UNIVERSITY OF TARTU
SCHOOL OF LAW
Department of Public Law

Kärt Raud

DATA PROTECTION IN mHEALTH

Master's Thesis

Supervisors
Mati Kaalep
Dr. Helen Eenmaa-Dimitrieva

Tartu
2016

TABLE OF CONTENTS

INTRODUCTION

Usage of smartphones and other smart devices has become common in our everyday lives. What makes such devices 'smart' is the fact that a major part of the user experience is based on the use of software applications. A multitude of different applications or 'apps' are available for various purposes and all of them operate on the basis of processing certain type of information or 'data'. Such data might either be inserted by the users, or collected via different monitoring devices transferring the data to the apps.

One specific category of apps consists of those used for health and medical purposes. Some health apps are rather simple and used for storing and analysing information which the user of the app provides, for example an app that makes it easy to keep track of the health parameters the user inserts. Other apps are connected with different technical devices, often called wearable devices, which use sensors in order to monitor the person's health parameters in real time and precise manner. These include, for example, a smartphone with an internal pedometer to track the steps taken during a day, or a specific device that is able to meter the glycose level of a diabetic. All these apps and devices form a part of the conception of mobile health or 'mHealth'.

mHealth is a sub-segment of eHealth and covers medical and public health practice supported by mobile devices. It includes the use of mobile devices for health and well-being services and information purposes as well as mobile health applications.[1] Predictions suggest that by 2017, 50% of all smartphone and tablet users will have accessed an mHealth application and the number of available mHealth applications will be approaching 1 million, with 62 different app stores functioning as software distributors.[2]

One of the key elements of mHealth is its potential to allow the establishment of treatment relationships between a patient and a physician who are not dependent on the geographical location.[3] However, this concept falls rather under the notion of telemedicine[4] and the issues

[1] mHealth – Digital Single Market. European Commission. - https://ec.europa.eu/digital-single-market/en/mhealth (28.04.2016).

[2] Mobile health app market report 2013–2017: The commercialization of mHealth. Research2Guidance. - http://www.researchandmarkets.com/reports/2497392/mobile_health_app_market_report_20132017 (5.02.2016), p 15.

[3] E. Mantovani, P. Quinn. mHealth and data protection – the letter and the spirit of consent legal requirements. - International Review of Law, Computers & Technology, 2014, 28:2, 222-236, p 222.

[4] Telemedicine is the use of medical information exchanged from one site to another via electronic communications to improve a patient's clinical health status. See: What is telemedicine? – American

regarding that kind of treatment relationship will not be analysed in this thesis. This thesis will focus on another aspect of mHealth, which concerns a situation when an enormous amount of data is collected through the apps. The collection and processing of data from the users of the apps have its benefits. By having a constant access to one's own health data, the individuals are more empowered to keep track of their health status. In addition, combing the data collected through the apps could lead to new discoveries regarding diseases and health management could be made which would benefit the whole society.

Despite the advantages of using mobile devices for health monitoring, there are also several risks and problems. Large part of the data that are processed in the apps falls under the notion of personal data. Processing personal data triggers the applicability of the data protection rules in order to protect the persons' right to privacy. The risks arising with the use of mHealth regarding the data protection will be the main focus in this thesis.

In Estonia, data protection is regulated on national level under the Personal Data Protection Act[5]. Nevertheless, for the purposes of more extensive analysis and practical use, the regulative base for this thesis shall be the law of the European Union. Over half the countries in the world have a data protection law and most are strongly influenced by the European approach.[6] The right of protection of personal data is a fundamental right under Art 8 of the Charter of Fundamental Rights of the European Union.[7] However, already before the Charter of Fundamental Rights of the European Union was adopted, the right for protection of personal data could be derived from Art 8 of the European Convention on Human Rights.[8] At the EU level, the need for separate data protection act arose during the 1990s. Free movement of goods, capital, services and people within the internal market required the free flow of data, which could not have been realised unless the member states could rely on a uniform high level of data protection.[9] Therefore, the Data Protection Directive[10] (hereinafter DPD) was

---

Telemedicine Association. - (http://www.americantelemed.org/about-telemedicine/what-is-telemedicine#.VyUgylaLRmM) (28.04.2016).

[5] Personal Data Protection Act. - RT I 2007, 24, 127

[6] G. Buttarelli. The EU GDPR as a clarion call for a new global digital gold standard. – International Data Privacy Law, Guest Editorial. - http://www.oxfordjournals.org/our_journals/idpl/featured.html (28.04.2016)

[7] Charter of Fundamental Rights of the European Union. - OJ C 326, 26.10.2012, p. 391–407.

[8] European Convention on Human Rights (entry into force 4.11.1950). - http://www.echr.coe.int/Documents/Convention_ENG.pdf

[9] Handbook on European Data Protection Law. Luxembourg: Publications Office of the European Union, 2014, p 17.

adopted in 1996 and is still in force. The DPD became an international standard of data protection by introducing common legal principles and concepts, such as individual control rights, purpose limitation principle, data quality and legitimacy of data processing.[11]

However, since 2010 the need for reform in the field of the personal data protection in the EU has been brought up. To start with, the member states have failed to implement the DPD into their national laws in uniform manner.[12] Furthermore, there was a legal uncertainty concerning how to deal with the significant risks associated with online activity.[13] Subsequently, in January 2012, the European Commission put forward the EU Data Protection Reform.[14] On 14 April, 2016, after prolonged negotiations, the European Parliament adopted two new sets of data protection rules: the General Data Protection Regulation[15] (hereinafter GDPR) and the Data Protection Directive for the police and criminal justice sector[16].

This thesis will analyse if and how the EU current and future data protection framework applies to the field of mHealth. While the usage of mHealth is increasing and the persons are willing to disclose more personal information to the apps, it is crucial to make sure that data

---

[10] 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.

