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

Mikko Ilmari Iiskola

Data Protection issues of collecting and processing Health data – in the light of the GDPR

Bachelor's thesis
HAJB08/17 - Law, European Union, and International Law

Supervisor: Thomas Hoffmann, PhD

Tallinn 2021

I hereby declare that I have compiled the thesis independently
and all works, important standpoints and data by other authors
have been properly referenced and the same paper
has not been previously presented for grading.
The document length is 8531 words from the introduction to the end of conclusion.

Mikko Ilmari Iiskola ……
(signature, date)
Student code: 183953HAJB
Student e-mail address: mikko.iiskola@hotmail.com

Supervisor: Thomas Hoffman, PhD:
The paper conforms to requirements in force

……
(signature, date)

Chairman of the Defence Committee:
Permitted to the defence
……
(name, signature, date)

TABLE OF CONTENTS

ABSTRACT

The ultimate purpose of this thesis is to research the fundamental impacts that the European Union's General Data Protection Directive (GDPR) has on the collecting and processing of the GDPR's special categorized data concerning health. The objective of this thesis is to research how the fundamental structure of the GDPR can be implemented to data processing and collecting of different systems concerning health data and whether it does address the significant data security issues. The viewpoint of Big Data systems, eHealth systems, legally allowed reasons for data collecting and processing, and cross-border data transfers are studied in the light of the GDPR to achieve a complete understanding of the current situation of legal issues in health data protection.

To achieve a well-analyzed understanding of the major impacts of the GDPR for health data protection, this thesis has its primary focus on three research questions. To guarantee that this research's standards, aims, and objectives have been satisfied, qualitative empirical research methods have been used.

In the introduction, the research topic and the research questions are introduced. In the first chapter, the reader will be provided the GDPR's objectives to provide a high level of data protection for individuals. The second part consists of an analysis of the GDPR's implementation on electronic health data collecting and processing systems. The third chapter highlights the major issues of data sharing to third parties in and outside of the EU borders. The final chapter will present the main findings and conclusions of this thesis.

Keywords: GDPR, health, Big Data, data protection, EU

1. INTRODUCTION

There has been a vast amount of changes in the European Union (EU) data protection methods. The General Data Protection Regulation (GDPR) was officially enforced in 2018, which replaced and repealed the 1995 Data Protection Directive in 2018. Unlike the previous Directive, the GDPR is directly enforceable in all EU Member States and should achieve immediate and thorough legislative harmonization.

In this thesis, the fundamental changes for the European Union data protection rules, under the GDPR are presented in the light of data concerning health. One of the most critical aspects of the GDPR in the field of data protection in healthcare is the element of sensitive data. The personal data controllers are obligated to implement higher security measures and ensure a high quality of security to minimize the chance of a personal data breach.[1] In the GDPR, data concerning health is specified as a special category of data described as "sensitive data," requiring extra careful protection. In healthcare, the data is collected and processed in sufficiently vast amounts. Under the GDPR, the data collectors are considered to be organizations collecting personal information from individuals, which are referred to as data subjects. A Data processor is a natural or legal person, which processes personal data. The Data processor can be the collector itself or a different organization that processes the data on behalf of the data collector.

The concept of Big Data refers to a large volume of data, structured and unstructured. The amount of Big Data collected and stored in the field of healthcare is vast but also crucial for the field to develop and treat patients more effectively. It also works as a tool for organizations to direct their marketing towards potential customers, which is one of the main reasons for the possible misusage of personal data. Unfortunately, healthcare data, among other "sensitive data," is facing security issues on a vast scale. The growing threat of data breaches and misusage of sensitive data are some of them. The means and methods of data processing and collection may

[1] Katulić T., Protrka, N. (2019) Information Security in Principles and Provisions of the EU Data Protection Law, *2019 42nd International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*, 1219-1225, Opatija, Croatia, IEEE

breach the data protection rules of the European Union. It is vital that the clients' private data are being protected by harmonized EU legislation across the Member States and beyond.

The purpose of this graduation thesis is to research the significant effects that the European Union's General Data Protection Regulation (2018) has on the implementation on the data collection and processing methods of special categorized data concerning health. This thesis investigates the typical structure of what measures and regulations do the GDPR offer in the protection of data concerning health. The concept of Big Data in health data is focused in this thesis since it plays a major part in the health data collection, storage, and procession. The research also focuses on investigating how the processing of data concerning health legally differs from data processed in other contexts. As a research method, academic articles, journals, and other sources have been researched with the relevant case law of the European Court of Justice. One of the main objectives for the European Union legislation authorities is to achieve harmonized data protection across the Member States and beyond. There are very strict regulations concerning the special categorized sensitive data in the GDPR. Its implementation on Electronic Health Records (EHR) and Mobile Health Applications are both focused on, as an example, to help to find an answer whether the GDPR offers enough protection for the data subjects when organizations are processing vast amounts of sensitive data.

Another significant issue of data concerning sensitive data is the data sharing and data breaches involving third parties, which can be, for instance, third-party companies, healthcare organizations, and countries all around the world. Cross-border health data transfer is a modern and growing challenge due to the nature of the European Union principle of free movement. However, where the data protection gets tricky is related to data flows and transfers outside the borders of the EU. In order to address the situation, GDPR offers systematic possibilities in terms of anonymization and pseudonymization in order to prevent the threat of data breaches and misusage. However, it is arguable if the GDPR does provide enough adequate provisions to tackle challenges concerning sharing data concerning health with third parties or countries in and outside of the EU's borders. To what extent can the GDPR be legally and effectively enforced while there are issues related to the scope of EU legislation outside the EU's borders?

