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

Sara Rasilainen

VALID CONSENT AND PURPOSE LIMITATION PRINCIPLE UNDER THE EU GENERAL DATA PROTECTION REGULATION

Bachelor's thesis

Programme HAJB, specialization European Union and International law

Supervisor: Associate Prof. Dr. Tatjana Evas

Tallinn 2020

I declare that I have compiled the paper independently
and all works, important standpoints and data by other authors
have been properly referenced and the same paper
has not been previously been presented for grading.
The document length is 11750 words from the introduction to the end of conclusion.

Sara Rasilainen ……
Student code: 177723HAJB
Student e-mail address: sarasi@taltech.ee

Supervisor: Dr. Tatjana Evas
The paper conforms to requirements in force

……

Chairman of the Defence Committee:
Permitted to the defence
……

TABLE OF CONTENTS

ABSTRACT

The thesis analyzes whether the current practices of collection and use of personal data by online platforms violate the consent requirement and the purpose limitation principle as stated in the European Union (EU) General Data Protection Regulation (GDPR). The business models of most online platforms are based on collecting and using vast amounts of personal data. The GDPR sets the consent of a data subject as one of the legal bases to the processing of personal data in Article 6(a). Specifically, to protect and limit the use of collected personal data, Article 5(b) of the GDPR includes the purpose limitation principle.

This research work provides an analysis of conditions for valid consent and conditions related to the purpose limitation principle stated in EU law and developed through European Court of Justice (CJEU) case law. The research employed a qualitative research method.

The hypothesis is that online platforms' practice of collecting and using personal data, violates Articles 5(b) and 6(a) of the GDPR. Based on the legal analysis of EU legislation, CJEU case law, Article 29 Working Party guidelines and secondary literature, this thesis argues that acquiring valid consent and complying with the purpose limitation principle in a way that people's right to self-determination is protected, is not effectively realized in the field of online platforms. Consequently Articles 5(b) and 6(a) of the GDPR should be revised.

Keywords: EU General Data Protection Regulation, consent, purpose limitation principle, rights of data subject

LIST OF ABBREVIATIONS

CJEU	European Court of Justice
Data Protection Directive	Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals regard to the processing of personal data and on the free movement of such data
ECHR	European Convention on Human rights
ePrivacy Directive	Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector
ePrivacy Regulation	Proposal for a regulation of the European Parliament and of the Council concerning the respect for private life and protection of personal data in electronic communications and repealing Directive 2002/58/EC
GDPR	Regulation (EU) 2016/679 of the European Parliament and of the Council 27 April 2016 on the Protection of natural persons with regard to the processing of personal data on the free movement of such data (General Data Protection Regulation) OJ L 119, 4.5.2016
The Charter	Charter of Fundamental Rights of the European Union

INTRODUCTION

The protection of individuals with regard to the processing of personal data is a fundamental right in the European Union (EU).[1] The protection of personal data has become more difficult due to constantly evolving technology and globalization. The amount of personal data collected and shared through online means has increased remarkably in recent years.[2] In response, the EU has reviewed and strengthened its data protection framework.[3] The EU General Data Protection Regulation (GDPR) that came into force in May 2018[4] increases the protection of privacy by further harmonizing data protection rules among EU member states.[5] The central elements the GDPR has strengthened are conditions for the consent of a data subject[6] and principles listed in Article 5, including the purpose limitation principle.[7]

The competitive value of many online platform businesses is based on the amount and quality of the data the business possesses.[8] The strategies of online platforms typically include gathering and using vast amounts of user data.[9] The term "big data" occurs repeatedly in connection with online platforms. Big data principally refers to a large volume of data produced at high speed from many sources.[10] The gathering of data includes so many different and unforeseen sources that user

1 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, (General Data Protection Regulation), OJ L 119, 4.5.2016, (GDPR), recital 1.
2 *Ibid*., recital 6
3 *Ibid*., recital 7
4 The 2018 GDPR revoked the previous data protection directive 95/46/EC, Zarsky, T. Z. (2016). Incompatible: the GDPR in the age of big data. -*Seton Hall L. Rev*., 47, p. 995-1020, p 995.
5 Voigt, P., & Bussche, A. (2017). *The EU general data protection regulation (GDPR): a practical guide*. Cham, Switzerland: Springer, p 1.
6 Article 4(11) of the GDPR, recitals 7 and 32 of the GDPR, for further analysis see e.g. Voigt, P., & Bussche, A. (2017). *supra nota* 5, p 93.
7 Article 5(b) of the GDPR. The purpose limitation principle states that personal data shall be "collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes." Other principles listed in Article 5 are lawfulness, fairness and transparency, data minimization, accuracy, storage limitation, integrity and confidentiality, Ustaran, E. (Ed.). (2018). *European Data Protection: Law and Practice*. United States: An IAPP Publication, International Association of Privacy Professionals. p 99.
8 Graef, I. (2015). Market definition and market power in data: The cases of online platforms." – *World Competition*, Vol 38, Issue 4, p 473.
9 Moore, M., & Tambini, D. (Eds.). (2018). *Digital dominance: the power of Google, Amazon, Facebook, and Apple.* New York, NY: Oxford University Press. p 22.
10 Communication from the Commission- Towards a thriving data-driven economy. COM (2014)442 final, p 4. Accessible: https://ec.europa.eu/digital-single-market/en/news/communication-data-driven-economy, 28.3.2020.

control of data can easily be lost. In many cases, the user is not aware of the processing or cannot keep track of how the data flows from one system to another.[11]

Before collection, data subject must give free, specific informed and unambiguous consent for the processing of personal data.[12] To comply with the purpose limitation principle, the data processor must inform the user about the purpose of collecting data and must adhere to this purpose during processing.[13] However, the foundations of big data operations are based on gathering data from different sources, in different contexts and for different purposes.[14] Often, the uses for collected data are determined later when considering further cases in which the data could be utilized.[15] In contrast to such big data operations, the GDPR requires that data subjects' "consent should cover all processing activities carried out for the same purpose or purposes. When processing has multiple purposes, consent should be given for all of them."[16] The purpose limitation principle additionally requires that the objectives for use of data are defined in advance.[17]

The thesis analyzes whether the collection and use of personal data by online platforms violate concept of consent and the purpose limitation principle under the GDPR. To answer this key research question, the thesis focuses on two specific questions: (a) How can data subjects give informed, specific, free and unambiguous consent within the meaning of the GDPR, if they do not know the exact purposes of and means of processing personal data? (b) Do big data collection operations conflict with the purpose limitation principle when the uses of data are determined after data collection and when the data subject is unaware of the sources from which data is collected?

To answer those questions, the thesis examines consent and the purpose limitation principle in the context of the operations used by online platforms and analyzes resulting legal issues. Specifically, the thesis focuses on the analysis of elements and principles considered in the European Court of Justice (CJEU) jurisprudence in determining whether an online platform provider violated its data

[11] ENISA (2015) The European Union Agency for Network and Information Security (ENISA), Privacy by design in big data – An overview of privacy enhancing technologies in the era of big data analytics, 2015, p 13. Accessible: https://www.enisa.europa.eu/publications/big-data-protection , 28.3.2020.
[12] Recital 32 of the GDPR
[13] Hoeren, T., Kolany-Raiser, B., & Bittner, L. (2018). *Big data in context: legal, social and technological insights*. Cham, Switzerland: Springer Open. p 32.
[14] *Ibid*., p 32.
[15] *Ibid*., p 32.
[16] GDPR recital 32, for further analysis see e.g. Basin, D., Debois, S., & Hildebrandt, T. (2018). On purpose and by Necessity: Compliance Under the GDPR. *Lecture Notes in Computer Science*, 10957, p 22.
[17] Team, I.P. (2017). *EU General Data Protection Regulation (GDPR): An implementation and Compliance Guide*. Second edition, United Kingdom: IT Governance Publishing. p 108.

protection obligations. The thesis follows the qualitative research method. Opinions and guidelines of the Article 29 Working Party are used to clarify the meaning and scope of consent and the purpose limitation principle. The thesis also reviews literature produced by legal scholars who have analyzed the relevant legal problems.

The main hypothesis of the thesis is that online platforms' practice of collecting data by using complex privacy policies, by employing "take-it-or-leave-it" methods and by gathering data from unexpected sources violates the consent requirement and the purpose limitation principle. Data works as a vital asset for those businesses and the fundamental right to protection of personal data can be seen as threatened. The legal question addressed by this thesis is topical and important because of the highly increased amount of the personal data collected and the need to protect the fundamental right to privacy.

The thesis consists of three parts. Chapter 1 analyzes how EU law protects the individual's right to protection of personal data. The EU legal instruments regarding protection of personal data and their main aims are introduced, and the purpose and scope of central EU legislation regarding protection of personal data are analyzed. Chapter 2 reviews elements of consent and the purpose limitation principle in detail. Chapter 2 also discusses what principles and conditions are considered in CJEU jurisprudence in determining whether an online platform has violated its obligations under Articles 5(b) and 6(a) of the GDPR. Furthermore, Chapter 2 addresses pertinent legal issues that have emerged in the jurisprudence of the CJEU. Chapter 3 reviews the different operations of online platforms and argues how those operations conflict with rights provided in the GDPR Articles 5(b) and 6(a). The thesis ends with a conclusion.