[11] C. Cuijpers, N. Purtova, E. Kosta. Data Protection Reform and the Internet: the draft Data Protection Regulation. - Tilburg Law School Research Paper 2014, No. 3. - http://ssrn.com/abstract=2373683 (05.04.2014), p 1.

[12] For example, see: CJEU 16.10.2012, C-614/10, Commission vs Austria.

[13] W. Kotschy. The proposal for a new General Data Protection Regulation - problems solved? - International Data Privacy Law, 2014, Vol. 4, No. 4, p 274-281, p 274.

[14] Commission proposes a comprehensive reform of data protection rules to increase users' control of their data and to cut costs for businesses. - European Commission Press Release. Brussels, 25 January 2012.- http://europa.eu/rapid/press-release_IP-12-46_en.htm?locale=en (17.04.2016).

[15] The official text of the General Data Protection Regulation has not yet been published in the Official Journal of the European Union at the time of submitting this thesis. Before the voting in the European Parliament, the Council of European Union published a final text of the GDPR on 6 April 2016. All the references to the GDPR in this thesis are made to named text. See: Position of the Council at first reading with a view to the adoption of a Regulation of the European Parliament and of the Council 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). ST 5419 2016 INIT - 2012/011 (OLP). Brussel, 6 April 2016. - http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_5419_2016_INIT&from=EN (1.05.2016).

[16] Position of the Council at first reading with a view to the adoption of a Directive of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA. ST 5418 2016 INIT - 2012/010 (OLP). Brussels, 6 April 2016. - http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_5418_2016_INIT&qid=1462066004286&from=EN (1.05.2016).

protection rules are followed applied unambiguously. The hypothesis of this thesis states that the current data protection framework is not suitable to apply to modern day realities like mHealth. Although, the new GDPR is already adopted, the author of this thesis is in the opinion that the GDPR will not improve the situation regarding the data protection in mHealth. Therefore, the central thesis question is whether the current EU data protection framework is sufficient in order to protect the personal data in the field of mHealth. As a new framework will be in force in two years, the thesis will also examine whether the GDPR will bring any changes to data protection regarding mHealth. Deriving from the central question, the thesis has been divided into three chapters.

The first chapter gives an overview of the concept of mHealth in relation to relevant data protection terms. In order to understand how data protection rules apply in the field of mHealth, it must be clarified how the realities of mHealth are transposed under the data protection rules. It will be described what kind of data is considered as personal data and what is considered as health data. As the classification of mHealth apps or devices under the notion of medical devices might change the applicability of data protection rules, it will be analysed, whether the apps and devices of mHealth could be considered as medical devices. Therefore, the main question of first chapter is whether the data protection terms are suitable in order to apply these to the realities of mHealth.

In the second chapter, the underlying concepts and principles of data protection will be brought out and analysed in the light of mHealth. In the first part, the notion of consent will be described and the possible problems of obtaining consent for processing of personal data will be brought out. In the second part, two of the data protection principles will be chosen – purpose limitation principle and data minimisation principle – and shown if and how the applying of those principles affects mHealth. The main question of the second chapter is whether the traditional data protection requirements are sufficient and clear enough in order to apply them for the protection of personal data in mHealth.

In the third chapter, it will be discussed if and how it is lawful to further use the health data collected in mHealth without the consent of the data subject. If such processing turns out to be lawful, it could seriously harm the persons' right to privacy and undermine their trust in mHealth solutions. The notion of big data will be explained and found whether the data protection principles should apply to big data processing. Then it will be analysed whether big data processing can be concluded without the consent of the data subject by applying the

exceptions on further use. The main question of the third chapter is whether and on what conditions the further use of health data is possible without the user's consent.

In order to answer to the raised questions, the author has used comparative and analytical methods. The analytical method is used to analyse the application of data protection regulations to the concepts of mHealth. The comparative method is used to compare the requirement of DPD and GDPR. Both methods are used throughout the thesis.

In the course of writing the thesis, the author has used the DPD and the GDPR in order to analyse the applicability and comparison of the rules of these laws. To understand the content behind the personal data protection rules, many opinion papers from the Article 29 Working Party[17] (hereinafter the Working Party) have been used, since the Working Party is considered the authority in the European data protection sphere. Moreover, several other opinions on mHealth by different data protection supervisory authorities have been used. As the field of mHealth, and especially the data protection issues relating to it are rather new, academic literature on this topic is relatively limited. However, several identified articles proved useful where the principles of data protection were analysed in the context of mHealth. Some of the standpoints from the articles were contested, while some were used to support the arguments of the author of this thesis.

The keywords taken from the Estonian Subject Thesaurus characterising this thesis are:

- Data protection
- Personal data
- Privacy
- Health data
- Information Technology

[17] Article 29 Working Party is the advisory body set up under the Data Protection Directive who issues opinions and recommendation on topics related to personal data protection.

1. THE CONCEPT OF mHEALTH

1.1 Introduction to Chapter

In order to understand how the data protection rules apply to field of mHealth, firstly, the relevant terms must be made described. The definition of personal data is described in order to move to the special categories of data which enjoy special protection under the data protection rules.

The definition of health data in mHealth apps is more complex as the apps collect various kinds of data which could in combination be considered as health data. The differentiation between regular personal data and health data is extremely important as the breaches concerning health data endanger the person's right to privacy in much more substantial way. It will be brought out what are the criterion for deciding whether the mHealth data could be considered health data.

In addition to different terms and notions of data protection, the definition of medical devices is also analysed. Although the medical devices might seem to be far from the regulation of data protection, actually the determination that an app or a wearable device could be considered as a medical device under the special directive, could change the applicability of the data protection rules to processing.