2. GDPR's effects and obligations on user's data when concerning Big Data systems in eHealth

The revolution of collection and processing of Big Data is a very current, problematic issue concerning the fact that all of the personal data are on the brink of a possible data breach. Particularly electronic health (eHealth) data, since it increases access to sensitive information of the patients and, if processed, is a severe risk for the privacy of individuals and data protection laws. Companies and healthcare organizations are storing, processing, and transferring massive amounts of data to achieve efficient and proper care. Since these organizations are storing and processing sensitive data, securing data from breaches is extremely important.[2] Healthcare organizations must implement security measures with respecting the European Union General Data Protection Regulation. In general, the GDPR regulates the collection, storage, and processing of personal data. (By its nature is linked to a specific natural person.) This includes direct personal identifiers such as full name, national ID number, and indirect identifiers such as phone numbers, IP addresses, or photos. eHealth data of patients are not commonly regarded as *anonymous* since the data does include personal identifiers. Thus, eHealth data of patients do fall in the scope of GDPR (Recital 26).[3] Every organization must know what personal health data they do have, its reason, the reason for collection, and how the collection is performed. Also, it is essential to know how the health data are processed.[4]

The GDPR does define some legal, organizational, and technical requirements for processing personal data. Firstly, the GDPR states that the processing of personal data does require that the subject of the data has given its consent. The consent given must be specified to justify its specific purpose for data processing. Article 5 of the GDPR states that personal data must be collected and processed for a "specific, explicit and legitimate" purpose.[5] It should not be further processed in an incompatible way with original purposes. Often the analysis of Big Data involves usage which neither the organization collecting data nor the data subject considered at

[2] Abouelmehdi, K., Beni-Hssane, A., Khaloufi, H., Saadi, M. (2017) Big data security and privacy in healthcare: A Review, Procedia Computer Science, Volume 113, 73-80, Elsevier
[3] Gruschka, N., Mavroeidis, V., Vishi, K., Jensen, M. (2018) Privacy Issues and Data Protection in Big Data: A Case Study Analysis under GDPR, *2018 IEEE International Conference on Big Data (Big Data)*, 5027-5033, Seattle, WA, USA, IEEE
[4] Almeida Teixeira, G., Mira D Silva, M., Pereira, R. (2019) The critical success factors of GDPR implementation: a systematic literature review, Digital Policy, Regulation and Governance, Vol. 21 No. 4, pp. 402-418, Emerald
[5] General Data Protection Regulation, 2016/679, §5

the moment of data collection.[6] In order to follow the GDPR specification rule, organizations collecting and processing Big Data must inform their data subjects of the possible forms of data processing *in futuro* and take great care not to exceed the permitted level of data processing.[7] The limitation explained *supra* is difficult since the health data processing organizations should tailor their practices to comply with the GDPR.

Data minimization is another principle that generally means limiting the collection, storage, and usage of personal data to the relevant extent and not more than necessary for carrying out the purpose.[8] When the data minimization principle is respected, data processors have fewer opportunities to exploit the data protection rights of the data subjects. With fewer data available, controllers will be unable to violate their client's or user's privacy. The data minimization requirements did feature in the 1995 Data Protection Directive. However, the enforcement of the GDPR did expand the reach of the principle of data minimization. Personal data should be "limited to what is necessary," according to the GDPR. It is a clear indication for data controllers to minimize data at their data practices.[9] Directly the term "Big Data" is not addressed by the GDPR, and these are not always compatible. For example, Big Data collection relies on data analysis for a massive amount of data, which can be contradictory with the principle of *data minimization*. Patients whose data is processed have given consent for a particular purpose according to the GDPR regulations. If Big Data is being processed, great care must be taken to follow the regulations of the GDPR.[10] Furthermore, the GDPR does offer exceptions that might enable some limited Big Data monitoring by pseudonymization, which refers to technological and statistical safeguards without the possibility to identify the data subjects. However, diligent applying of *data minimization*, as explained *supra*, limits the utility and benefits of processing Big Data since removing identifiers, the potential quality of the results of data processing may be undermined.[11]

The specific legal rules governing decision-making processes are set forth by the GDPR Article 22. The decision-making processes in hand are both fully automated and considerably affect individuals, for instance, recruiting or credit applications. In this provision, the individual is

[6] Zarsky, T. Z. (2017). Incompatible: The GDPR in the age of big data. *Seton Hall Law Review, 47(4),* 995-1020, HeinOnline
[7] *Ibid.*, 1006
[8] Almeida Teixeira, G., Mira D Silva, M., Pereira, R. (2019), *supra nota* 4
[9] Zarsky, T. Z. (2017), *supra nota* 6, 1010.
[10] Gruschka, N., Mavroeidis, V., Vishi, K., Jensen, M. (2018), *supra nota 3, 2.*
[11] Zarsky, T. Z. (2017), *supra nota* 6, 1066.

provided with the right not to be subjected to these processes. Furthermore, this general rule includes some exceptions where such automated decision-making is not allowed, for instance, unconscious data subject. The member states of the EU are able to monitor such a process. It will *de facto* be allowed if deemed necessary to enter into a contract. Such methods could help in order to detect fraudulent activity in automated processes.[12]

Consequently, when interpreting the rights of the data subject in this manner, the GDPR does provide some important rights when facing automated decisions. Firstly, an individual has a right to "obtain human intervention" and "contest the decision." Secondly, data subjects must receive access to background data and be informed of their existence in data processing with the relevant information. There are several arguments related to these rights. At first, when faced with important decisions, a human should be treated as having a human decision-maker address his personal matter. Secondly, *de facto,* these automated processes unfold without presenting sufficient perceptions that those affected by it impair the right to "due process."[13] The processing of big data is directly impacted by Article 22 of the GDPR since it prevents automated analysis, which undermines the utilization of Big data. In addition, if even some of the exceptions provided by the article are met, for instance, the call for human response, the Big Data process must be able to interpret and be explained for the data subjects.[14] In a way that he or she understands. The GDPR does show some important marks that it does reject Big Data. The signal of distrust towards automated processes is notable. This rule could probably make organizations to change their technological structures and business models in order to comply with this rule. In practice, the provision could be avoided by using minimal human interaction since then the decision would not be "solely" automated and would not fall into the scope of this article.[15]

The GDPR Article 9 does prohibit the processing of "special categories" data which does include so-called "sensitive data," including data concerning health.[16] The processing of such data is still possible in terms of explicit consent or specific exceptions. Nevertheless, the GDPR provides a list of general and specific exceptions that allow the processing of sensitive data, which is

[12] *Ibid, 1015.*
[13] *Ibid*, 1017.
[14] *Ibid*, 1017.
[15] *Ibid*, 1016.
[16] General Data Protection Regulation 2016/679, §9

especially important in the field of health data. The idea of special categorizing data constitutes all the categories that individuals consider to be the most private. GDPR has developed the protection of several categories by expanding their definitions. In the context of "health," recital 35 of the GDPR states that the category of "health data" should include various factors, mentioned such as "medical history" and "disease risk."[17]