1. GENERAL LEGAL FRAMEWORK ON DATA PROTECTION IN THE EUROPEAN UNION

Data protection laws aim to facilitate the free flow of information while safeguarding personal data.[18] The term "data protection" emerged as an outcome of the development and use of computers.[19] Data protection refers to the provisions meant to regulate collection, retention, use and transfer of personal data.[20] The central question of this thesis is whether collection and use of personal data from individuals for the purposes of big data analytics by online platforms violates the concept of consent and the purpose limitation principle under the GDPR. To answer this key research question, Chapter 1 introduces the main definitions, concepts and principles of the EU data protection law. Chapter 1 also explains what operations fall within the scope of the GDPR and in which situations the online platforms must comply with the GDPR.

In order to discuss and highlight the relevance of the topic and the legal challenges it entails, analyses of the key definitions, concepts and principles, are based on the hypothetical example of a common situation that many natural persons face daily. Consider the following: An individual, a natural person, wants to create a user account on Platform A, where the user can, *inter alia*, share thoughts and pictures. In order to create the account, this individual is asked to agree to the general terms and conditions used by the Platform A and to provide their name, surname and e-mail address. While surfing on Platform A, the individual is asked to accept to the collection of cookies. The individual's personal data later is sold to a third party that intends to use the data for targeted advertising. The following sections are based on the hypothetical case analysis. First, the thesis analyzes what legal rules relating to protection of personal data apply to this hypothetical case. Section 1.1 focuses on data protection as fundamental right under EU law; sections 1.2 and 1.3 analyze how the rights of a data subject are currently protected in EU legislation.

[18] Gutwirth, S., R., & de Hert, P. (2015). *Reforming European Data Protection Law*. Vol 20. Netherlands: Dordrecht Springer. p 16.
[19] Bennett, C. J. (1992). *Regulating privacy: Data Protection and public policy in Europe and the United States*. New York: Cornell University Press. p 2.
[20] *Ibid*., p 13.

1.1 Data Protection as Fundamental Right in the European Union

EU primary law, Article 7 of the Charter of Fundamental Rights of the EU (the Charter) and Article 8 of the European Convention on Human Rights (ECHR) [21] guarantee the individual the right to a private life. Furthermore, Article 8 of the Charter differentiates the right to data protection as a right independent from the right to privacy.[22] Article 8 of the Charter guarantees everyone the right to the protection of personal data by stating that "processing of such data must be done fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law." Article 8 also grants the individual the right to data collected concerning them and the right to have it rectified.

The CJEU has interpreted the elements and meaning of Articles 7 and 8 of the Charter in a number of cases. The importance of these Articles can be seen when considering ruling of the CJEU in the joined cases *C-293/12 and C-594-12 Digital Rights Ireland*.[23] In the joined cases the CJEU declared secondary law invalid on the basis that it exceeded the limits imposed by the principle of proportionality in the light of Articles 7 and 8.[24] In the case C-131/12 *Google Spain*, the CJEU confirmed that the economic interests of the operator of a search engine cannot supersede the fundamental rights provided in Articles 7 and 8 of the Charter.[25]

In practical terms, analysis confirms that in the hypothetical case analyzed in this thesis, an individual who created a user account on Platform A is a data subject and has the fundamental right to data protection under EU primary law and public international law.

[21] Council of Europe, 1950, European Convention on Human Rights.
[22] Lynskey, O. (2014). Deconstructing data protection: the added value of a right to data protection in the EU legal order. – *International & Comparative Law Quarterly*, Vol 63 Issue 3, p 569.
[23] Court decision, 8.4.2014, *Digital Rights Ireland Ltd,* joined cases *C*-293/12 and C-594-12, EU:C:2014:238.
[24] *Ibid.,* paragraph 69. The Court stated that "Directive 2006/24 entails a wide-ranging and particularly serious interference with fundamental rights enshrined in Articles 7 and 8 of the charter." Furthermore the Court noted that "the Directive 2006/24 does not provide for sufficient safeguard, as required by the Article 8 of the Charter, to ensure effective protection of the data retained against the risk of abuse and against any unlawful access and use of that data comprise the essence of the right to privacy or data protection, the interference did not meet the principles of proportionality and necessity."
[25] Court decision, 13.5.2014, *Google Spain* SL and Google Inc. V Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, C-131/12, EU:C:2014:317, paragraph 99. The Court stated that: "The data subject may, under Articles 7 and 8 of the Charter, request that the information in question no longer be made available to the general public on account of its inclusion in such a list of results, those rights override, as a rule, not only the economic interest of the operator of search engine but also the interest of the general public in having access to that information upon a search relating to the data subject's name."

1.2 The European Union General Data Protection Regulation

In addition to the protection provided by EU primary law and public international law, as discussed in Section 1.1. above, an individual also benefits from the safeguards of the EU secondary law. This section specifically outlines the applicable data protection law which has been recently renewed.

1.2.1 Background

The individual's fundamental right to data protection is further specified in the EU secondary law. The first EU legal instrument specifically intended to strengthen the protection of personal data was the Data Protection Directive (Directive 95/46/EC).[26] Directive 95/46/EC built an important foundation for the protection of personal data in the EU but was not sufficient.[27] As a result, to address the shortcomings of the 1995 directive, the GDPR was adopted, and it came into force in May 2018.[28] The purpose of the GDPR is to protect the rights, privacy and freedoms of natural persons in the EU and to reduce barriers to business by facilitating the free movement of personal data throughout the EU.[29] As detailed later in this chapter, the GDPR provides a number of rights to individuals regarding their personal data.[30] To ensure the protection of these rights, the GDPR imposes a number of obligations on the organizations and companies that collect, store and process personal data. [31]

Although the "information society" is not a completely new concept, the true value of personal data has only recently become evident.[32] The continuing advance of technology and the big data operations used by online platforms provide opportunities to track and forecast users' behavior.[33]

[26] Already before GDPR there was a legal framework related to protection of personal data applicable to the EU Member States. On the international level, in 1981 Council of Europe adopted Convention 108 which was the first binding international instrument setting rules to the protection of individuals personal data. In the EU, in 1995 to answer the increased processing of personal information the Data Protection Directive (Directive 95/46/EC) was adopted. However, the lack of uniformity and novel more detailed ways of gathering and analyzing personal data lead to the decision to replace Data Protection Directive with Regulation. For further analysis see Ustaran, E. (Ed.). (2018). *supra nota* 7, p 10 and Kirsch, M. S. (2011). Do-not-track: Revising the EU's data protection framework to require meaningful consent for behavioral advertising. – *Richmond Journal of Law & Technology*, Vol 18 Issue 1, p 17.
[27] Tikkinen-Piri, C. *et al*. (2018). EU General Data Protection Regulation: Changes and implications for personal data collecting companies. – *Computer Law & Security Review*, Vol 34 Issue 1, p 137.
[28] *Ibid*., p 137.
[29] Team, I.P. (2017). *supra nota* 17. p 12.
[30] *Ibid*., p 14. For the further discussion of the rights in more detail see Section 1.2.2 below.
[31] *Ibid*., p 14.
[32] *Ibid.*, p 11.
[33] *Ibid*., p 11.

Consequently, concerns regarding cyber theft and misuse of personal data have grown.[34] The GDPR aims to address these problems by further harmonizing data protection rules and advancing the privacy levels of individuals affected.[35] Compared to Directive 95/46/EC, the GDPR is binding in its entirety and directly applicable in the member states.[36]

1.2.2 Purpose and scope of the European Union General Data Protection Regulation

Article 2 of the GDPR defines its material scope. In the above-mentioned hypothetical case, the GDPR becomes applicable because, as stated in Article 2, it applies to any processing of personal data. "Personal data" is defined in the GDPR as "any information relating to an identified or identifiable natural person ('data subject')."[37] Any information, in any format, that could identify the data subject can constitute a personal data.[38] Because an individual provides their name, surname and email address to Platform A, they are issuing personal data. Platform A then "processes" this personal data by means of an operation or set of operations, whether automated or not.[39] Virtually any treatment of personal data, such as collecting, recording, organizing, structuring or storing, can be considered processing. When Platform A collects the name, surname and address of an individual, it already is conducting a processing operation.

The GDPR applies to all who process or control the processing of personal data.[40] The controller refers to the organization that defines the purposes and means of processing personal data.[41] In the hypothetical case, Platform A is the controller of the data. "Controller" is defined as "the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data."[42] In above mentioned case C-131/12 *Google Spain*, the CJEU was referred the question of "whether the operator of a search engine must be regarded as 'controller' in respect of the processing of that personal data?"[43] In

[34] *Ibid*., p 11.
[35] Voigt, P., & Bussche, A. (2017). *supra nota* 5, p 1.
[36] Barnard, C., & Peers, S. (Eds.). (2014). *European Union Law*. Oxford: Oxford University Press. p 99.
[37] Article 4 of the GDPR. "An identifiable natural person is one who can be identified, directly or indirectly particular by reference to an identifier such as 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"
[38] Calder, A. (2018). *EU GDPR: A Pocket Guide*, School's Edition: Vol. School's edition. United Kingdom: IT Governance Publishing Ltd. p 18.
[39] Voigt, P., & Bussche, A. (2017). *supra nota* 5, p 10.
[40] *Ibid*., p 10.
[41] *Ibid*., p 19.
[42] Article 4 of the GDPR.
[43] Court decision, 13.5.2014, *Google Spain* SL and Google Inc. V Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, EU:C:2014:317, paragraph 21.

this case, the CJEU stated that because the search engine operator chooses the objectives and means of that activity and thus of the processing of personal data that it itself carries out within the framework of the activity, it is a controller regarding of that processing.[44]

In the hypothetical case analyzed here, the rules of the GDPR apply regardless of where Platform A performs the actual data processing if the platform is based in the EU.[45] Furthermore, even if Platform A is a non-EU organization, it must comply with the GDPR if it provides services in the EU and those services involve the processing of personal data.[46] To conclude, when an online platform determines the purposes and means of the processing of personal data and carries out that operation, it can be regarded as a controller in terms of the GDPR. Moreover, even if the online platform is located outside the EU, it must comply with the GDPR when it processes the personal data of users located in the EU. Accordingly, the individual in the hypothetical case, provided they are located in the EU, can benefit from other rights guaranteed in secondary EU legislation in addition to the rights provided by EU primary law.