1.2 Health Data

1.2.1 Definition of Personal Data

Pursuant to Article 2 (a) of the DPD, personal data is defined as information relating to an identified or an identifiable natural person. An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity. Working Party has analysed the concept of personal data in its Opinion 4/2007.[18] According to the Working Party, the definition of personal data in Art 2 (a) of the DPD contains four main building blocks: 'any information', 'relating to', 'an identified or/and

[18] Article 29 Working Party, Opinion 4/2007 on the concept of personal data, adopted on 20th June, WP136.

identifiable' and 'natural person'.[19] These four main elements will be described in more detail on the basis of the Working Party's opinion. In order to understand how these elements should be applied in practice when assessing whether data is considered as personal data, an example will be used. The example set of data is data, which consists of a number of steps taken by a person during one day collected through a specific app[20] on a smartphone.

The first element, term 'any information', refers to the wide interpretation and broad concept of personal data. The nature of the information can be either objective (fact about a certain person) or subjective (opinions or assessments). The content of the information can be any sort of information. The term 'personal data' includes information concerning the individual's private and family life, but also information about the types of activities undertaken by the individual.[21] Considering the format or the medium on which that information is contained, the concept of personal data includes information available in whichever form, be it alphabetical, numerical, graphical, photographical or acoustic.[22] The example of the number of steps fulfils this condition, as it shows the activity of a person. Therefore, even a number on an app, which at first sight might seem to have no value, could be considered as personal data.

The second element is 'relating to' which is important to precisely identify and distinguish the relations/links that matter. In general terms, information can be considered to 'relate' to an individual when it is about that individual.[23] Information relates to an individual if it refers to the identity, characteristics or behaviour of an individual or if such information is used to determine or influence the way in which that person is treated or evaluated.[24] The example of the number of steps fulfils this condition if it is possible to relate the number of steps to a specific person, for example, if only one person has held the smartphone throughout the specific day. The link between the data subject and the data must exist, which in case of mobile apps is relatively easy to identify because apps are usually used to collect information about oneselves.

---

[19] Working Party, Opinion 4/2007, p 6.

[20] The author of this thesis does not use as an example a specific existing app, but rather the idea of such app. However, many apps with the same purpose are available in the market.

[21] Working Party, Opinion 4/2007, p 6.

[22] *Ibid*, p 7.

[23] *Ibid*, p 9.

[24] Article 29 Working Party. Working Document on data protection issues related to RFID technology, adopted on 19.1.2005, p 8.

The third element is ‘identified or identifiable’. In general terms, a natural person can be considered as ‘identified’ when, within a group of persons, he or she is ‘distinguished’ from all other members of the group. Accordingly, the natural person is ‘identifiable’ when, although the person has not been identified yet, it is possible to do it.[25] Taken the example of the number of steps, this means that it must be possible to determine the person whose steps have been counted. If the app on the same device has been used by several persons and it is not possible to determine whose steps were counted, it cannot be considered as personal data.

The fourth element is ‘natural person’ meaning that the protection applies to human beings. The right to the protection of personal data is, in that sense, a universal one that is not restricted to nationals or residents in a certain country.[26] Recital 2 of the DPD explicitly makes this point by stating that ‘data processing systems are designed to serve man’ and that they ‘must, whatever the nationality or residence of natural persons, respect their fundamental rights and freedoms’. Here, the example of number of steps does not even raise a question whether it is about a natural person, because the collecting activity and the nature of the data exclude the possibility that the data concerns a judicial person.

In some cases, the data which initially had the characteristics of personal data is no longer considered as personal data. This is called anonymised data, which has been explained in Recital 26 of the DPD. Data are anonymised if all identifying elements have been eliminated from a set of personal data. No element may be left in the information which could, by exercising reasonable effort, serve to re-identify the person(s) concerned. Where data have been successfully anonymised, they are no longer considered as personal data and the principles and requirements of DPD do not apply to the processing of such data.[27]

In the GDPR, the definition of personal data still includes the same four main elements. However, personal data is defined in a slightly more precise manner and adds name, location data, online identifier and also genetic information as potential identifiers of a person.[28] The

[25] Working Party, Opinion 4/2007, p 12.

[26] *Ibid*, p 21.

[27] Handbook on European Data Protection Law, p 44.

[28] GDPR, Art 4(1): ’personal data’ means any information relating to an identified or identifiable natural person 'data subject'; an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person;

reason for this, as acknowledged by the Working Party[29] and increasingly emphasized by scholars[30], is that all data could potentially be personal data. Data, which at one moment in time may contain no information about a specific person whatsoever, may in the future be used, through advanced techniques, to identify or individualise a person.[31] Moreover, data that may not alone identify a person can increasingly be linked, among other means through interconnecting and harvesting databases, and be used to create profiles so that two or more non-identifying datasets may become identifying datasets if integrated.[32]

The GDPR continues to state that the anonymised data is not considered as personal data and the principles of data protection should therefore not apply to anonymous information. That is information which does not relate to an identified or identifiable natural person or to data rendered anonymous in such a way that the data subject is not or no longer identifiable. Therefore, the GDPR does not concern the processing of such anonymous information, including for statistical and research purposes.[33]

After Working Party's suggestion[34], the concept of pseudonymisation was introduced to the GDPR. Art 4 (3) (b) defines pseudonymisation as the processing of personal data in such a way that the data can no longer be attributed to a specific data subject without the use of additional information, as long as such additional information is kept separately and subject to technical and organisational measures to ensure non-attribution to an identified or identifiable person. In practice, data is pseudonymised when the identifiers (name, date of birth etc) in the personal information are replaced by one pseudonym, which is achieved, for example, by encryption or hashing of those identifiers.[35]

In contrast to anonymised data, pseudonymised data is still considered personal data according to Recital 23 of GDPR. The pseudonymisation of data by data processors and controllers is encouraged in the GDPR, as it gives them several benefits. For example, the

[29] Article 29 Working Party, Opinion 05/2014 on Anonymisation Technique, adopted on 10 April 2014, WP216, p 9.