2.1. The GDPR's obligation towards individual's sensitive data processing

Nowadays, the amount of personal data collected and processed is vast. One of the essential GDPR Regulations can be found in Article 5 since it states that it is not allowed to keep personal data longer than necessary and without altering the original purpose. This is a crucial element when debating patient data safety since it prevents possible misusage of sensitive personal data. Assuring that data controllers comply with the GDPR's purpose limitation principle, it would allow data subjects to maintain at least some control over their personal information, theoretically.[18]

Legally and in practice, it has been desired that data subjects are able to have some kind of control over their personal data.[19] However, this cannot be seen as an objective of the GDPR since the GDPR does more to address the data controller's obligation to collect no more than the minimal amount of data required for a certain purpose. Even the GDPR does not address full attention towards data subjects' control, and it does not appropriately address the threats of data breaches. For instance, GDPR requires data controllers to put policies on their website to inform data subjects about privacy risks even though the data subjects do not adequately understand the policies. Also, data subjects should give their consent for data processing. However, in reality, the data subjects do not think of the consequences properly, which leads to *de facto* that individuals simply consent no matter what is being confronted with a consent request.[20] The GDPR does introduce provisions concerning data controllers and data processors. Those who establish personal data are data controllers, while the organizations or individuals processing information on behalf of the controller are data processors. In the light of GDPR, any company

[17] Zarsky, T. Z. (2017), *supra nota* 6, 1012.
[18] Zarsky, T. Z. (2017), *supra nota* 6, 1006.
[19] van Ooijen, I., Vrabec, H.U. (2019) Does the GDPR Enhance Consumers' Control over Personal Data? An Analysis from a Behavioural Perspective. *J Consum Policy* 42**,** 91–107, SSRN
[20] *Ibid*, 92.

that stores the personal data of European citizen is considered as a data controller. The concept of "data concerning health" aggregates all personal data consisting of patients' health information. Article 4 (15) of the GDPR defines "data concerning health" as "personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status."[21]

GDPR does contain references to individual control. For instance, Recital 7 presents that natural persons should have control over their own personal data. The GDPR strives to improve individual's control of data. Articles 13 and 14 of the GDPR regulates that before processing personal data, the subject must be informed about the purposes, data controller's identity, recipients of the personal data, and storage period. Also, the GDPR states that a data controller should provide information about "the existence of automated decision making, including profiling."[22]

The right to data access and portability is stated by Article 20 of the GDPR. It suggests that the data subject has the right to obtain information about the undergoing processing of personal data. The reason for this is to allow individuals to check whether their data is processed by following legal rules. Furthermore, the data controller should be provided information about categories, purposes of processed data, and the right to object to the data processing, according to the GDPR Article 21. (in addition to the information requirements presented *supra*.) *Et cetera.* Also, as stated in Recital 63 of the GDPR, the data controller may provide a secure system that would work as the data subjects' tool to access the data.[23] Consequently, it can be argued that this is a non-binding element. However, it would help data subjects to maximize the advantages of Big Data and the benefit from the value created by the use of their personal data with third parties. For instance, it would help them use the data for private purposes or even share data with third parties in exchange for services. As recital 68 of the GDPR expresses, data portability's primary goal is to strengthen data subjects' control over their data. It would theoretically make the data subjects able to influence how their data is used but also reused. However, the issue is that all personal data cannot be made portable. Article 20 of GDPR presents that only the data that the subject has provided by herself fall *infra* the definition of portable data. For instance, observed

[21] General Data Protection Regulation 2016/679, §4 (15)
[22] Zarsky, T. Z. (2017), *supra nota* 6
[23] Van Ooijen (2019), *supra nota* 19

data, such as location tracking, is left out[24] , which is a very problematic issue when considering, for instance, Mobile Health Applications.

Another aspect of data subjects' control of their own data is the right to erasure. Article 17 of the GDPR states that in situations wherein data processing does not comply with the GDPR, the processing may be seen as unlawful and data subjects should be able to exercise their right to have the data erased. For instance, if the data is no longer necessary for its original purpose, it was collected and processed. *Infra* the GDPR, the data subjects' control of their data has increased, and the right to erasure exists. However, it is still quite unclear what conditions can be seen as unlawful. The right to erasure is still dependent on the EU Member State's drafted freedoms. For instance, the data's erasure is not required when it would be related to unreasonable effort.[25]

2.2. The processing of data in other contexts versus data concerning health - Case-law analysis

As discovered, the data subjects' technical monitor of its data is challenging, if not impossible, after the consent is given and data has been handed over to the data collector. Even though the GDPR does give efforts in order to prevent misusage of data, the fundamental objective of it is to minimize the amount of data being collected for a specific and restricted purpose. The European Court of Justice has played a significant part in order to ensure the implementation of the GDPR to be as effective as possible. *De facto*, in order to understand the effects of the GDPR on person identifiable, sensitive data, in other contexts, it is important to see relevant case law concerning biometric data from 2015. The case is from three years before the GDPR was officially enforced, and the biometric data is nowadays considered also as a "sensitive" special categorized data in light of the GDPR. Article 4 (14) of the GDPR defines biometric data as "personal data resulting from specific technical processing relating to the physical, physiological or behavioral characteristics of a natural person, such as facial images or dactyloscopic data."[26]

[24] *Ibid.*
[25] *Ibid.*
[26] General Data Protection Regulation 2016/679, §4 (14)

This paragraph demonstrates the difference between how the processing of data concerning health may legally differ from the processing of other special categorized data – biometric data. The following case law in hand is the joined cases of C-446/12 to C-499/12. As it comes to the facts as presented in the case, regulation 2252/2004/EC, the Member States of the European Union are required to collect and store biometric data, which includes fingerprints, passports, and other travel documents in order to identify the data subject and verification the authenticity of the documents. However, the data can be stored and used for other purposes such as national security, prevention of a crime, or identification not concerning the certain purposes introduced for the data subject. The applicant refused to provide their fingerprint data due to its nature to breach the Charter of Fundamental Rights of the EU Article 7 (respect for private life) and Article 8 (Protection of personal data).[27] To keep in mind, this case was before the GDPR was enforced, and the case law is primarily used to analyze how the GDPR affects the collection and processing of personal "sensitive data." The most important aspect of this case linked to this thesis is whether there were enough legal grounds for the Member States to guarantee that the biometric data collected will not be processed further than their original purposes.