1.3 ePrivacy Directive and Proposed ePrivacy Regulation

In addition to the GDPR, which applies generally to the processing of personal data, Directive 2002/58/EC (ePrivacy Directive) further "particularizes and complements" the provisions of the GDPR regarding processing of personal data in the electronic communication sector.[47] The ePrivacy Directive was adopted in 2002 to complement the Directive 95/46/EC.[48] The ePrivacy Directive aims to ensure the protection of rights provided in Articles 7 and 8 of the Charter when the public makes use of electronic communication networks.[49] To address the changing landscape of the Internet, the ePrivacy Directive was amended in 2009.[50] The amended Directive obliges companies to ask prior consent, before they use tracking cookies and similar technologies.[51]

[44] *Ibid.*, paragraph 33.
[45] The European Commission (2019). p 5, Accessible: https://ec.europa.eu/info/sites/info/files/data-protection-factsheet-sme-obligations_en.pdf, 28.3.2020.
[46] Team, I.P. (2017). *supra nota* 17, p 16.
[47] European Data Protection Board (2019). Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities. p 8, Accessible: https://edpb.europa.eu/sites/edpb/files/files/file1/201905_edpb_opinion_eprivacydir_gdpr_interplay_en_0.pdf, 26.3.2020.
[48] Kirsch, M. S. (2011). *supra nota* 26, p 6.
[49] European Data Protection Board (2019). *supra nota* 47 p 11.
[50] Kirsch, M. S. (2011). *supra nota* 26, p 6.
[51] Zuiderveen Borgesius, F. J. *et al*. (2017). Tracking walls, take-it-or-leave-it-choices, the GDPR, and the ePrivacy regulation. – *Eur. Data Prot. L. Rev*., 3, p 359.

Article 5(3) of the ePrivacy Directive states that storing of information or gaining access to information stored in the equipment of user is only allowed when clear and comprehensive information about purposes of processing is offered and user has right to refuse such processing.[52]

The GDPR influences the interpretation of the ePrivacy Directive because the directive refers to the GDPR definition of consent.[53] Furthermore, CJEU case law states that processing can fall within the material scope of both the ePrivacy Directive and the GDPR.[54] In the case C-40/17 *Fashion ID*, the CJEU applied both the Directive 95/46/EC and the ePrivacy Directive, whereas in case C-673/17 *Planet49*, the CJEU referred to the GDPR and the ePrivacy Directive. These cases are further analyzed in the next chapter.

Recital 173 of the GDPR states that "once this Regulation on is adopted, Directive 2002/58/EC should be reviewed in particular in order to ensure consistency with this Regulation."[55] The European Commission published a proposal on January 10, 2017 for an ePrivacy Regulation to replace the ePrivacy Directive.[56] As with the ePrivacy Directive, the regulation proposal governs cookies and online tracking.[57] The purpose of the proposed ePrivacy Regulation is to further harmonize privacy legislation relating to electronic communications in the EU and to guarantee conformity with the GDPR.[58] In the hypothetical case, Platform A should abide by, in addition to the GDPR, ePrivacy Directive Article 5(3) because it requires companies to request an Internet user's prior consent before they use tracking cookies and similar technologies.[59]

Based on the analysis in this Chapter, the individual in the hypothetical case is protected under EU primary law, public international law and EU secondary law. The GDPR sets the general data protection rules on the Platform A when it collects and processes personal data, while ePrivacy

[52] Article 5(3) of the ePrivacy Directive.
[53] Ustaran, E. (Ed.). (2018). *supra nota* 7, p 95.
[54] European Data Protection Board (2019), *supra nota* 47, p 11.
[55] Recital 173 of the GDPR, for further analysis see Ustaran, E. (Ed.). (2018). *supra nota* 7, p 95.
[56] Proposal for a regulation of the European parliament and of the council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)
[57] Zuiderveen Borgesius, F. J. *et al*. (2017). *supra nota* 51, p 361. The proposed Article 8(1) states: "The use of processing and storage capabilities of terminal equipment and the collection of information from end-users 'terminal equipment, including about its software and hardware, other than by the end-user concerned shall be prohibited, except on the following grounds: b.) the end-user has given his or her consent."[57]
[58] Ustaran, E. (Ed.). (2018). *supra nota* 7, p 57.
[59] Zuiderveen Borgesius, F. J. *et al*. (2017). *supra nota* 51, p 359.

Directive specifically defines rules relating to cookies and online tracking. Chapter 2 analyses further the central principles that follow from the EU law and aim to protect rights of data subject.

2. CONSENT AND THE PURPOSE LIMITATION PRINCIPLE

Following the discussion of the background underlying the EU's legal framework, Chapter 2 focuses specifically on two central elements of the EU data protection: the concept of consent and the principle of purpose limitation, provided in Articles 6(a) and 5(b) of the GDPR. These two concepts are interrelated and central to understanding the collection and use of data by platforms.

This chapter therefore analyzes following questions: first, whether in the hypothetical case, an individual's consent to the processing of the personal data on Platform A constitutes a valid 'consent' within the meaning of the EU law and, second, whether this consent can be extended to the use of personal data by a third party or whether this consent should be limited to a specific purpose of use by Platform A. To answer those questions, section 2.1 first discusses the definition of the consent, including elements and conditions under which the CJEU finds consent valid. Section 2.2 then analyzes the elements of purpose limitation in detail and examines what must be considered to comply with the principle.

2.1 Elements of the Concept of Consent

An online platform can process personal data only on lawful grounds.[60] Consent, according to Article 6 of the GDPR, is one of six lawful grounds for processing personal data.[61] Article 6(1)(a) of the GDPR gives data subjects an explicit right to decide if they permit processing of personal data and to what extent.[62] When a controller - Platform A, in the hypothetical case - begins activities that involve the processing of personal data, it must consider lawful grounds for the

[60] Zuiderveen Borgesius, F. J. *et al.* (2017). *supra nota* 51, p 359. Informed consent and individual choice have a central role in European data privacy law.
[61] Kirsch, M. S. (2011). *supra nota* 26, p 18.
Inconsistencies between Member State's legislations regarding informed and free consent was especially an area of concern when the GDPR was drafted. Compared to its predecessor Directive 95/46/EC and e-Privacy Directive GDPR clarifies the requirements for obtaining and demonstrating valid consent.
[62] Botta, M., & Wiedemann, K. (2019). The interaction of EU competition, consumer, and data protection law in the digital economy: the regulatory dilemma in the Facebook odyssey. – *The Antitrust bulletin*, Vol 64, Issue 3, p 431.

process.[63] Processing of personal data is allowed only for the specific and defined purpose for which the data subject has given consent.[64]

According to Article 4(11) of the GDPR, four elements of valid consent must be fulfilled. The consent must be freely given, specific, informed and unambiguous.[65] Although Article 4(11) of the GDPR defines consent, it does not disclose in detail what freely given, specific, informed or unambiguous consent means.[66] Each element of valid consent, as interpreted by the CJEU and the Article 29 Working Party, is analyzed below.

2.1.1 Freely given

The first element of the valid consent is "freely given". To be regarded as free consent, the data subject must be offered real freedom of choice and must be able to withdraw consent at any time.[67] In the above-mentioned example case, Platform A should provide real freedom of choice for the individual on whether to create an account and on whether to provide personal data to Platform A. There should be no risk of coercion, intimidation, deception or any other prominent negative consequences if the data subject refuses to consent.[68] Freely given consent emphasizes that data subjects have the right to self-determination regarding personal data.[69] If the terms and conditions are non-negotiable or if the data subject is not able to withdraw consent without disadvantages, consent is not regarded as freely given.[70] Furthermore, in cases where there is a clear imbalance between the data subject and the controller, the consent should not be relied on.[71] The clear