[30] For full reference see: B. Van der Sloot. Do data protection rules protect the individual and should they? An assessment of the proposed General Data Protection Regulation. - International Data Privacy Law, 2014, Vol. 4, No. 4, p 309, fn 22.

[31] Van der Sloot, p 309.

[32] M. R. Koot, Measuring and Predicting Anonymity, Amsterdam: Informatics Institute cop., 2012, p 101.

[33] GDPR, Recital 23.

[34] Article 29 Working Party, Opinion 01/2012 on the data protection reform proposals, adopted on 23 March 2012, 00530/12/EN WP 191, p 11

[35] Handbook on European Data Protection Law, p 45.

data breach notification requirements are mitigated (Art 32 (3) (a) of the GDPR) and there is greater flexibility to conduct data profiling without data subject's consent (Art 20 (1a) (b) of the GDPR). However, Working Party has expressed the opinion that pseudonymised data should not be defined as a new category of data, allowing for derogations from certain obligations defined under the GDPR.[36] The GDPR also encourages pseudonymisation in the interests of enhancing security and as a privacy by design measure (Recital 61 of the GDPR), which is also supported by the Working Party.[37]

1.2.2 Special Protection of Sensitive Data

Some forms of personal data are considered to be of a particular sensitive nature requiring stricter protection.[38] Art 8 (1) of the DPD lists such data as revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life. In Recital 33 of the DPD these data are referred to as data which are capable by their nature of infringing fundamental freedoms or privacy. Therefore, these forms of data are more strictly protected and in general processing of such data is prohibited, except for certain cases as stipulated in Art 8.

The rationale behind regulating particular categories of data in a different way stems from the presumption that misuse of these data could have more severe consequences on the individual's fundamental rights, such as the right to privacy and non-discrimination, than misuse of other, 'normal' personal data. Misuse of sensitive data, such as health data or sexual orientation (e.g. if publicly revealed), may be irreversible and have long-term consequences for the individual as well as his social environment.[39] The European Court of Human Rights[40]

---

[36] Article 29 Working Party, Letter to Mr Jan Philipp ALBRECHT, 17 June 2015. - http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2015/20150617_letter_from_the_art29_wp_on_trilogue_to_mralbrecht_en.pdf (18 March 2016); Article 29 Working Party, Letter to Mr Jan Philipp ALBRECHT, Appendix, 17 June 2015. - http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2015/20150617_appendix_core_issues_plenary_en.pdf (18 March 2016).

[37] Article 29 Working Party, Letter to Mr Jan Philipp ALBRECHT.

[38] The EU Charter of Fundamental Rights. Commentary. Hart Publishing: Oxford, p 253.

[39] Article 29 Working Party Advice Paper on Special Categories of Data (sensitive data). - http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2011/2011_04_20_letter_artwp_mme_le_bail_directive_9546ec_annex1_en.pdf (20.02.2016), p 4.

[40] The European Court of Human Rights is established by the European Convention of Human Rights, a human rights instrument drafted by the Council of Europe. The Council of Europe has adopted its own regulation for the protection of personal data – Convention for the protection of individuals with regard to the automatic

has also confirmed the special nature of such sensitive data: 'the protection of personal data, in particular medical data, is of fundamental importance to a person's enjoyment of his or her right to respect for private and family life'.[41]

1.2.3 The Definition of Health Data

In 2011, the Working Party issued an advice paper on special categories of data, where it acknowledged that health data represents one of the most complex categories of sensitive data due to the wide range of personal data that may fall into the category of health-related data.[42] However, despite providing high level of protection for health data, the DPD does not define what is meant under the term 'health data'. In order to apply the special protection to health data, it must be understood when the data can be considered as health data.

Until now, it has been left to the courts and data protection agencies to decide on a case-by-case basis whether data constitute health data. For example, the European Court of Justice found in the *Lindqvist* case that the fact that an individual has injured her foot and is on half-time on medical grounds constitutes personal data concerning health within the meaning of Article 8 (1) of the Data Protection Directive.[43] Some other examples from national legislators, judges and data protection agencies when data have constituted as health data include: a fact that a person is wearing glasses or contact lenses; data about a person's intellectual and emotional capacity (such as IQ), information about smoking and drinking habits; data on allergies disclosed to private entities (such as airlines) or to public bodies (such as schools); data on health conditions to be used in an emergency (for example information that a child taking part in a summer camp or similar event suffers from asthma); membership of an individual in a patient support group (e.g. cancer support group), Weight Watchers, Alcoholics Anonymous or other self-help and support groups with a health-related objective.[44]

---

processing of personal data (Convention 108). See: Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Council of Europe, CETS No. 108, 1981.

As the Convention 108 uses the same language while defining personal data and special categories of personal data, the judgment of ECtHR can be applied to interpret the DPD.

[41] ECtHR, I v Finland, No. 20511/03, 17 July 2008.

[42] Article 29 Working Party Advice Paper on Special Categories of Data (sensitive data), p. 10.

[43] European Court of Justice, Judgment of 6 November 2003, Case C-101/01 - Bodil Lindqvist.

[44] Working Party, Annex, p 6.

A case-by-case analysis of data might have been sufficient means to determine the health data at the time when the processing of such data mostly concerned the relation between physicians and data subject, and in some cases also the employer and the data subject. However, since the emergence of the internet, technological developments have given everyone the chance to collect and process different personal data and a large proportion of it might fall under the notion of health data. Therefore, in order for the app developers to comply with the regulations concerning processing health data, and also the data subjects to protect their rights, there should be a more precise meaning of the term 'health data'.