As mentioned earlier, since the enforcement of the GDPR, biometric data is considered as a special categorized data requiring extra careful protection. When comparing the processing of health data and biometric data, it can be argued that biometric data does offer more elements than data concerning health for implementation of the GDPR's Article 9 provisions to allow its further processing.[28] For instance, necessary reasons of substantial public interest (such as collecting fingerprint data for national security, prevention of a crime, or identification of victims of a disaster) are perhaps more relevant for biometric data since due to the nature of the EU's principle of free movement. To be able to identify individuals' biometric data is more common and practical to support public interests presented *supra* than for data concerning health. However, processing data concerning health for reasons of public interest could be relevant in case of a very specific event, for instance, during the COVID-19 worldwide pandemic. Recital 54 of the GDPR states that "the processing of special categories of personal data may be necessary for reasons of public interest in the areas of public health without consent of the data subject."

[27] Court decision, 16.4.2015, joined cases, C-446/12, C-447/12, C-448/12, C-449/12, EU:C:2015:238
[28] General Data Protection Regulation 2016/679, §9

Consequently, Recital 53 of the GDPR presents that "The Member States should be allowed to maintain or introduce further conditions, including limitations with regard to the processing of genetic data, biometric data or data concerning health. However, this should not hamper the free flow of personal data within the Union when those conditions apply to cross-border processing of such data."[29] The recital is an indication that even the EU's objective is to harmonize data protection legislation across the EU, it does not blindly ignore the possible utility of national legislation when it comes to "sensitive data" such as genetic, biometric, and health data.

Another interesting case law is C-25/7 Jehovan todistajat. Here, The Finnish Data Protection Board followed the decision of the Court, which prohibits the Jehovah's Witnesses Community from collecting and processing personal data (by means of door to door preaching). The Court judged that the collection and processing methods did not follow the rules set out by (the GDPR's predecessor) Directive 95/46/EC Article 3 (2).[30] In this case, the major problem of data protection was within the fact that the Jehovah's Witnesses Community were collecting personal data by making notes while door to door preaching. These notes consisted of personal data that was collected without data subjects' consent and was processed for more than one specific purpose. The information collected may have included even health data (in the form of a medical condition.) It was an insignificant effect that the EU implemented GDPR in their legislative framework. Together with the CJEU, this is another example of their success in developing the European Union data protection.

[29] General Data Protection Regulation 2016/679, Recital 53
[30] Court decision 10.7.2018, Jehovan todistajat, C-25/17, EU:C:2018:551

3. Data safety over eHealth systems

The patients of healthcare have faced a vast amount of changes in their data protection rights with evolved principles of the GDPR. As mentioned *supra*, the GDPR does define data concerning health as "special categorized data." Also, for patients under healthcare, it is an important aspect that the GDPR does define personal data as any complex information (physical, genetic, mental, cultural, social, *et cetera*) that can be utilized to identify a person directly or indirectly. Since the GDPR entered into force, even IP address information and cookies are considered as personal data if they can be used to identify a person.[31] These types of categorized data are extra carefully protected and are in importance for the field of healthcare. The procession of Big Data in the nature of sensitive data and data concerning health poses legal challenges since the personal nature of the information is confined. These legal challenges include the risk of endangered privacy, personal data autonomy, and effects on public demand for transparency, trust, and fairness when collecting and processing Big Data. Notably, the significant issues endangering Big Data in healthcare are resulting from inappropriate infrastructures for data storage.[32] This part of the thesis illustrates the effects and objectives of the GDPR in eHealth systems such as Mobile Health Applications and Electronic Health Records. The growing usage of smartphone applications has wakened up legal issues. Not only the patient healthcare applications of healthcare organizations but also the mobile health applications of other companies (Google, Samsung, Apple) that are collecting sensitive data can be considered as severe threats to individual's data privacy.

[31] O.P. Stan, L. Miclea, (2019) New Era for Technology in Healthcare Powered by GDPR and Blockchain, Springer
[32] Pastorino, R., De Vito, C., Migliara, G., Glocker, K., Binenbaum, I., Ricciardi, W., Boccia, S. (2019) Benefits and challenges of Big Data in healthcare: an overview of the European initiatives, *European Journal of Public Health*, Volume 29, 23–27, Oxford University Press

3.1. Mobile Health Applications (mHealth apps)

Smartphones have radically changed the interaction with mobile devices and the information exchanged. Since there are a vast amount of sensitive data collected by different application providers, it should be expected that the well-known security and privacy guidelines and legally binding data protection provisions are being followed to ensure data privacy and the clients' safety. Nevertheless, many applications processing sensitive data often fail to provide regular data protection. This is due to either improper implementations or poor design choices.[33]

After recognizing the fact where the problems are arising legally in this area, it should interpret the GDPR's impact on Mobile Health Applications. There are some fundamental changes that are designed to protect the user at the moment of interaction with the application. One of them is the standard regulations of privacy policies and special data categories. Another essential impact the GDPR presents, as mentioned earlier in this thesis, is that health data or biometric data is considered as sensitive data and a "special categorized data" in light of the GDPR. According to the GDPR Article 12, information should be presented briefly, transparent, comprehensive, and easily accessible form, using clear and plain terms. For example, mobile privacy policies and the extra information about the terms and conditions can begin with an icon, label, picture, or link. That will lead to the screen with major points of terms and conditions and privacy policy. In this short form of notice, a link to the full privacy policy should be accessible. Also, the privacy policy should be visible at all times via an icon while the application is in user interaction. Another change provided by GDPR's Articles 4 and 22[34] is that when users are required to make a decision, should the consent be given to the collection of personal information, there must be a clear, specific button or include targeted information. Also, when the user consent is given, there should be one consent given per one data collection purpose, according to Article 6 of GDPR.[35]

When it comes to the privacy settings, a user must now have access to a dashboard where the control of their privacy settings is possible. The tools should be made easily accessible with

[33] Papageorgiou, A., Strigkos, M., Politou, E., Alepis, E., Solanas, A., Patsakis, C. (2018) Security and Privacy Analysis of Mobile Health Applications: The Alarming State of Practice, in *IEEE Access*, vol. 6, 9390-9403
[34] General Data Protection Regulation 2016/679, §4 & §22
[35] General Data Protection Regulation 2016/679, §6

explanations of certain choices. The permissions user has already given must now be visible, and there should be a possibility to edit them. The applications should have a list of permissions, and each of them must have a description of their effects on privacy. Particularly important with sensitive data associated with mobile health applications. Furthermore, Article 17 of the GDPR presents that users should now have the opportunity to monitor their own profile and delete it if wished.[36]

As presented, the GDPR's approach towards Mobile Health Application providers, which are also the data collectors and processors, has been effective. In my own experience, most of the applications are fulfilling the requirements and elements presented in this chapter of the thesis. The applications are much more user-interface friendly when it comes to data privacy and security. However, the real question is can the Mobile Health Application services could be really trusted when it comes to data protection. Designing the applications to "feel" more "secure" for the users it may lure the users into giving away more sensitive data as they would have before. Then there is the aspect of cross-border data transfer, which is very applicable to mHealth apps since many of the service providers are big companies operating outside of the European Union. More research and discussion on cross-border data transfer can be found in Chapter 3.2. of this thesis.