[63] Article 29 Working Party, Guidelines on Consent under Regulation 2016/679, (2017), p. 4 Accessible: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051, 20.2.2020
[64] Hameurlain, A., & Wagner, R. (2018). *Transactions on Large-Scale Data- and Knowledge- Centered Systems.* Berlin, Heidelberg: Springer eBooks., 6th Ed. p 43.
[65] Article 4(11) of the GDPR. "Consent of the data subject means any freely given, specific, informed and unambiguous indication of the data subjects wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her."
[66] Interpretation help can be sought from the recitals of GDPR, case law of the CJEU and the Article 29 Working Party's guidelines on consent. The Article 29 Working Party was established under Article 29 of Directive 95/46/EC and it acted as an independent European advisory body on data protection and privacy. On May 25, 2018 the Article 29 Working party was replaced by the European Data Protection Board (EDPB). However, the guidelines given by Working party regarding consent remain relevant. The guidelines of Article 29 Working party provide a thorough analysis of the notion of consent under GDPR. The guidelines are non-binding, soft law instruments which aim at harmonization in a non-coercive way. Article 29 Working Party, Guidelines on Consent under Regulation 2016/679, (2017), *supra nota* 63, p 3. For further analysis see. Hijmans, H. (2016). *The European Union as guardian of internet privacy: The Story of Art 16 TFEU*. Switzerland: Springer. p 399.
[67] Ustaran, E. (Ed.). (2018). *supra nota* 7, p 114.
[68] Article 29 Working Party, Guidelines on Consent under Regulation 2016/679, (2017), *supra nota* 63, p 7.
[69] Kosta, E. (2013). *Consent in European Data Protection Law*. Leiden: BRILL. p 386.
[70] Article 29 Working Party, Guidelines on Consent under Regulation 2016/679, (2017), *supra nota* 63., p 5.
[71] Recital 43 of the GDPR

imbalance of power often occurs when the controller is a public authority.[72] Moreover, the relationships in the working environment between employee and employer constitute an imbalance in which consent is usually not deemed valid.[73] However, there are exceptions if the consent is actually free and there occurs no disadvantages for employees, regardless of whether they consent.[74] It could be argued that there is also an imbalance between online platform companies and their users. For instance, some users of dominant online platforms feel that they do not have the choice to consent because the platform and the data subject do not have equal negotiation power.[75] Additionally, according to Recital 43 of the GDPR, the consent is not freely given if data subjects lack the option to give separate consent for different data processing operations.[76]

In a different context, in the joined cases C-92/09 and C-93/09 *Volker und Markus Schecke GbR/Hartmut Eifert v. Land Hessen*[77] (related to agricultural subsidies), the Advocate General (AG) Eleanor Sharpston provided a useful guidance regarding under what conditions consent could be considered freely given under Directive 95/46/EC.[78] Although the AG did not explicitly give an opinion on whether consent was freely given in the particular case, it was argued that if individuals have no alternative but to consent to the publishing of personal data due to economic reasons, consent cannot be regarded as valid.[79]

In case C-673/17 *Planet49,* the CJEU found that the practices of an online gaming company to obtain consent were in noncompliance with the GDPR and ePrivacy Directive. The CJEU stated that consent could not be deemed informed or specific.[80] In *Planet49,* the company had made the entry to a promotional lottery conditional on users' consent to the use of their personal data for

[72] Article 29 Working Party, Guidelines on Consent under Regulation 2016/679, (2017), *supra nota* 63, p 6.
[73] *Ibid*., p 6.
[74] *Ibid*., p 6.
[75] Zuiderveen Borgesius, F. J. *et al*. (2017). *supra nota* 51, p 361.
[76] Recital 43 of the GDPR
[77] Court decision, 9.11.2010, *Volker und Markus Schecke GbR/Hartmut Eifert v. Land Hessen*, C-92/09 and C-93/09 (Joined Cases), EU:C:2010:662. The case was about applicants who received agricultural subsidies from the European Agencies, after applying from local authorities. In the application form it was stated that information on the beneficiaries of funds and the amounts received are published. (par 26) Applicants wanted to prevent publication of data relating to them and stated that publication is not justified by overriding public interests. (par 28)
[78] Opinion of Advocate General, *Volker und Markus Schecke GbR/Hartmut Eifert v. Land Hessen,* 17.6.2010, C-92/09 and C-93/09 (Joined Cases), EU:C:2010:353. The main issue in which AG focused was whether the consent for publication of information was freely given. Land Hessen had argued that applicants could have avoid the publication of information by forgo the aid. However, AG reminded that the aid may represent between 30 % and 70% of a farmer's income and stated that "significant economic duress sufficed to render consent non-voluntary (and thus not 'freely given' in the meaning of Article 2(h) of Directive 95/46)."
[79] *Ibid*., paragraph 82, for further analysis see e.g. Kosta, E. (2013). *supra nota* 69, p 187.
[80] Court decision, 1.10.2019, *Planet49*, C-673/17, EU:C:2019:801, paragraph 58.

advertising purposes.[81] The question arises of whether this constituted freely given consent since users had to agree to the advertising to participate. Unfortunately, the CJEU was not asked about the issue of freely given consent, so it did not provide an opinion on that. According to the Article 29 Working Party, the GDPR does not exclude all incentives but the controller must demonstrate that consent was still freely given.[82] However, a review of the AG's opinion in this case and the GDPR's guidance regarding consent suggests that consent cannot be deemed freely given in these circumstances. As the AG pointed out, consent should be separate in addition to active. Therefore, to be regarded as freely given in this case, consent should have been separate from the indication to participate in the lottery.[83]

To conclude, only when the individual has real freedom of choice, when the individual is not subjected to coercion and when there is no clear imbalance of powers can consent be considered freely given within the meaning of EU law and as interpreted by the CJEU.

2.1.2 Specific

The next element of valid consent is "specific", meaning that the consent should be given to a specific processing operation and not to operations in general.[84] Article 6(1)(a) of the GDPR states that the data subject should have "given consent to the processing of his or her personal data for one or more 'specific' purposes."[85] The specific consent should guarantee data subjects control and a degree of transparency.[86] When there are different purposes, all of them must be clearly explained, and consent should be acquired for each.[87]

In case C-543/09 *Deutsche Telekom AG*, the CJEU noted that if a data subject has been informed about the processing of their personal data for a specific data processing operation, renewed consent is not needed even if the data controller changes.[88] However, in the more recent *Planet49* (discussed above), the CJEU strengthened the requirement that consent must be specific and stated

[81] *Ibid*., paragraph 64.
[82] Article 29 Working Party, Guidelines on Consent under Regulation 2016/679, (2017), *supra nota* 63, p 11.
[83] Opinion of Advocate General, 21.3.2019, *Planet49*, C-673/17, EU:C:2019:246, paragraph 66.
[84] Ustaran, E. (Ed.). (2018). *supra nota* 7, p 115.
[85] Article 6(1)(a) of the GDPR
[86] Article 29 Working Party, Guidelines on Consent under Regulation 2016/679, (2017), *supra nota* 63, p 11.
[87] Ustaran, E. (Ed.). (2018). *supra nota* 7, p 115.
[88] Court decision, 5.5.2011, *Deutsche Telekom AG v Bundesrepublik Deutschland*, Case C-543/09, EU:C:2011:279, paragraph 67.

that consent must relate specifically to the processing of the data in question and cannot be inferred for other purposes.[89]

In our example case, Platform A should acquire consent for each specific processing operation. Furthermore, Platform A should clearly separate information concerning consent for data processing activities from information about other matters.[90] Other processing actions cannot be hidden behind the function for which consent has been given.[91] Specific consent is closely related to the purpose limitation principle (discussed in section 2.2) because together they secure the progressive widening of purposes for which data is used.[92] If Platform A wants consent for many purposes, it should acquire separate specific consent for specific processing purposes.[93]

2.1.3 Informed

The third element of valid consent is "informed", meaning that the data subject is informed about relevant aspects of processing, such as the controller's identity, the type of information to be collected and used, the purpose of each processing operation for which consent is sought, the right to withdraw consent and appropriate safeguards.[94] The GDPR does not describe the form in which the information should be presented in order to be regarded as informed consent.[95] However, Article 7(2) and Recital 32 of the GDPR set requirements for informed consent.[96] When obtaining consent, the language of the request should be clear and ordinary and not unnecessarily disruptive to the use of service for which consent is given.[97] To create adequate informed consent, privacy policies should be reasonable in length and understandable for an average person.[98] Consent must be separate from other subjects, and it cannot be hidden behind general terms and conditions.[99]

CJEU has interpreted meaning of informed consent in the case C-40/17 *Fashion ID.*[100] In the case an online clothing retailer set on its website the "Like" button from the social network Facebook. Because of the button embedded in the website, visitors' personal data were transmitted to

89 *Planet49*, C-673/17, paragraph 58.
90 Article 29 Working Party, Guidelines on Consent under Regulation 2016/679, (2017), *supra nota* 63, p 11.
91 Team, I.P. (2017). *supra nota* 17, p 208.
92 Article 29 Working Party, Guidelines on Consent under Regulation 2016/679, (2017), *supra nota* 63, p 12.
93 *Ibid*., p 12.
94 Article 29 Working Party, Guidelines on Consent under Regulation 2016/679, (2017), *supra nota* 63, p 13.
95 *Ibid*., p 13.
96 *Ibid*., p 13.
97 Recital 32 of the GDPR
98 Article 29 Working Party, Guidelines on Consent under Regulation 2016/679, (2017), *supra nota* 63, p. 14.
99 *Ibid*., p. 14.
100 Court decision, 29.7.2019, *Fashion ID*, C-40/17, EU:C:2019:629.

Facebook Ireland. The transmission occurred without visitors being aware of it and even if visitors did not click the Like button or did not have a Facebook account.[101] The CJEU stated that since Fashion ID collected data and shared it with Facebook Ireland, Fashion ID can be considered a controller jointly with Facebook Ireland.[102] Consequently, the CJEU ruled that as a controller, Fashion ID must obtain consent regarding operations involving the processing of personal data. In addition, Fashion ID is responsible for informing users that personal data will be transferred to Facebook.[103]

Based on this analysis, before obtaining consent, Platform A should provide sufficient information to guarantee that the data subject understands the agreement. Thus, informed consent is close to the specific consent because if the purposes for which consent is given are not specific, the data subject cannot be regarded as properly informed.