In 2015, the Working Party issued a document analysing the meaning of health data in apps and devices.[45] They found that there is one category of information that can be uniformly found as health data, that is, medical data – a category of data about the physical or mental health status of a data subject that are generated in a professional, medical context. This includes all data related to contacts with individuals and their diagnosis and/or treatment by providers of health services, and any related information on diseases, disabilities, medical history and clinical treatment. This also includes any data generated by devices or apps, which are used in this context, irrespective of whether the devices are considered as 'medical devices'.

However, in addition to medical data, all data concerning the health of individual subjects can fall under the notion of health data. Furthermore, data used in administrative context (e.g. data disclosed to public authorities about disabilities or specific diseases for tax allowances or data; documents related to the health of the employee in the employment relationship)[46] and also data about the purchase of medical products, devices and services constitute health data.[47] The collected data does not need to establish 'ill health', for example, when a person fills in an online questionnaire with the purpose of providing health advice, the collected data are considered as health data regardless of the input the person provides.[48]

[45] Article 29 Working Party, Annex (Health data in apps and devices) to a Letter to European Commission in answer to Green Paper, 05.02.2015. - http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2015/20150205_letter_art29wp_ec_health_data_after_plenary_annex_en.pdf (20.02.2016), p 2.

[46] EDPS Guidelines concerning the processing of health data in the workplace by Community institutions and bodies, September 2009, p. 2.

[47] Working Party, Annex, p 2.

[48] *Ibid*, p 2.

The absence of definition of health data has resulted in a situation where it is difficult for both the processors and controllers, but also the data subjects to understand whether the data in question could be processed at all and how it should be protected. In order to clarify this issue, the latest version of the proposed GDPR includes a definition of health data. Art 4 (1) (15) states that 'data concerning health' means personal data related to the physical or mental health of an individual, including the provision of health care services, which reveal information about his or her health status.

In addition, the GDPR also includes a comprehensive, but non-exhaustive list in Recital 26 about the meaning of health data. It reads that 'personal data concerning health should include all data pertaining to the health status of a data subject which reveal information relating to the past, current or future physical or mental health status of the data subject; including information about the individual collected in the course of the registration for and the provision of health care services as referred to in Directive 2011/24/EU to the individual; a number, symbol or particular assigned to an individual to uniquely identify the individual for health purposes; information derived from the testing or examination of a body part or bodily substance, including genetic data and biological samples; or any information on e.g. a disease, disability, disease risk, medical history, clinical treatment, or the actual physiological or biomedical state of the data subject independent of its source, such as e.g. from a physician or other health professional, a hospital, a medical device, or an in vitro diagnostic test.'

At first sight it seems that reading Recital 26 could possibly solve the question of deciding when data is considered as health data. However, when breaking down the definition in Art 4 (1) (12) and the Recital 26 of the GDPR, they actually do not say much new compared to the knowledge about health data that had been developed over the years when applying the DPD. Art 4 (1) (12) simply reiterates the opinion that health data is basically any personal data which reveals information about the health status of the data subject. The first part of the non-exhaustive list in Recital 26 focuses rather on the data collected in the professional medical context (administrative data, data collected testing and examination of a body part or bodily substance). However, the last part of Recital 26 – 'or any information on e.g. a disease, disability, disease risk, medical history, clinical treatment, or the actual physiological or biomedical state of the data subject independent of its source, such as e.g. from a physician or other health professional, a hospital, a medical device, or an in vitro diagnostic test,' – indicates a broader scope of the health data. The part 'independent of its source' may refer to the data collected by devices analysing a person's urine and blood, and apps measuring blood

pressure or heart rate, regardless of whether the testing is performed by medical professionals or by devices and apps freely available on the commercial market and irrespective whether these devices are marketed as medical devices or not. A clear example of such medical health data is a glucose-metering app that warns when the glucose level is too high and advises the user to take action.[49]

Another interesting part of Recital 26 is the term 'disease risk' which refers to data concerning the potential future health status of a data subject. According to the Working Party, health data therefore also includes information about a person's obesity, high or low blood pressure, hereditary or genetic predisposition, excessive alcohol consumption or drug use or any other information where there is a scientifically proven or commonly perceived risk of disease in the future.[50] Accordingly, any individual piece of information, which could possibly affect the health status of a person, would be considered as health data. When blood pressure could be considered as information relating to person's health already at the moment, then consumption of alcohol, for example, would not normally be considered as information directly referring to a person's health. However, under the new explanation of the health data in Recital 26, such information could at some point be considered as health data.

1.2.4 Health data in mHealth

mHealth largely consists of different health and well-being mobile apps which have the purpose to collect and analyse data that users provide. The data collected can vary from the steps taken in a day to measuring glucose level in blood sugar. All this data could possibly show the health status of a person. However, Article 29 Working Party has dismissed the notion that any information about a person's habits or acts would constitute health data. This concerns data from which no conclusions can reasonably be drawn about the health status of a data subject. Not all raw data collected (measurements) qualify as information (from which meaning can be derived) about the health of a person. For example, if a mobile app would only count the number of steps during a single walk, without being able to combine those data with other data from and about the same data subject, and in the absence of specific medical context in which the app data are to be used, the collected data are not likely to have a significant impact on the privacy of the data subject and do not require the extra protection of the special category of health data. They are thus considered raw (relatively low impact

[49] Working Party, Annex, p 2.

