review* 114:583 (2014): pp. 585-676.
47. Solove Daniel "Privacy self-management and the consent dilemma" *Harvard Law Review* 126 (2013): pp.1880-1903.
48. Solove Daniel "I've got nothing to hide and other misunderstandings of privacy" *San Diego Law Review* (2007) pp. 745-772.

1.10.2 Books

49. Kosta, Eleni. *Consent in European Data Protection Law.* Leiden: Martinus Nijhoff Publishers, 2013.
50. Lessig, Lawrence. *Code Ver 2.0.* New York: Basic books, 2006.
51. Lynskey, Orla. *The Foundations of EU Data Protection Law* Oxford: Oxford University Press, 2015.
52. Moore Martin, Tambini Damian, "*Digital Dominance: the Power of Google, Amazon, Facebook and Apple"* Oxford: Oxford University Press, 2018.
53. Solove, Daniel J. Digital person: Technology and Privacy in the Information Age New York: New York university press, 2004.

1.10.3 Working papers, reports, official papers

54. The European Data Protection Board. Guidelines 05/2020 on consent under Regulation 2016/679 of, paragraph 67. Available on: https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_en accessed 06.06.2020.
55. Article 29 Working Party Guidelines on Transparency under Regulation 2016/679 as of 29 November 2017. Available on: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051 accessed June 06, 2020.
56. Article 29 Working Party Guidelines on Consent under Regulation 2016/679. Available on: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051 accessed June 06, 2020.
57. Article 29 Working Party Opinion on Purpose limitation 3/2013 Available on: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm#maincontentSec5 accessed June 06, 2020.
58. The European Consumer Organization. Study report. "CLAUDETTE meets GDPR". Available on: http://www.beuc.eu/search?keys=claudette&field_reference_value=&field_creation_date_value%5Bmin%5D%5Bdate%5D=&field_creation_date_value%5Bmax%5D%5Bdate%5D= accessed June 06, 2020.
59. European commission. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - Online Platforms and the Digital Single Market Opportunities and Challenges for Europe (COM(2016)288) Available on: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52016DC0288 accessed 01.06.2020.
60. European commission. Communication on data-driven economy. Available on: https://ec.europa.eu/digital-single-market/en/news/communication-data-driven-economy accessed 01.06.2020.
61. Lynskey Orla, "Regulating "Platform power" LSE Law, Society and Economy Working Papers 1/2017 p.13 Available on: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2921021 accessed 09 June, 2020.
62. C. Jensen, C. Potts "The privacy policies as Decision-Making Tools: An Evaluation of Online Privacy Notices." CHI '04: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, April 2004, p. 471-478.

1.10.4 Online magazines

63. MIT Technology review. Available on: https://www.technologyreview.com/2020/05/07/1000961/launching-mittr-covid-tracing-tracker/ accessed May 25, 2020.
64. The Telegraph. Available on: https://www.telegraph.co.uk/news/science/science-news/12108412/Facebook-users-have-155-friends-but-would-trust-just-four-in-a-crisis.html Accessed 27.05.2020.

1.10.5 Data sources

65. EU Open Data Portal. Special Eurobarometer 359: Attitudes on Data Protection and Electronic Identity in the European Union. p.23. Available on: https://data.europa.eu/euodp/en/data/dataset/S864_74_3_EBS359 accessed June 01, 2020.
66. EU Open Data Portal. Special Eurobarometer 487a: The General Data Protection Regulation. Available on: https://ec.europa.eu/info/law/law-topic/data-protection/eu-data-protection-rules_en Accessed June 06, 2020.
67. Amnesty international. Available on: https://www.amnesty.org/en/latest/news/2019/12/big-tech-privacy-poll-shows-people-worried/ Accessed May 19, 2020.
68. Harvard center for Ethics. White paper 5. Available on: "Outpacing the Virus: Digital Response to Containing the Spread of COVID-19 while Mitigating Privacy Risks" https://ethics.harvard.edu/outpacing-virus Accessed May 25, 2020.
69. Federal Trade Commission Privacy Online: Fair Information Practices in the Electronic Marketplace: A Federal Trade Commission Report to Congress. Available on https://www.ftc.gov/reports/privacy-online-fair-information-practices-electronic-marketplace-federal-trade-commission Accessed May 25, 2020.
70. Data protection and online privacy. Available on: https://europa.eu/youreurope/citizens/consumers/internet-telecoms/data-protection-online-privacy/index_en.htm Accessed May 25, 2020.
71. Google the privacy policy. Available on: https://policies.google.com/privacy?fg=1 Accessed 27.05.2020.
72. Facebook Investor Relations. Available on: https://investor.fb.com/investor-news/press-release-details/2020/Facebook-Reports-First-Quarter-2020-Results/default.aspx Accessed 27.05.2020.
73. Facebook data policy. Available on: https://www.facebook.com/privacy/explanation/ Accessed 27.05.2020.
74. Alphabet Inc. Annual Report. Available on: https://abc.xyz/investor/static/pdf/20200204_alphabet_10K.pdf?cache=cdd6dbf Accessed 29.05.2020.
75. Microsoft privacy statement. Available on: https://privacy.microsoft.com/en-gb/privacystatement Accessed 29.05.2020.
76. Microsoft Annual Report 2019. Available on: https://www.microsoft.com/investor/reports/ar19/index.html Accessed 29.05.2020.
77. Apple The privacy policy. Available on https://www.apple.com/legal/privacy/en-ww/ Accessed 29.05.2020.
78. Apple Investor Relations. Available on: https://www.apple.com/newsroom/2020/04/apple-reports-second-quarter-results/ accessed May 30, 2020.
79. Facebook. Terms of service. Available on: https://www.facebook.com/legal/terms accessed June 01, 2020.
80. Linkedin. Available on: https://www.linkedin.com/ accessed June 02, 2020.

81. Linkedin. The privacy policy. Available on: https://www.linkedin.com/legal/privacy-policy?trk=homepage-basic_footer-privacy-policy accessed June 02, 2020.