2.1.4 Unambiguous

The fourth element of valid consent as stated in the GDPR is that the consent must be unambiguous. Consent must be given in a statement or by a clear affirmative action, which indicates that to be unambiguous, consent must be given by an active motion or declaration.[104]

In the above-mentioned *Planet49* case, the CJEU reviewed the concept of consent relative to the use of cookies by examining the ePrivacy Directive and stated that "Although Article 5(3) states expressly that the user must have 'given his or her consent' to the storage of and access to cookies, the provision does not indicate the way in which consent must be given." However, "according to literal interpretation of the Article, *action* is required in order to give consent."[105] Recital 17 of the ePrivacy Directive states that, "for the purposes of this directive, consent of a user should have the same meaning as the data subject's consent as defined and further specified in Directive 95/46/EC." Directive 95/46/EC defines a data subject's consent as being "any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed."[106] In addition, the CJEU referred to the AG's opinion which noted that "indication" of the data subject's wishes clearly points to active rather than passive

[101] *Ibid.*, paragraphs 25 and 27.
[102] *Ibid*., paragraph 84.
[103] *Ibid*., paragraphs 101 and 104.
[104] Article 4(11) of the GDPR.
[105] *Planet49*, C-673/17, paragraph 49.
[106] *Ibid.*, paragraphs 50-51.

behavior. Consent given by a preselected tick of a checkbox does not imply active behavior by the website user.[107] Ultimately, the court referred to Article 7(a) of Directive 95/46/EC and noted that a data subject's consent may make processing lawful if the data subject has given their consent unambiguously, and only active behavior of the data subject with a prospect of giving consent may fulfill that requirement.[108] To conclude, when obtaining consent, in the hypothetical case Platform A cannot use for example pre-ticked boxes, but consent must be give through active behavior in order to be regarded unambiguous.

Based on the analysis above, according to Article 6(a) of the GDPR, a platform can lawfully process personal data only on the basis of valid consent. Four conditions are necessary for consent to be considered valid: The consent must be freely given, specific, unambiguous and informed. Each element of valid consent leaves a degree of flexibility and interpretation. Analysis of the so-far limited CJEU case law suggests, however, that the court interprets each condition and considers the cumulative effect of the four elements.

2.2 Purpose Limitation Principle

The concept of consent, as discussed above, is the necessary first element of the lawful processing of personal data. Consent presupposes that the data subject gives the data controller the right to use their data for a specific purpose. What obligations does the data controller have if it wants to use the collected data for other purposes - for example, to share it with third parties? To avoid an abuse of concept, the EU data protection regime includes a purpose limitation principle, which is analyzed in this section.

Purpose limitation is a fundamental principle in the EU's data protection field that aims - in combination with the five other principles listed in Article 5 of the GDPR - to guarantee lawful, fair and transparent processing of data.[109] Its legal background can be found in Directive 95/46/EC, and the principle is also taken into account in Article 8(2) of the Charter.[110] Purpose limitation maintains legal certainty and trust, which is why the purpose limitation principle is one of the basis

[107] *Ibid.*, paragraph 52.
[108] *Ibid.*, paragraph 54.
[109] Article 5 of the GDPR. Other data processing principles listed in Article 5 of the GDPR are lawfulness, fairness and transparency, data minimization, accuracy, storage limitation and integrity and confidentiality.
[110] Zarsky, T. Z. (2016). *supra nota* 4, p 1006.

of data protection.[111] The purpose limitation principle is closely related to the theory of privacy as informational control, which means that a person can have full control over their personal data when they understand the purposes for data processing before providing information.[112]

The purpose limitation principle is determined in Article 5(1b) of the GDPR, which states that "personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes."[113] The Article 29 Working Party gave an opinion regarding the purpose limitation principle in 2013. The following section analyzes the three main elements of the purpose limitation principle: specified, explicit and legitimate purposes.

2.2.1 Specified purposes

The first element central to the purpose limitation principle is that the collected data must be for specified purposes. Before Platform A from our example case starts to collect personal data, it must clearly determine the specified purpose or purposes for collecting that data. After specifying the purposes as a controller, the platform must consider whether collection and processing are necessary to achieve those purposes.[114] This signifies that personal data that is unnecessary, inadequate or irrelevant for the purposes intended to be served should not be collected.[115] To ascertain whether data processing is based on legal grounds and what data protection safeguards should be used, one must first determine the specified purposes for which the personal data is to be collected.[116] Purposes should be specified prior to, and not after, the collection of personal data.[117] Vague or general purposes such as "future research" or "improving the user experience" do not fulfill specificity criteria.[118] The detail required depends on the context.[119] However, purposes expressed by lengthy legal language may hinder rather than promote the data subject's understanding.[120]

111 Article 29 Working Party, Opinion 03/2013 on purpose limitation p. 4 Accessible: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf, 20.2.2020
112 Gutwirth, S. *et al*. (2014). *Reloading data protection: multidisciplinary insights and contemporary challenges.* Netherlands: Dordrecht Springer. p 304.
113 Article 5 of the GDPR
114 Forgó, N. *et al.* (2017). The principle of purpose limitation and big data. – *New technology, big data and the law*. Springer, Singapore, p 27.
115 *Ibid*., p 27.
116 Article 29 Working Party, Opinion 03/2013 on purpose limitation (2013) *supra nota* 111, p 15.
117 *Ibid.*, p 15.
118 *Ibid*, p 16.
119 *Ibid.*, p 16.
120 *Ibid.*, p 16.

2.2.2 Explicit purposes

The second element of the purpose limitation principle is that the purposes of collecting personal data should be explicit, which means that purposes must be explained and expressed in a clear manner.[121] There should be no vagueness or ambiguity about the purposes for which data is collected.[122] The data subject should understand the purposes in the same way as the persons who collect the data, including all relevant persons working with data and data protection authorities.[123] Explicitness enhances predictability and adds transparency.[124]

2.2.3 Legitimate purposes

The third element of the purpose limitation principle is that the purposes should be legitimate. To be regarded as legitimate, a purpose of processing must at every stage and at all times be based on at least one of the legal grounds listed in Article 6(1) of the GDPR.[125] The legitimacy of the purposes indicates that purposes of collecting shall accord with existing law in the broadest sense.[126] This requirement means that written legislations, including primary as well as secondary legislation, judicial precedents, fundamental rights and principles and so forth should be followed.[127] Furthermore, the overall context and facts of the cases can be also considered - for example, the relationship between the controller and the data subject.[128]

2.2.4 Compatibility

The purpose limitation principle prohibits further processing if the purposes are incompatible with the initial purposes. Thus, further processing as such is not prohibited; it is prohibited only if such processing is incompatible with the initial purposes.[129] Thus, the compatibility of further processing with the initial purposes must be considered. Further processing for statistical purposes, scientific or historical research purposes or archiving purposes in the public interest are not considered incompatible if processing is conducted according to the limits set by the EU or a member state's law that governs the particular processing.[130] If further processing of data does not

121 *Ibid*, p 17.
122 *Ibid*., p 17.
123 *Ibid*., p 17.
124 *Ibid*., p 17.
125 *Ibid*., p 97.
126 Voigt, P., & Bussche, A. (2017) *supra nota* 5, p 89.
127 Article 29 Working Party, Opinion 03/2013 on purpose limitation (2013) *supra nota* 111, p 20.
128 Forgó, N. *et al*. (2017). *supra nota* 114, p 28.
129 Article 29 Working Party, Opinion 03/2013 on purpose limitation (2013) *supra nota* 111, p 3.
130 Ustaran, E. (Ed.). (2018). *supra nota* 7, p 104.

relate to these purposes, the compatibility of processing must be evaluated.[131] Further processing operations should accord with the foremost purpose, or, if contrary, renewed consent should be obtained.[132] To determine whether use accords with the initial purposes, one should especially consider the following:

"any link between purposes for which the personal data have been collected and the purposes of the intended further processing, the context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller, the nature of the personal data, in particular whether special categories of personal data are processed, the possible consequences of the intended further processing for data subjects and the existence of appropriate safeguards, which may include encryption or pseudonymization."[133]

All these requirements should be contemplated to consider whether further processing is regarded to be compatible with the initial purposes.[134] However, if the processing is considered incompatible with the initial purposes, there needs to be a distinct legal basis for processing.[135]

To conclude, according to Article 5(b) of the GDPR, a platform can process data only for purposes that are specified, explicit and legitimate. All of these elements must be fulfilled for the processing of personal data to be deemed lawful. Further processing is not entirety declined; however, it must be compatible with the initial purposes. If platform A wants to further process data acquired, it must consider, among other aspects is there a sufficient link between purposes for which data was initially collected and purposes to which it wants to further process data.

131 Article 29 Working Party, Opinion 03/2013 on purpose limitation (2013) *supra nota* 111, p 3.
132 Voigt, P., & Bussche, A. (2017) *supra nota* 5, p 89.
133 Recital 50 of the GDPR and Article 6 (4) of the GDPR.
134 Ustaran, E. (Ed.). (2018). *supra nota* 7. p 104.
135 *Ibid*., p 104.