[50] *Ibid*, p 2.

lifestyle) personal data (provided, the app does not process location data), not information from which knowledge about that person's health can be inferred.[51]

There exist data that are 'too raw' to draw any conclusions from about the data subject's health but at the same time, in some cases these same data become sufficient to be considered health data. At the moment, there is no clear answer to the question where to draw the line. At the same time, it is crucial to differentiate personal data and sensitive personal data. If data are health data, but mistakenly treated as 'ordinary' personal data, there is a risk that the high level of protection deemed necessary by the European legislator is undermined. Working Party has warned that if seemingly innocuous raw data are tracked over a period of time, combined with other data, or transferred to other parties who have access to additional complementary datasets, it may well be that even the seemingly most innocuous data, combined with other data sources, and used for other purposes, will come within the definition of 'health data'.[52]

European Data Protection Supervisor is on the opinion that there is no simple definitive answer to the question whether the data processed in health and well-being apps is considered health data. The assessment can only be done on a case-by-case basis. In the absence of a clear definition, after an assessment of the case-specific circumstances, the notion of what constitutes health data should be construed broadly, so as to include any data relating to a person's physical and mental health information. Due account must be taken of the fact that it is not only the intrinsic nature of the information that identifies it as health data. The circumstances surrounding the gathering and processing of such information also play a role.[53] As argued by the French national data protection authority, there is not always a clear distinction between the notion of health data and well-being information. [54] Rather, there is a continuum from cases where well-being information has little or no relation whatsoever to individual's health to cases where - depending on the circumstances of data collection and

[51] Working Party, Annex, p 3.

[52] *Ibid*, p 3.

[53] EDPS Opinion 1/2015 Mobile Health, 21 May 2015. - https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2015/15-05-21_Mhealth_EN.pdf (5.03.2016), p 6.

[54] Commission Nationale de l'Informatique et des Libertés (CNIL), Le Corps, Nouvel Object Connecté, Cahiers IP no 2.

processing, including its scale and the purposes of the processing - the information clearly constitutes health data and is perhaps even used in a medical context.[55]

In order to differentiate the processing of raw personal data and health data, the Working Party has brought out some more detailed aspects which should be taken into consideration.[56] In addition to looking at the character of the data, their intended use must also be taken into account in order to determine whether the data is considered as health data. For example, a single registration of a person's weight, blood pressure or pulse/heart rate, at least without any further information about age or sex, does not allow for the inference of information about the actual or likely future health status of that person. However, when those measurements and information are collected over time, they may be used to determine a significant aspect of an individual's health, such as health risks related to obesity or an illness causing a significant loss of weight, high/low blood pressure, arrhythmia etc. A significant loss of weight may be due to several reasons, some positive (a drastic diet), some negative (impact of a harsh medical treatment; depression, etc.). When conclusions are drawn about someone's health, regardless of their reliability, these conclusions are to be treated as health data.[57]

Moreover, there has to be a demonstrable relationship between the raw data set and the capacity to determine a health aspect of a person, based on the raw data or on the data in combination with data from other sources. For example, if a diet app only counts the calories as calculated from input provided by the data subject, and the information about the specific foods eaten would not be stored, it would be unlikely that any meaningful conclusions can be drawn with regard to the health of that person (unless the daily intake of calories is excessive in absolute terms). But if data from a diet app, or heart rate monitor or sleep diary app are combined with information provided by the data subject (directly or indirectly, for example based on information collected from that person's social networking profile), conclusions (whether accurate or inaccurate) may be drawn about that person's health condition, such as medical risk or diabetics. In these cases it is likely that health data can be inferred from the combined data.[58]

[55] EDPS Opinion, p 6.

[56] *Ibid*, p 3.

[57] Ibid.

[58] Ibid.

In conclusion, although many cases must be looked individually, there are three different types of data which could be considered as health data for the purposes of mHealth. Firstly, when the data are inherently medical data (for example when the usage of a blood sugar measuring app is prescribed by the doctor in a patient-doctor relationship and the data is transferred to doctor). Secondly, when the data are raw sensor data that can be used in or in combination with other data to draw a conclusion about the actual health status or health risk of a person (for example the long-term data about person's daily activity and alcohol consumption in order to evaluate the risk of certain diseases). Thirdly, when conclusions are drawn about a person's health status or health risk.[59]

1.3 Processing of Personal Data

'Processing' is an essential term when analysing the applicability of the data protection rules to certain activities regarding personal data. The scope of the DPD as well as the GDPR is limited with those activities which involve processing of personal data.[60] Therefore, it is important to understand the meaning of the term 'processing'. Art 2 (b) of the DPD defines processing as 'any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction'. The definition includes various activities which could be carried out with personal data and it is hard to imagine an activity which entails personal data and which is not understood as processing.

There is not a major change regarding the definition of processing in the GDPR. According to Art 4 (3) of the GDPR 'processing' means any operation or set of operations which is performed upon personal data or sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. There are only two noticeable changes. Firstly, 'structuring' is added to the list of means, which in the view of the author of this thesis does not lead to major changes in practice. Secondly, the term 'blocking' is substituted with 'restriction', which is broader in the meaning and indicates that

[59] Working Party, Annex, p 5.

[60] DPD, Art 3 (1); GDPR, Art 2 (1)

the activity does not have to completely block the data but also setting limits to accessing it (restriction) can count as processing.

In order to analyse the processing activities that take place in mHealth, a short overview of the platforms used must be given. Most of the mHealth solutions are based on apps. Apps are software applications designed for a specific task to be carried out on smartphones, tablet computers and smart watches. They organise information in a way suitable for the specific characteristics of the device and often closely interact with the hardware and operating system features present on the devices. The underlying operating system will also include software or data structures that are important for the core services of the smart device, for example, the address book of a smartphone. The operating system is designed to make these components available to apps through Application Programming Interfaces (APIs). Those APIs offer access to the multitude of sensors which may be present on smart devices. Such sensors include: a gyroscope, a digital compass and an accelerometer to provide speed and direction of movement; front and rear cameras to acquire video and photographs; and a microphone to record audio. The type, accuracy and frequency of these sensor data varies by device and the operating system. Through the API, app developers are able to collect such data continuously, access and write contact data, send email, SMS or social network messages, read/modify/delete SD card contents, record audio, use the camera and access stored pictures, read the phone state and identity, modify the global system settings and prevent the phone from sleeping. APIs can also provide information relating to the device itself through one or more unique identifiers and information about other installed apps. These data sources can be further processed, typically to provide a revenue stream, in a manner which may be unknown or unwanted by the end user.[61]

When putting together the definition of processing and the description of apps' working principles, it is possible to conclude that whenever personal data is involved in the apps (no matter if the person enters it himself or it is being collected by sensors to the app), the apps are processing personal data.