3.2. Electronic Health Records

Electronic Health Records (EHR) store a massive amount of structured data information consisting of diagnostics, laboratory tests, medication, and ancillary clinical data. Processing EHR can be an effective tool for improving clinical research or help with other healthcare challenges.[37] A large amount of data in Electronic Health Records are represented by private health information, and its owner should govern it. The GDPR establishes requirements for data control and also states some obligations for healthcare systems as data protectors. EHRs are collected and processed by public and private organizations to utilize them for medical practitioners and researchers. Since secondary uses and misuses of data are an issue that was wished to address when GDPR was adapted. In healthcare, the GDPR does serve a dual purpose.

[36]J. Muchagata, A. Ferreira, (2018) Translating GDPR into the mHealth Practice *2018 International Carnahan Conference on Security Technology (ICCST)*, Montreal, QC, Canada, 2018, 1-5, IEEE
[37] Andreu-Perez, J. Poon, C. C. Y., Merrifield, R. D., Wong, S. T. C., Yang, G. (2015) Big Data for Health, in *IEEE Journal of Biomedical and Health Informatics*, vol. 19, no. 4, 1193-1208, IEEE

Firstly, its objective is to strictly prevent misusage of personal data in the private and public sectors. Secondly, by keeping in mind data privacy, it does facilitate access to personal data as a necessary requirement for research purposes.[38]

[38] Forcier, M., Gallois, H., Mullan, S., & Joly, Y. (2019). Integrating artificial intelligence into health care through data access: Can the GDPR act as beacon for policymakers?. *Journal of Law and the Biosciences, 6(1),* 317-335.

4. GDPR implementation for personal data collecting and processing third parties

The organizations collecting, processing, and utilizing personal health data must comply with the GDPR. During the time when GDPR has implemented, the major challenge for companies was a lack of awareness and understanding of the forthcoming changes and requirements presented by the GDPR.[39] Compared to the old Directive 95/46/EC, GDPR offers evolved general provisions and principles and transparency and modalities. Furthermore, the GDPR does govern extended territorial scope for the processing of personal data. This basically means that the GDPR applies to the data controllers or processors that are not established in the EU if they offer their operations or monitor the data subjects in the EU. Besides, GDPR presents specific definitions that are relevant and important in terms of implementing and complying with the GDPR to companies operating with personal data. These additions include transparency of data processing, accountability, and processing which does not require identification. GDPR further elucidates some already existed principles such as the data minimization principle, conditions for consent, and criteria for lawful processing.[40]

In Article 5(2) and Article 25 of the GDPR, the principle of accountability refers to data controllers' requirements to adopt a dynamic data protection approach. Data processors and controllers must implement appropriate technical and organizational standards to ensure that data processing complies with the GDPR.[41] Since the GDPR provides unpolished measures to fulfill the data controller’s obligations, it consequently makes those measures dependent on nature, scope, context, and purposes of the processing at hand. The principle of accountability does offer a view that the GDPR is bound to promote a controller-based or case-sensitive approach to data protection.[42]

[39] Tikkinen-Piri, C., Rohunen, A., Markkula, J. (2018) EU General Data Protection Regulation: Changes and implications for personal data collecting companies, Computer Law & Security Report, Elsevier
[40] *Ibid.*
[41] *Ibid.*
[42] *Ibid.*

The penalties for breach of the GDPR are notable. In a tiered approach to penalties, organizations can face a hefty fine for breaches of the principles of the GDPR. These penalties can apply to data controllers and data processors, which means that these (cloud) service providers are not exempt from GDPR.[43] With the penalties becoming more severe in case of breaching the GDPR, theoretically, it is more likely that the organizations collecting and processing personal data intend to comply with the GDPR and avoid breaching data protection rules. However, the issue here is that the complete tracking of data flows is technically almost impossible.

4.1. Anonymisation and Pseudonymization and personal data breaches

The term anonymization refers to several techniques to reduce the identifiability of individuals. *Anonymisation* is a process where identifying information is manipulated in order to prevent data subject identification.[44] However, the GDPR does not apply to anonymous data or does not mention any specific *anonymization* methods. It results in greater flexibility in the legislation and enables data protection authorities to decide whether anonymizing methods should apply.[45] The new definition presented by GDPR to the term *pseudonymization* refers to personal data processing. In the EU Article 29 Working Party (2014), guidance was produced that *pseudonymization* is not a method of *anonymization,* and it simply reduces the linkability of a dataset with the original data subject's identity. The data cannot be attributed to a particular data subject without any further information, which requires holding such additional information independently from the data subject to technical and organizational measures.[46] According to the GDPR, the purpose of the application of *pseudonymization* is the advanced possibility to reduce the risks to the data subjects and help data controllers and processors to satisfy data protection section obligations. *Pseudonymization* faces the issue of re-identification of the data subject. According to the GDPR, for re-identification, there must be legitimate reasons. Consequently, re-

[43] Dove, E. S. (2019) The EU General Data Protection Regulation: Implications for International Scientific Research in the Digital Era., Journal of Law, Medicine & Ethics, 46(4), Cambridge University Press
[44] Esayas S. Y. (2015) The role of anonymisation and pseudonymisation under the EU data privacy rules: beyond the 'all or nothing' approach", in European Journal of Law and Technology
[45] Dove, E. S. (2019), *supra nota* 43.
[46] Tikkinen-Piri, C., Rohunen, A., Markkula, J. (2018) *supra nota* 39.

identification must fall in the information data processer passes to the data subject, according to the GDPR Article 13.[47]

Along with the principle of data concerning health, GDPR includes binding corporate rules that refer to personal data protection policies concerning controllers or processors for personal data transfer to third countries for organizations to utilize the data. This leads to the principle of Personal data breach, referring to a breach of data security that can result in accidental or illegal destruction, loss, modification, unauthorized exposure of personal data, or unauthorized access to the data stored or processed.