3. PROBLEMS IN THE FIELD OF ONLINE PLATFORMS

The analysis in Chapter 1 and Chapter 2 suggest that EU law provides a detailed legal framework and conditions applicable to the collection and processing of personal data. This legal framework applies to very broad spectrum of issues. Building on the analysis above, the Chapter 3 focuses on the application of the principles of consent and purpose limitation in the context of practices that online platforms use to collect and analyze 'Big Data'. Specifically, Chapter 3 describes the challenges that techniques and practices used by online platforms present to the realization of these legal rights analyzed in Chapter 2.

3.1 Big Data

Trends in high-tech platforms such as social networks, the cloud and big data constitute a powerful surveillance society with multiple benefits, but also with privacy challenges and threats.[136] Possibly the most crucial challenge in the sphere of data protection and privacy in the digital age is the increase of big data.[137] The term "big data" relates to the procedures of analyzing and creating extensive datasets, including personal data.[138] In the literature, big data has been defined by four Vs: the volume of data, the velocity with which the data can be analyzed, the variety of sources, and the veracity of the data that arguably could be achieved through analysis.[139] Big data also refers to new ways that companies can combine diverse digital datasets and, through analysis, extract hidden information and correlations.[140] In big data operations technology is used to assist on the collection and storage of huge amount of data and algorithms to support in analyzing and understanding value and connections of different data sets.[141]

136 Politou, E. *et al*. (2018). Forgetting personal data and revoking consent under the GDPR: Challenges and proposed solutions. – *Journal of Cybersecurity*, Vol 4, Issue 1, Oxford: Oxford Academic., p 2.
137 Zarsky, T. Z. (2016). *supra nota* 4, p 996.
138 Zarsky, T. Z. (2016). *supra nota* 4, p 996.
139 *Ibid.*, p 999.
140 Rubinstein, I (2013). Big data: the end of privacy or a new beginning? – *International Data Privacy Law*, Vol 3, Issue 2, p. 74.
141 Gonçalves, M. E. (2017). The EU data protection reform and the challenges of big data: remaining uncertainties and ways forward. – *Information and Communications Technology Law,* Vol 26, Issue 2, p 94.

3.1.1 Big Data as an Important Asset for Businesses

The way people express their opinions, receive information, discuss, argue and learn is widely influenced by dominant online platforms such as Facebook and Google.[142] The competitive strength of online platforms and businesses is increasingly dependent on the amount and quality of the data they possess.[143] This data economy has apparent benefits, and although the fact that companies collect information from customers is not new, the level of detailed observation of user data and specifically personal data is greater than ever.[144] The way businesses collect and use personal data improves efficiency, quality and productivity.[145] Because personal data has the potential to create added value for companies and consumers, it has been described as a new asset.[146] Whereas in the past, money was a prerequisite to obtain services before, today many online companies receive their payment in the form of data.[147]

3.1.2 Purpose Limitation Principle and Big Data

As presented in Chapter 2 processing of personal data is only allowed for specified, explicit and legitimate purposes and further processing for different purposes is not allowed, unless these purposes are compatible with initial purposes. To comply with the specified purposes requirement platform should clearly and specifically identify purpose of the collection.[148] Furthermore, data that is not necessary should not be collected.[149] However, the gathering of big data is performed by using various sources[150] and one of the main functions of big data is to reuse collected data for new purposes.[151] Big data also contains methods and uses which were not known by the collector or data subject in the time of collection.[152] These techniques and methods hinder the realization of specified purposes.

142 Jørgensen, R., & Kaye, D. (2019). *Human rights in the age of platforms.* Cambridge, Massachusetts: The MIT Press. p 53.
143 Graef, I. (2015). *supra nota* 8, p 473.
144 Goldfarb, A., & Tucker, C. (2012). Privacy and innovation. – *Innovation policy and the economy,* Vol 12, Issue 1, p 65.
145 Tikkinen-Piri, C. *et al*. (2018). *supra nota* 27, p 13
146 Spiekermann, S. *et al.* (2015). The challenges of personal data markets and privacy. – *Electronic markets*, Vol 25, Issue 2, p 161.
147 Graef, I. (2015). *supra nota* 8, p 474.
148 Article 29 Working Party, Opinion 03/2013 on purpose limitation (2013) *supra nota* 111, p 15.
149 *Ibid.*, p 15.
150 ENISA (2015), *supra nota* 11, p 13.
151 Gonçalves, M. E. (2017). *supra nota* 141, p 96.
152 Zarsky, T. Z. (2016). *supra nota* 4, p 1006.

Purposes for collecting data should be also explicit which means that there shouldn't be vagueness about the purposes for which data is collected and purposes should be clearly presented.[153] However, in big data operations uses for collected data can be determined later when discovering other purposes the data can be used.[154] Thus explicit purposes can be difficult to determine at the time of the collection.

As presented above purpose limitation principle requires that purposes are legitimate.[155] To comply with the legitimacy requirement, purposes must base on one of the legal grounds presented in Article 6 of the GDPR. In the case of online platforms this legitimate ground for processing is usually user consent, because rarely in case of online platforms processing of personal data is based on other grounds established in Article 6.[156] Thus, when an online platform wants to use data acquired earlier, for purposes incompatible with the initial purposes, it must obtain renewed consent from the data subject.[157] However, acquiring new consent can be difficult because, as stipulated in the GDPR and discussed in Chapter 2, conditions for consent are relatively strict. Furthermore, as case *Planet49* illustrates, for consent to be regarded as valid, access to or use of the service cannot be conditioned on the consent, because that can make the consent forced.

Considering these aspects, complying with the purpose limitation principle can prove to be costly and in some cases impossible.[158] Defining purposes for future uses widely and broadly would not resolve this matter since according to the purpose limitation purposes should be defined in a specific manner.[159] There is, however, an exemption in the purpose limitation principle that allows further processing of personal data for statistical purposes.[160] This can be seen as way for GDPR drafters to enable the uses of big data techniques to some extent.[161] However, recital 162 of the GDPR states that results of statistical processing "are not used in support of measures or decisions regarding any particular natural person."[162] To conclude, it is impossible to protect purpose

153 Article 29 Working Party, Opinion 03/2013 on purpose limitation (2013) *supra nota* 111, p 17.
154 Hoeren, T. *et al*. (2018). *supra nota* 13, p 32.
155 *Ibid*., p 32.
156 Other grounds presented in the Article 6 of the GDPR are: processing is necessary for the performance of a contract, for compliance with a legal obligation, protect vital interests of the data subject or other natural person, performance of a task carried out in the public interest or in exercise of official authority vested in the controller, legitimate interests pursued by the controller or a third party.
157 Voigt, P., & Bussche, A. (2017) *supra nota* 5, p 89.
158 Recital 162 of the GDPR, for further analysis see. Zarsky, T. Z. (2016). *supra nota* 4, p 1006.
159 Hoeren, T. *et al*. (2018). *supra nota* 13, p 32.
160 Article 5(b) of the GDPR
161 Mayer-Schonberger, V.; Padova, Y. (2016). Regime change: Enabling big data through Europe's new data protection regulation. – *Columbia Science and Technology Law Review*, Vol 17, Issue 2, p 326.
162 Zarsky, T. Z. (2016). *supra nota* 4, p 1008.

limitation principle provided in the GDPR in the field of big data analytics used by online platforms.

3.2 Consent and Online Platforms

3.2.1 Consent in Concentrated Markets

As stated above in a case of online platforms amount of data platform possess usually determines its success.[163] Thus markets in the field of online platforms are often concentrated or monopolistic. Popular and free services are based on business models in which revenue derives user data-based profiling and advertising.[164] To gain access to the website, the user usually must provide some personal information. Privacy policies used by platforms often have little or no room for negotiation, and the user must provide information to use the service.[165] When it comes to the major digital service providers such as Google, Facebook and Twitter, there are no comparable alternatives to choose.[166] People tend to use certain online platforms such as Facebook or Twitter because their social contacts use the same service.[167]

When comparing above-mentioned concentration of markets of online platforms with the concept of consent as presented in Chapter 2, it seems problematic in many ways. Firstly, consent should fulfill four cumulative conditions and be "freely given, informed, specific and unambiguous."[168] However, when markets in the field of online platforms are concentrated users have only few or no alternatives from which they can choose. Thus, user don't have alternative but to consent for privacy policies that dominant platforms use. When markets are concentrated user has not been offered with freedom of choice, which is one of the prerequisites of valid consent, so the consent cannot be regarded freely given.

163 Graef, I. (2015). *supra nota* 8, p 473.
164 Koops, B. J. (2014). The trouble with European data Protection law. – *International data privacy law*, Vol 4 Issue 4, p 252.
165 Bergemann, B. (2017). The Consent Paradox: Accounting for the Prominent Role of Consent in Data Protection. In: – *IFIP International Summer School on Privacy and Identity Management*. Springer, Cham, p 6.
166 Koops, B. J. (2014). *supra nota* 164, p 251.
167 Bergemann, B. (2017). *supra nota* 165, p 6.
168 Recital 32 of the GDPR

3.2.2 Consent and the Complexity of Privacy Policies

As detailed in the Chapter 2, in order to process personal data platform should acquire valid consent and after that process data only for purposes which are compatible with those purposes that consent was initially sought. When informing users about processing operations they are consenting, online platforms use privacy policies. Unfortunately, these policies are often legalistic and complex.[169] Even if users of online platforms are technically informed about the use of their data, they often do not entirely understand the nature and extent of their consent.[170] Although the GDPR aims at consumers' self-determination and autonomy, consumers do not often operate as envisioned by GDPR drafters. Possessors of data know this and act accordingly.[171] The "privacy paradox" refers to the situation in which most users are very concerned about breaches privacy, but few use the privacy options available.[172] Despite the demand for privacy and data protection, consumers use the free services.[173] When faced with the question of whether they want to use a service at the cost of handing over their personal data or whether they want to be excluded from using the service, most users choose to use the service.[174] Due to the absence of alternatives and regardless of their preferences, users drift into agreeing to privacy policies.