However, not all processing of personal data falls under the protection of the data protection regulations. Art 3 (2) of the DPD stipulates that the DPD shall not apply when personal data

[61] Article 29 Working Party, Opininon on apps on smart devices, adopted on 27 February 2013, WP 202. - http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp202_en.pdf (20.03.2016), p 4.

is processed by a natural person in the course of a purely personal or household activity. Recital (12) of the DPD names – as an example – correspondence and the holding of records of addresses as such household activities. In today's world the current DPD's approach to personal or household processing has an unrealistically narrow scope that no longer reflects individuals' capacity to process data for personal and household activities and has therefore become anachronistic.[62] The GDPR adds to the list of examples that can fall under the household exemption social networking and on-line activity.[63]

According to the Working Party, the household exemption could also apply to certain cases of processing of health data in mHealth. They argue that if the data processing only takes place on the device itself, and no personal data are transmitted outside the device, the law would not apply to the user, because of the exception of purely personal use, as laid down in Article 3 (2) of the Data Protection Directive 95/46/EC.[64] The author of this thesis agrees with the Working Party in this matter for two reasons. Firstly, the concerned personal data processed in the app or device is most likely the data of the owner of the device. Therefore, even when the app processes the data, it is being done only with regards to the person who has permitted the app to process it (by downloading and using the app). Secondly, if the personal data processed stays in the device and is not transmitted, there is much smaller risk that the processing could be a threat to the data subject's privacy.

In the GDPR, the household exemption stays in force. Therefore, it would still apply in the case of processing personal data in the device itself and not transmitting it. However, Recital 15 states that the GDPR should apply to controllers or processors which provide the means for processing personal data for such personal or household activities, meaning that they still have a role to play in ensuring the processing complies with data protection law.[65]

[62] Article 29 Working Party, Letter to EU Council president, Annex 2: Proposals for Amendments regarding exemption for personal or household activities, Brussels, 11 December 2013. - http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2013/20130227_statement_dp_annex2_en.pdf (20.03.2016), p 2.

[63] GDPR, Recital 15.

[64] Working Party, Annex, p 5.

[65] Working Party, Annex 2, p 5.

1.4 Medical Devices

When health data are being processed in the apps and devices, a question arises whether these apps and devices could fall under the category of 'medical devices'. In the European Union, the medical devices are regulated under the Council Directive 93/42/EEC dated 14 June 1993 (the Medical Devices Directive). The core legal framework consists of 3 directives: Directive 90/385/EEC regarding active implantable medical devices, Directive 93/42/EEC regarding medical devices and Directive 98/79/EC regarding in vitro diagnostic medical devices. They aim at ensuring a high level of protection of human health and safety and the good functioning of the Single Market. These three main directives have been supplemented over time by several modifying and implementing directives, including the last technical revision by Directive 2007/47/EC. On 26 September 2012, the European Commission adopted a Proposal for a Regulation of the European Parliament and of the Council on medical devices and a Proposal for a Regulation of the European Parliament and of the Council on in vitro diagnostic medical devices which will, once adopted by the European Parliament and the Council, replace the existing three medical devices directives.[66]

According to Art 1 (2) (a) of Directive 90/385/EEC (as amended by Directive 2007/47/EC) 'medical device' means any instrument, apparatus, appliance, software, material or other article, whether used alone or in combination, together with any accessories, including the software intended by its manufacturer to be used specifically for diagnostic and/or therapeutic purposes and necessary for its proper application, intended by the manufacturer to be used for human beings for the purpose of:

- diagnosis, prevention, monitoring, treatment or alleviation of disease;
- diagnosis, monitoring, treatment, alleviation of or compensation for an injury or handicap;
- investigation, replacement or modification of the anatomy or of a physiological process;
- control of conception;

and which does not achieve its principal intended action in or on the human body by pharmacological, immunological or metabolic means, but which may be assisted in its function by such means.

[66] International telecommunication Union. Filling the gap: Legal and Regulatory Challenges of Mobile Health (mHealth) in Europe, 2014. - https://www.itu.int/en/ITU-D/Regional-Presence/Europe/Documents/ITU%20mHealth%20Regulatory%20gaps%20Discussion%20Paper%20June2014.pdf (20.03.2016), p 7.

An accessory is defined in Art 1 (2) (b) of Directive 90/385/EEC as being 'any article which whilst not being a device is intended specifically by its manufacturer to be used together with a device to enable it to be used in accordance with the use of the device intended by the manufacturer of the device'.