4.2. Cross-border health data transfer and processing

With people increasingly making personal information available globally using modern technologies, data is not limited to countries' borders. Data can be transferred, stored, and processed around the world. GDPR does offer strict rules when it comes to transferring data outside of the EU. The increase of data flows outside of the European Union has set up a growing issue where there is a vast amount of health data stored in the companies' cloud servers. Once the data is in cloud servers, its flow is harder to trace. If privacy policies are being analyzed, usually the data can be shared with "other partners." The problem is that the "other partners" are unknown, and the data if transferred, can possibly be stored in their cloud server, and the difficulty level of tracing data increases.[48] Article 3 of the GDPR presents that the processing of personal data of data subjects in the EU by a controller or processor is not established in the EU if the processing operations are related to offering goods or services or monitoring data subjects' behavior. One objective of the GDPR is to provide a similar data protection level for data subjects in the EU regardless of the data being processed outside the EU. The meaning is that the companies and organizations, whether or not established in the EU, processing health data of data subjects *intra* the EU need to comply with the GDPR.[49]The lack of transparency regarding the use, location, and storage of the health data is a major issue since the privacy policies are unclear about the third parties and countries. The data flow is difficult to

[47] Bolognini, L., Bistolfi, C. (2016) Pseudonymization and impacts of Big (personal/anonymous) Data processing in the transition from the Directive 95/46/EC to the new EU General Data Protection Regulation, Computer Law & Security Review, Elsevier
[48] Mulder, T., Tudorica, M., (2019) Privacy policies, cross-border health data and the GDPR, Information & Communications Technology Law, Routledge
[49] *Ibid.*

trace since it is unknown who has the data, where the data is stored, and what the intentions are to do with it.

More importantly, the practical determination of jurisdiction seems to be an issue here since, referring to the reasons presented *supra*, it is difficult for data subjects to exercise their rights in case of a data breach. The GDPR states that its scope reaches across the world if EU citizens' are being processed. However, this statement's actual exercise is more difficult since the legal systems in non-EU countries may not recognize or may not have knowledge of the GDPR.[50]

According to the GDPR Article 4 (23), cross border data processing means either "processing of personal data which takes place in the context of the activities of establishments in more than one Member State of a controller or processor in the Union where the controller or processor is established in more than one Member state" or " processing of personal data which takes place in the context of the activities of a single establishment of a controller or processor in the Union but which substantially affects or is likely to substantially affect data subjects in more than one Member State."

The GDPR has restricted cross-border personal data transfer in certain conditions. However, the European Commission has negotiated and can negotiate international agreements in order to continue data flow. In general terms, GDPR sets out the principle that collection and processing of the data that transfers to the country or organization outside the EU's borders comply with the GDPR.[51] The GDPR's chapter five (considers transfers of personal data to third countries or international organizations.) Article 44 of the GDPR "General principle for transfers" states that any data transfer to a third country or international organization is allowed only if the conditions of this chapter are complied with by the data collector or processor. Referring to the GDPR's restricted circumstances through which the GDPR and European Commission may permit data transfer outside the EU to be justified. One of them is transfers made legal on the basis of an adequacy decision. The GDPR Article 45 allows a cross-border data transfer outside the borders of the EU. An adequacy decision can be granted by the European Commission if a certain country meets the required level of data protection. Even though an adequacy decision is favored and commonly the most reassuring basis for data transfer, it has weaknesses. For instance, the

[50] *Ibid.*
[51] Voss, W. (2020). Cross-border data flows, the gdpr, and data governance. *Washington International Law Journal, 29(3),* 485-532.

GDPR is not approved in all countries.[52] Another element is the binding corporate rules which are presented in Article 47 of the GDPR. Intended use is in large organizations transcending national borders that may need to transfer personal data to another country while staying *intra* the organization's own divisions. The organization must meet the requirements of Article 47 of the GDPR and be approved by the relevant data protection authority. However, due to relatively time-consuming, complicated, and expensive investments, the approach of binding corporate rules will not be the best transfer mechanism for health data *nisi* carried out by a huge international organization.[53]

Furthermore, the GDPR provides that the personal data may be allowed to be transferred to that organization. Suppose an organization's loyalty to follow a code of conduct targeted at a specific sector is complying with the GDPR and is approved by the European Commission. May the personal data be allowed to be transferred to that organization. Even if the Code of Conduct provides evidence of an organization to comply with the GDPR generally, it does not possibly show any proof of compliance. In the light of health data, the code of conduct may become the most attractive transfer method. Firstly, it would help to avoid the persistent legal uncertainty *per contra* the more common transfer mechanisms. Secondly, in international transfers, the code of conduct could provide practical certainty in guidance on how the data protection rules, in general, apply in the context of data concerning health.[54]

The relationship between the territorial scope of EU legislation and the rules considering data transfer outside the EU borders is a challenging aspect. As discovered, the main legal issues with the GDPR's and European Union's objective to be effective in order to protect EU data transferred outside the Member States arising from the fact that EU legislation is unfortunately not possible to operate as effective outside of the European Union. This can be explained by the fact that its foundations are in the European Union's legal framework of fundamental rules. For instance, such elements as the rule of law, enforcement of judgments and recognition, independence of judicial system, the data protection acts, and similar essential areas that will not probably work as effectively in third countries.[55]

[52] Phillips, M. (2018) International data-sharing norms: from the OECD to the General Data Protection Regulation (GDPR), Springer
[53] *Ibid.*
[54] *Ibid.*
[55] Kuner, C. (2021) Territorial Scope and Data Transfer Rules in the GDPR: Realising the EU's Ambition of Borderless Data Protection, University of Cambridge, SSRN

In order to explain the relationship of the territorial scope of EU legislation and its implementation outside the borders of the EU, the relevant case law can be researched. In case C-507/17 Google v CNIL, the European Court of Justice judged that Google is not obliged under the EU law to apply the European Union citizen right to be forgotten.[56] The importance of this case is significant since it illustrates perfectly the critical problem of the GDPR cross-border data protection, which is the lack of enforceability of the Regulation with data processors outside the Member States. However, the case also illustrates that the GDPR and EU data protection laws do have sufficient power outside the EU since, due to Court's judgment, Google is required to remove any linkable personal data from internet searches that have been made inside the European Union. According to the opinion of the Advocate General, the internet searches made outside the European Union should be excluded from this certain part of the EU data protection rules.[57]

4.3. Proposals for reform

As discussed, the main difficulty of cross-border data protection is to achieve effective enforceability of the GDPR outside the European Union. This is due to the nature of difficulties in territorial scope of EU legislation and data transfer rules. Mainly, the states and organizations recognizing the GDPR are active on the European market and are in a crosshair of the data protection laws.[58] The European Union's objective should be that the GDPR utilizes every provision it provides relating to its territorial scope and data transfers. The foundations for this are promising and the development to the positive direction should happen during the coming years. Subsequently, more and more organizations acting on the European market should recognize themselves within the European data protection requirements[59], set out by the GDPR.