Privacy policies could provide the necessary transparency that would let users inform themselves about the privacy practices of certain platforms.[175] However, many users do not read privacy policies carefully enough to enhance privacy.[176] In addition, privacy policies are usually written by lawyers for lawyers, which makes understanding them difficult.[177] When users do not have capabilities to understand or read long and complicated privacy policies they cannot be regarded informed.[178] The complex privacy policies contradict with the concept of consent which requires as presented in Chapter 2 that consent is informed and specific. GDPR states in the recital 42 that "a declaration of consent pre-formulated by the controller should be provided in an intelligible and

169 Carolan, E. (2016). The continuing problems with online consent under the EU's emerging data protection principles. – *Computer Law & Security Review: The International Journal of Technology Law and Practice,* Vol 32 Issue 3, p 465.
170 *Ibid.*, p 463.
171 Botta, M., & Wiedemann, K. (2019). *supra nota* 62, p 429.
172 Hallam, C., & Zanella, G. (2017). Online self-disclosure: The privacy paradox explained as a temporally discounted balance between concerns and rewards. – *Computers in Human Behavior*, Vol 68, p 219.
173 Botta, M., & Wiedemann, K. (2019). *supra nota* 62, p 429.
174 Belli, L. *et al*. (2017). Selling your soul while negotiating the conditions: from notice and consent to data control by design. – *Health and Technology*, Vol 7, Issue 4, p 456.
175 Jørgensen, R., & Kaye, D. (2019). *supra nota* 142, p 266.
176 Botta, M., & Wiedemann, K. (2019). *supra nota* 62, p 432.
177 Cate, F. H., & Mayer-Schönberger, V. (2013). Notice and consent in a world of Big Data. – *International Data Privacy Law*, Vol 3 Issue 2, p 67.
178 Botta, M., & Wiedemann, K. (2019). *supra nota* 62, p 432.

easily accessible form, using clear and plain language."[179] Furthermore the privacy policies should be reasonable in length and understandable for an average person in order to create adequate informed consent.[180] Besides, consent should be given for specific processing operation and not just generally.[181] In cases where user don't fully understand functions to which they are consenting or do not have capabilities to internalize information provided, they cannot give valid consent as required in the GDPR.

3.2.3 Consent and Take-It-or-Leave-It Methods

Some websites use the take-it-or-leave-it methods when users try to access the site. Tracking walls are barriers that website users can pass only if they consent to tracking by third parties.[182] The cookie wall blocks users' access to the website unless the user performs certain functions, such as pressing a digital button.[183] However on the contrary to take-it-or-leave-it methods, Article 7(4) of the GDPR, states that:

"When assessing whether consent is freely given, utmost account shall be taken of whether, *inter alia*, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract."[184]

When taking into account the Article 7(4) of the GDPR as well as other elements of consent presented in the Chapter 2 it can be argued that in the case where platform uses take it or leave it models, consent does not fulfill objective of freely given. Even tough cookie walls or other methods which require consent of the user to access website fulfil the obligations of affirmative action and provide sufficient information, the lack of freedom of choice makes contradiction between "take it or leave it" and valid consent.[185] As presented in Chapter 2 user should have real freedom of choice and there should not be coercion, intimidation, deception or any other negative consequences if user does not consent.[186]

179 Recital 42 of the GDPR
180 Article 29 Working Party, Guidelines on Consent under Regulation 2016/679, (2017), *supra nota* 63, p. 14.
181 Ustaran, E. (Ed.). (2018). *supra nota* 7, p 115.
182 Zuiderveen Borgesius, F. J. *et al.* (2017). *supra nota* 51, p 353.
183 Ustaran 2018, Cookie Consent Is the New Panic – [web article], accessible: https://www.hldataprotection.com/2018/07/articles/international-eu-privacy/cookie-consent-is-the-new-panic/, 8.4.2020
184 Article 7(4) of the GDPR
185 Ustaran 2018, Cookie Consent Is the New Panic. *supra nota* 183.
186 Article 29 Working Party, Guidelines on Consent under Regulation 2016/679, (2017), *supra nota* 63, p 7.

CONCLUSION

The thesis analyzed whether and how methods for data processing and collection could be reconciled with the obligations following from EU primary and secondary law on data protection. Thesis aimed to resolve a practical situation, as exemplified by a hypothetical case, to determine whether the current practice of online platforms to collect and use personal data violate the elements of consent and purpose limitation principle provided in the EU General Data Protection Regulation. The main hypothesis of the thesis is confirmed. The methods for big data collection and use analyzed in Chapter 3, compared against obligations from primary and secondary law analyzed in Chapter 1 and 2 suggest that not all elements of valid consent are fulfilled in the field of online platforms. Furthermore, analysis presents that purpose limitation principle is not in conformity with big data operations.

In order to test the hypothesis, thesis focused on two more specific research questions. (a) How can data subjects give informed, specific, free and unambiguous consent within the meaning of the GDPR, if they do not know the exact purposes of and means of processing personal data? And (b) Do big data collection operations conflict with the purpose limitation principle when the uses of data are determined after data collection and when the data subject is unaware of the sources from which data is collected?

The analysis in Chapters 1 and 2 presents that individuals right to data protection is regulated comprehensively in legal framework of the European Union. The GDPR sets consent as one of the legal bases for the processing of personal data and defines it as any freely given, specific, informed and unambiguous indication of a data subject's wishes. Furthermore, to protect and limit the use of collected data, the GDPR includes the purpose limitation principle, which requires that personal data be collected for specified, explicit and legitimate purposes and not be further processed in a manner incompatible with those purposes. These principles aim to protect individuals' fundamental rights to privacy and data protection. One of the aims of the GDPR is to guarantee individuals control over their own personal data.

However, as the analysis in Chapter 3 indicates, the way online platforms collect and use personal data serves opposite purposes than legal rights presented in Chapters 1 and 2. Competitive value of online platforms is to an increasing extent dependent on the quantity and quality of the data they possess. Strategies of online platforms to collect and use data contain a variety of measures and sources. Furthermore, platforms use collected data to purposes which were not known at the time of the collection. Big data operations create and analyze extensive datasets, which often include personal data. However, the purpose limitation principle demands that personal data is used only for purposes it has been initially collected. These purposes must be specified, explicit and legitimate. Complying with requirement that purposes should be specified and explicit is problematic because big data operations include reuse of data for new purposes which may have been unknown at the time of collection.

Purpose limitation principle also demands that processing is based on legal grounds. Usually this legal ground is user consent. If online platform wants to process personal data for further purposes which are incompatible with initial ones, it must acquire new consent. However, as analyzed in Chapter 2 elements of concept of consent are rather strict and to obtain valid consent, the GDPR must be precisely followed. Also, as the CJEU stated in case *Planet49*, consent must relate specifically to the processing of the data in question and cannot be inferred from an indication of the data subject's wishes for other purposes. These aspects make the exercise of purpose limitation costly and some cases impossible for online platforms to comply with. The purpose limitation principle makes an exception which allows further processing on new grounds for statistical purposes. However, if all big data operations that seek further processing were acceptable, the purpose limitation would be made void.

Because the data is essential value for online platforms markets in the field are often concentrated. This means that individuals have only few or no alternatives. One of the elements of consent analyzed in the thesis, is that consent must be 'freely given'. In concentrated markets individuals don't have other choice than to agree collection and use of personal data by platform if they want to use service. Thus, consent cannot be regarded as freely given. Furthermore, users of online platforms are presented with privacy policies which are often long and written in a legal language. Individuals who use online platforms, from several different service providers have neither time nor resources to internalize information in a way that would constitute informed consent. Some platforms also use take-it-or-leave it models. This technique prevents user access to the site completely or partially unless they give permission to the processing of their personal data. In the

cases where an online platform uses take-it-or-leave-it methods, consent is not freely given, because consent is required to continue using the service.

Even though the GDPR regulates the elements of consent and purpose limitation precisely, rights provided are not realized effectively, because of the way online platforms collect and use data in today's information society. The use of data can be seen as an essential facility for many online businesses, and big data operations have increased due to the benefits. Although the conditions of consent are strictly regulated, the realization of valid consent is hindered by lack of alternatives, complex privacy policies, and take-it-or-leave-it methods. Furthermore, although the purpose limitation principle requires that the uses of data are determined before collection, big data operations are based on the collection of data from a variety of sources. The GDPR aims to guarantee natural persons' control over their personal data, however in the field of big data, such a guarantee seems unrealistic. Based on research concept of consent and the purpose limitation principle are inadequate and ineffective concepts to protect individuals' fundamental rights in the age of big data and Articles 5(b) and 6(a) of the GDPR should be revised in a way that individuals right to self-determination is safeguarded.

LIST OF REFERENCES

Scientific books

1. Barnard, C., & Peers, S. (Eds.). (2014). *European Union Law*. Oxford: Oxford University Press.

2. Bennett, C. J. (1992). *Regulating privacy: Data Protection and public policy in Europe and the United States*. New York: Cornell University Press.