Firstly, the practice of other GDPR provisions that protects EU data from external threats should be improved, for instance, Article 27 (1) of the GDPR, which obligates non-EU data controllers and processors to appoint a representative, is under-utilized.[60] The European Data Protection

[56] Court decision, 24.9.2019, Google v CNIL, C-507/17, EU:C:2019:772
[57] Opinion of Advocate General Szpunar 10.1.2019, C-507/17, EU:C:2019:15
[58] Klar, M. (2020), Binding effects of the european general data protection regulation (GDPR) on U.S. companies. Hastings Science and Technology Law Journal, *11(2)*, 103-104, HeinOnline
[59] *Ibid.* 104
[60] Kuner, C. (2021), *supra nota 55*, 33

Board (EDPB) and the EU Commission could create an operational market for data protection representatives in the EU. For instance, by investigating the reliability of the data collecting or processing organizations that are offering their services as representatives, to discuss with the data subjects, collectors and processors to gather feedback and analyze practical issues.[61]

Secondly, before any changes are made to the law, unbiased research should be made to establish how the affiliation between the territorial scope of EU legislation and data transfer rules works in practice, and whether it causes problems. Even if any changes should be made through legislation, for transparency and legality, it would not rule out the possibilities from the work of the European Data Protection Board, as long as the EDPB does not compliance with the changes.[62]

Shortly, on very basic terms, what is required to develop the relationship between the EU legislation's territorial scope data transfer rules are the maximum practical utilizing of the current GDPR provisions, practice effective coordination between the parties of the data transfers, to research well the applicability and to follow transparency and legality when making changes to law.

[61] *Ibid.*
[62] *Ibid.*

5. CONCLUSION

To conclude, this thesis illustrates the significant effects that the European Union General Data Protection Regulation provides for data privacy concerns in the field of digital healthcare. The GDPR does offer regulations for data collecting and processing organizations that should work as an adequate base for a higher level of quality of data protection. For the Big Data systems, the GDPR does not comprehensively have any direct regulations or methods to prevent data breaches or misusage in that manner. As found in this thesis, the general objective relevant for Big Data systems is to obligate that the data collectors and processors minimize the data utilized for a certain specific purpose. Subsequently, the GDPR does offer a vast amount of regulations and systematic propositions that can be implemented in relation to Big Data in digital healthcare and other special categorized data.

The general issue arising with discussion, from collecting and processing personal health data, is its sensitive nature. The reason why GDPR has a special categorized data requiring extra careful protection is to protect data *Id est* the most private considered by individuals. Especially in health data, it is vital that patients and users enjoy as high a level of data protection as possible over their data. In addition, an essential element of data protection is to have transparency of personal data after consent is given. The rights to receive information on how and why the personal data is being used and for how long, to be able to monitor the data and to have the possibility to erase the data. The GDPR does not offer enough provisions in order to ensure that the data subjects retain at least some of the rights over the measures presented in the previous sentence. The data protection of personal data and the main elements presented are being somehow satisfied. The GDPR can be generally criticized since it does not offer good enough protection for data subjects' data control. It only focuses on obligating data collectors to gather the minimum amount of data necessary for processing for a particular purpose.

When it comes to eHealth systems, Mobile Health Applications, and Electronic Health Records, the GDPR offers provisions to tackle possible data breach issues. Research in this thesis shows

that the GDPR has offered a significant data protection overhaul in order to make the Mobile Health Applications and Electronic Health Records more private and protected. Unfortunately, the observed data flows are not entirely trackable in order to make sure that the enforcement of the GDPR is practically followed and the "sensitive data" has not flowed to the nets of organizations that can potentially misuse the data—for instance, tracking data. Seemingly, it does not entirely fall in the scope of GDPR, which is very problematic for data protection, especially for Mobile Health Application data protection.

The GPRD's implementation for personal data collecting organizations does meet the satisfactory level to ensure data protection. Generally, the GDPR's provisions are promising. The provisions of the GDPR extend the scope outside the EU to ensure a high level of data protection for EU Citizens. It regulates the methods of how the health data is legally collected and processed. Furthermore, the data controllers and processors must ensure that the methods comply with the GDPR, which means that the GDPR managed to build foundations for better data privacy and protection.

The GDPR does offer a strict structure of rules determining cross-border data transfer. Perhaps the number one aspect of these rules is (as presented earlier) that the EU Citizens should be ensured the same level of data protection whether in or outside of the EU. However, these rules set out by the GDPR are not working as efficiently as they should. Notably, the lack of transparency and the element of uncertainty, and the lack of approval of the GDPR are significant reasons why the GDPR does face insuperable challenges in ensuring high quality of data protection outside the EU. Nevertheless, GDPR offers some systematic proposals and methods to ensure private and safe data transfer. Even though it can be argued how functional they are in practice, the same goes by when interpreting GDPR's provisions that allow the personal data transfer across borders, even it has European Commission's support as a decision-maker. The major issue here is that what does bind the EU legislation and its legal framework to the third parties outside the borders of the European Union. In order to ensure more collective and harmonized data protection, the relationship between the territorial legal scope and EU legislation should be developed even further.