3. Calder, A. (2018). *EU GDPR: A Pocket Guide*, School's Edition: Vol. School's edition. United Kingdom: IT Governance Publishing Ltd.

4. Gutwirth, S., Leenes, R., De Hert, P. (2014). *Reloading data protection: multidisciplinary insights and contemporary challenges*. Netherlands: Dordrecht Springer.

5. Gutwirth, S., R., & de Hert, P. (2015). *Reforming European Data Protection Law*. Vol 20. Netherlands: Dordrecht Springer.

6. Hameurlain, A., & Wagner, R. (2018). *Transactions on Large-Scale Data- and Knowledge- Centered Systems*. Berlin, Heidelberg: Springer eBooks., 6th Ed.

7. Hijmans, H. (2016). *The European Union as guardian of internet privacy: The Story of Art 16 TFEU*. Switzerland: Springer.

8. Hoeren, T., Kolany-Raiser, B., & Bittner, L. (2018). *Big data in context: legal, social and technological insights.* Cham, Switzerland: Springer Open.

9. Jørgensen, R., & Kaye, D. (2019). *Human rights in the age of platforms.* Cambridge, Massachusetts: The MIT Press.

10. Kosta, E. (2013). *Consent in European Data Protection Law*. Leiden: BRILL.

11. Moore, M., & Tambini, D. (Eds.). (2018). *Digital dominance: the power of Google, Amazon, Facebook, and Apple.* New York, NY: Oxford University Press.

12. Team, I.P. (2017). *EU General Data Protection Regulation (GDPR): An implementation and Compliance Guide*. Second edition, United Kingdom: IT Governance Publishing.

13. Ustaran, E. (Ed.). (2018). *European Data Protection: Law and Practice*. United States: An IAPP Publication, International Association of Privacy Professionals.

14. Voigt, P., & Bussche, A. (2017). *The EU general data protection regulation (GDPR): a practical guide*. Cham, Switzerland: Springer.

Scientific articles

15. Basin, D., Debois, S., & Hildebrandt, T. (2018). On purpose and by Necessity: Compliance Under the GDPR. – *Lecture Notes in Computer Science*, 10957, 20-37.

16. Belli, L., Schwartz, M., & Louzada, L. (2017). Selling your soul while negotiating the conditions: from notice and consent to data control by design. – *Health and Technology*, Vol 7, Issue 4, 453-467.

17. Bergemann, B. (2017). The Consent Paradox: Accounting for the Prominent Role of Consent in Data Protection. In: – *IFIP International Summer School on Privacy and Identity Management*. Springer, Cham, 111-131.

18. Botta, M., & Wiedemann, K. (2019). The interaction of EU competition, consumer, and data protection law in the digital economy: the regulatory dilemma in the Facebook odyssey. – *The Antitrust bulletin*, Vol 64, Issue, 3, 428-446.

19. Carolan, E. (2016). The continuing problems with online consent under the EU's emerging data protection principles. – *Computer Law & Security Review: The International Journal of Technology Law and Practice,* Vol 32, Issue 3, 462-473.

20. Cate, F. H., & Mayer-Schönberger, V. (2013). Notice and consent in a world of Big Data. – *International Data Privacy Law,* Vol 3, Issue 2, 67-73.

21. Forgó, N. Hänold, S. and Schütze, B. (2017). The principle of purpose limitation and big data. – *New technology, big data and the law*. Springer, Singapore, 17-42.

22. Goldfarb, A., & Tucker, C. (2012). Privacy and innovation. – *Innovation policy and the economy,* Vol 12, Issue 1, 65-90.

23. Gonçalves, M. E. (2017). The EU data protection reform and the challenges of big data: remaining uncertainties and ways forward. – *Information and Communications Technology Law,* Vol 26, Issue 2, 90-115.

24. Graef, I. (2015). Market definition and market power in data: The cases of online platforms. – *World Competition*, Vol 38, Issue 4, 473-505.

25. Hallam, C., & Zanella, G. (2017). Online self-disclosure: The privacy paradox explained as a temporally discounted balance between concerns and rewards. – *Computers in Human Behavior*, Vol 68, 217-227.

26. Kirsch, M. S. (2011). Do-not-track: Revising the EU's data protection framework to require meaningful consent for behavioral advertising. – *Richmond Journal of Law & Technology*, Vol 18, Issue 1, 1-50.

27. Koops, B. J. (2014). The trouble with European data Protection law. – *International data privacy law*, Vol 4, Issue 4, 250-261.

28. Lynskey, O. (2014). Deconstructing data protection: the added value of a right to data protection in the EU legal order. – *International & Comparative Law Quarterly*, Vol 63, Issue 3, 569-570.

29. Mayer-Schonberger, V.; Padova, Y. (2016). Regime change: Enabling big data through Europe's new data protection regulation. – *Columbia Science and Technology Law Review*, Vol 17, Issue 2, 315-335.

30. Politou, E., Alepis, E., & Patsakis, C. (2018). Forgetting personal data and revoking consent under the GDPR: Challenges and proposed solutions. – *Journal of Cybersecurity*, Vol 4, Issue 1, 1-20.

31. Rubinstein, I (2013). Big data: the end of privacy or a new beginning? – *International Data Privacy Law*, Vol 3, Issue 2, 74-87.

32. Spiekermann, S., Acquisti, A., Böhme, R., & Hui, K. L. (2015). The challenges of personal data markets and privacy. – *Electronic markets*, Vol 25, Issue 2, 161-167.

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

34. Zarsky, T. Z. (2016). Incompatible: the GDPR in the age of big data. – *Seton Hall L. Rev*, 47, 995-1020.

35. Zuiderveen Borgesius, F. J., Kruikemeier, S., Boerman, S. c., & Helberger, N. (2017). Tracking walls, take-it-or-leave-it-choices, the GDPR, and the ePrivacy regulation. – *Eur. Data Prot. L. Rev*, 3, 359.

EU and international legislation

36. Charter of Fundamental Rights of the European Union, OJ C 326, 26.10.2012, 391-407.

37. Directive 2002/58/EC of the European Parliament and of the Council 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), OJ L 201, 31.7.2002, 37-47.

38. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data OJ L 281, 23.11.1995, 31-50.

39. European Convention on Human Rights, Council of Europe, 1950.

40. Proposal for a regulation of the European parliament and of the council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), 10.1.2017.

41. Regulation (EU) 2016/697 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 on such data and repealing Directive 95/46/EC (General Data Protection Regulation) OJ L 119, 4.5.2016, 1-88.

Court decisions

42. Court decision, 9.11.2010, *Volker und Markus Schecke GbR/Hartmut Eifert v. Land Hessen* C-92/09 and C-93/09 (Joined Cases), EU:C:2010:662.

43. Court decision, 5.5.2011, *Deutsche Telekom AG v Bundesrepublik Deutschland*, C-543/09, EU:C:2011:279.

44. Court decision, 8.4.2014, *Digital Rights Ireland Ltd*, C-293/12 and C-594-12 (Joined cases), EU:C:2014:238.

45. Court decision, 13.5.2014, *Google Spain*, C-131/12, EU:C:2014:317.

46. Court decision, 29.7.2019, *Fashion ID*, C-40/17, EU:C:2019:629.

47. Court decision, 1.10.2019, *Planet49*, C-673/17, EU:C:2019:801.

Opinions of Advocate Generals

48. Opinion of Advocate General, 17.6.2010, C-92/09 and C-93/09 (Joined Cases), *Volker und Markus Schecke GbR/Hartmut Eifert v. Land Hessen*, EU:C:2010:353.

49. Opinion of Advocate General, 21.3.2019, C-673/17, *Planet4*, EU:C:2019:246.

Other sources

50. Article 29 Working Party, Guidelines on Consent under Regulation 2016/679, (2017). Accessible: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051, 20 February 2020.

51. Article 29 Working Party, Opinion 03/2013 on purpose limitation. Accessible: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf, 20 February 2020.

52. Communication from the Commission –Towards a thriving data-driven economy. COM (2014)442 final. Accessible: https://ec.europa.eu/digital-single-market/en/news/communication-data-driven-economy, 28 March 2020.

53. ENISA (2015) The European Union Agency for Network and Information Security Privacy by design in big data – An overview of privacy enhancing technologies in the era of big data analytics. Accessible: https://www.enisa.europa.eu/publications/big-data-protection, 28 March 2020.

54. European Data Protection Board (2019). Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities. Accessible: https://edpb.europa.eu/sites/edpb/files/files/file1/201905_edpb_opinion_eprivacydir_gdpr_interplay_en_0.pdf, 26 March 2020.

55. The European Commission (2019). Accessible: https://ec.europa.eu/info/sites/info/files/data-protection-factsheet-sme-obligations_en.pdf, 24 March 2020.

56. Ustaran E. (2018), Cookie Consent Is the New Panic – [web article]. Accessible: https://www.hldataprotection.com/2018/07/articles/international-eu-privacy/cookie-consent-is-the-new-panic/, 8 April 2020.

Appendix 1. Non-exclusive licence

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

I Sara Rasilainen (10.03.1996)

1.Give Tallinn University of Technology a permission (non-exclusive licence) to use free of charge my creation Valid consent and purpose limitation principle under the EU General Data Protection Regulation, supervised by Tatjana Evas,

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

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

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

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

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