LIST OF REFERENCES

Scientific articles

1. Almeida Teixeira, G., Mira D Silva, M., Pereira, R. (2019) The critical success factors of GDPR implementation: a systematic literature review, Digital Policy, Regulation and Governance, Vol. 21 No. 4, pp. 402-418, Emerald

2. Andreu-Perez, J. Poon, C. C. Y., Merrifield, R. D., Wong, S. T. C., Yang, G. (2015) Big Data for Health, in IEEE Journal of Biomedical and Health Informatics, vol. 19, no. 4, pp. 1193-1208, IEEE

3. Bolognini, L., Bistolfi, C. (2016) Pseudonymization and impacts of Big (personal/anonymous) Data processing in the transition from the Directive 95/46/EC to the new EU General Data Protection Regulation, Computer Law & Security Review, Elsevier

4. Dove, E. S. (2019) The EU General Data Protection Regulation: Implications for International Scientific Research in the Digital Era., Journal of Law, Medicine & Ethics, 46(4), Cambridge University Press

5. Esayas S. Y. (2015) The role of anonymisation and pseudonymisation under the EU data privacy rules: beyond the 'all or nothing' approach", in European Journal of Law and Technology

6. Forcier, M., Gallois, H., Mullan, S., & Joly, Y. (2019). Integrating artificial intelligence into health care through data access: Can the GDPR act as beacon for policymakers?. Journal of Law and the Biosciences, 6(1), 317-335.

7. Klar, M. (2020), Binding effects of the European general data protection regulation (GDPR) on U.S. companies. Hastings Science and Technology Law Journal, *11(2)*, 103-104, HeinOnline

8. Kuner, C. (2021) Territorial Scope and Data Transfer Rules in the GDPR: Realising the EU's Ambition of Borderless Data Protection, University of Cambridge, SSRN

9. Mulder, T., Tudorica, M., (2019) Privacy policies, cross-border health data and the GDPR, Information & Communications Technology Law, Routledge

10. Papageorgiou, A., Strigkos, M., Politou, E., Alepis, E., Solanas, A., Patsakis, C. (2018) Security and Privacy Analysis of Mobile Health Applications: The Alarming State of Practice, in IEEE Access, vol. 6, pp. 9390-9403

11. Pastorino, R., De Vito, C., Migliara, G., Glocker, K., Binenbaum, I., Ricciardi, W., Boccia, S. (2019) Benefits and challenges of Big Data in healthcare: an overview of the European initiatives, European Journal of Public Health, Volume 29, pp. 23–27, Oxford University Press

12. Phillips, M. (2018) International data-sharing norms: from the OECD to the General Data Protection Regulation (GDPR), Springer

13. Tikkinen-Piri, C., Rohunen, A., Markkula, J. (2018) EU General Data Protection Regulation: Changes and implications for personal data collecting companies, Computer Law & Security Report, Elsevier

14. van Ooijen, I., Vrabec, H.U. (2019) Does the GDPR Enhance Consumers' Control over Personal Data? An Analysis from a Behavioural Perspective. *J Consum Policy* 42**,** 91–107, SSRN *7(4),* 995-1020, HeinOnline

15. Voss, W. (2020). Cross-border data flows, the gdpr, and data governance. *Washington International Law Journal, 29(3),* 485-532.

16. Zarsky, T. Z. (2017). Incompatible: The GDPR in the age of big data. *Seton Hall Law Review, 47(4),* 995-1020, HeinOnline

EU and International legislation

17. Charter of Fundamental Rights of the European Union OJ C 326, 26.10.2012, p. 391–407, art. 7-8.

18. 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, p. 31–50

19. 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, p. 1–88, art. 3-6, 9, 12-14, 17, 20-22, 25, 44-45, 47. Recital no 7, 26, 35, 53-54, 63, 68

Court Decisions

20. Court decision 10.7.2018, Jehovan todistajat, C-25/17, EU:C:2018:551

21. Court decision, 16.4.2015, joined cases, C-446/12, C-447/12, C-448/12, C-449/12, EU:C:2015:238

22. Court decision, 24.9.2019, Google v CNIL, C-507/17, EU:C:2019:772

23. Opinion of Advocate General Szpunar 10.1.2019, C-507/17, EU:C:2019:15

Other sources

24. Abouelmehdi, K., Beni-Hssane, A., Khaloufi, H., Saadi, M. (2017) Big data security and privacy in healthcare: A Review, Procedia Computer Science, Volume 113, pp. 73-80, Elsevier

25. Gruschka, N., Mavroeidis, V., Vishi, K., Jensen, M. (2018) Privacy Issues and Data Protection in Big Data: A Case Study Analysis under GDPR, *2018 IEEE International Conference on Big Data (Big Data)*, pp. 5027-5033, Seattle, WA, USA, IEEE

26. J. Muchagata, A. Ferreira, (2018) Translating GDPR into the mHealth Practice *2018 International Carnahan Conference on Security Technology (ICCST)*, Montreal, QC, Canada, 2018, pp. 1-5, IEEE

27. Katulić T., Protrka, N. (2019) Information Security in Principles and Provisions of the EU Data Protection Law, *2019 42nd International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*, pp. 1219-1225, Opatija, Croatia, IEEE

28. O.P. Stan, L. Miclea, (2019) New Era for Technology in Healthcare Powered by GDPR and Blockchain, Springer

Appendix 1. Non-exclusive licence

A non-exclusive licence for reproduction and publication of a graduation thesis[163]

I Mikko Ilmari Iiskola

1. Grant Tallinn University of Technology free licence (non-exclusive licence) for my thesis Data Protection issues of collecting and processing Health data – in the light of the GDPR,

supervised by Thomas Hoffmann PhD,

1.1 to be reproduced for the purposes of preservation and electronic publication of the graduation thesis, incl. to be entered in the digital collection of the library of Tallinn University of Technology until expiry of the term of copyright;

1.2 to be published via the web of Tallinn University of Technology, incl. to be entered in the digital collection of the library of Tallinn University of Technology until expiry of the term of copyright.

2. I am aware that the author also retains the rights specified in clause 1 of the non-exclusive licence.

3. I confirm that granting the non-exclusive licence does not infringe other persons' intellectual property rights, the rights arising from the Personal Data Protection Act or rights arising from other legislation.

---

11 May 2021

[63] *The non-exclusive licence is not valid during the validity of access restriction indicated in the student's application for restriction on access to the graduation thesis that has been signed by the school's dean, except in case of the university's right to reproduce the thesis for preservation purposes only. If a graduation thesis is based on the joint creative activity of two or more persons and the co-author(s) has/have not granted, by the set deadline, the student defending his/her graduation thesis consent to reproduce and publish the graduation thesis in compliance with clauses 1.1 and 1.2 of the non-exclusive licence, the non-exclusive license shall not be valid for the period.*