The International Telecommunication Union has analysed these definitions and has found the following. Medical device is recognized, above and beyond its functions, by its intended use as defined by the manufacturer; a medical device is therefore, to a certain extent, a finished product that should be regulated by a set of rules different from those governing any adaptations or uses that might be made of it independently of the end-uses assigned to it by its manufacturer. Software intended to be used specifically for diagnostic and/or therapeutic purposes is a medical device. Accordingly, it seems difficult to label a mobile terminal used by patient as a medical device, to the extent that this terminal does not meet the intended end-uses of a medical device as defined above. However, software designed for diagnostic and/or therapeutic purposes that may be downloaded to a mobile telephone meets or may meet the preceding definitions and, consequently, may lie within the scope of the Directive of 14 June 1993.[67]

In order to provide guidance to the software developers, European Commission has issued non-binding Guidelines on the Qualification and Classification of Stand Alone Software Used in Healthcare within the Regulatory Framework of Medical Devices (the Guidelines)[68]. The Guidelines constitute a code of practice that the companies launching mHealth apps need to take into account. As the Guidelines offer more clarity on the question, whether the mHealth apps or devices could be considered as medical devices, the main criterion of the Guidelines will be brought out.

The Guidelines' decisive criterion to classify medical devices is whether the software is intended to interpret (or to facilitate the interpretation of) data by modifying or representing health related individual information. Altering the representation of data purely for embellishment purposes is a nonmedical task.[69] Therefore, a mHealth app is not a medical

[67] International telecommunication Union, p 8.

[68] Guidelines on the Qualification and Classification of Stand Alone Software Used in Healthcare within the Regulatory Framework of Medical Devices. European Commission, DG Health and Consumer, Directorate B, Unit B2 'Health Technology and Cosmetics', January 2012.

[69] Guidelines, p 10.

device if it performs an action limited to storing, archiving, compressing or transferring medical data, without interpreting/altering it.[70] The same conclusion applies to an app limited to collecting and transmitting medical data from a(n) (in vitro) diagnostic medical device in the home environment to a doctor, without modifying its content.[71]

The Directives do apply to tools combining medical knowledge with patient-specific physiological parameters.[72] In addition, apps providing immediate decision-triggering information, or altering the representation of data in a way that contributes to the interpretative tasks performed by medical professional are subject to the Directives.[73] Also, apps intended to provide additional information that contributes to diagnosis and/or treatment are qualified as medical devices.[74]

The question whether an mHealth app or device falls under the medical devices regulations plays a role in the data protection regulation as well. Firstly, medical devices need to be in conformity with specific requirements set out in the Annex I of the Directive 90/385/EEC. Therefore, when an app or a device qualifies as a medical device, it imposes many different requirements on the developers and producers in order to show that their product is of good quality and does not endanger the health of a person. In the view of the author of this thesis, the data production requirements could also fall under the requirements of the medical devices and therefore, strict privacy policies and means to protect data should be adopted.

Secondly, the question of consent arises. According to Art 8 (1) of the DPD, processing of sensitive data (including health data) shall be prohibited. However, there are several exceptions when this is allowed and the most relied upon exception is stipulated in Art 8 (2) (a) which allows processing of sensitive information if the data subject has given his or her explicit consent to the processing. Another exception comes from Art 8 (3), which states that processing is allowed (without data subject's consent) if it is done for medical purposes by a health professional. In the field of mHealth, the last exception might not apply, as the processing is in many cases not specifically done by a professional, but rather by a software (automated processing). However, the circumstances are different when the GDPR enters into

[70] Guidelines, p 10, 20.

[71] *Ibid*, p 14, 15, 20, 26.

[72] *Ibid*, p 20, 25.

[73] *Ibid*, p 10, 11.

[74] *Ibid*, p 20.

force. Art 9 (2) (a) of the GDPR allows processing of sensitive data when 'processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union law or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 4'. Paragraph 4 states that the processing must happen by or under the responsibility of a professional subject to the obligation of professional secrecy. Therefore, it allows the processing by automated means in the apps and devices as long as it happens under the responsibility of a professional subject to the obligation of professional secrecy. In conclusion, it means that mHealth apps and devices falling under the definition of medical devices can process users' sensitive data without the explicit consent requirements.

1.5 Conclusion of the Chapter

Understanding the content of the term 'personal data' is the basis of the data protection and has been already defined in the DPD and also analysed by Working Party. The four elements of the definition of personal data – 'any information'; 'relating to'; 'identified or identifiable' and 'natural person' – have remained the same in the GDPR and should be used in order to evaluate the nature of data used in the apps.

The author of this thesis is in the opinion, that by adding the pseudonymisation tool to the GDPR, a better ground is established for the protection of the personal data in mHealth. As the pseudonymisation of data does put a heavy burden on the data processors but at the same time gives them several benefits, they are most probably willing to use the pseudonymisation tool. At the same time, the benefit for individual data subjects is considerable as the data subjects are no longer identified but their rights are still protected under the data protection principles.

As the DPD does not have a definition of health data, it could have been argued that the protection of health data is therefore not sufficiently guaranteed as it is complicated to understand what health data entails. However, as it was brought out, the notion of health data has been explained by the courts and data protection authorities and the author of the thesis is in the position that deriving from these opinions it is possible to conclude what entails health data in mHealth. In conclusion, there are three types of health data in mHealth: medical data;

raw sensor data used in combination with other data to draw conclusions about person's health; conclusions made about person's health.

Furthermore, the GDPR now includes a definition of health data which shows the legislator's wish to put more emphasis on the protection of health data and eliminate possible confusions. The definition of health data includes the part 'independent of its source' which in the view of the author of this thesis aims to broaden the notion of health data making it not dependent on the provision of healthcare services. This is also relevant regarding mHealth as many apps measures health parameters but are not provided by health care professionals. Therefore, as the definition of health data is broader, data subjects can count on stricter protection of these kinds of data that have been collected in mHealth apps.

In addition, it was brought out that regulations on medical devices can also play a role in the protection of personal data. If mHealth app or device is considered as a medical device, certain requirement must be fulfilled to bring the product to the market which means that the compliance with the data protection rules will also be guaranteed.

2. DATA PROTECTION REQUIREMENTS IN MHEALTH

2.1 Introduction to Chapter

In general, in order for the processing of personal data to be legitimate, two sets of most important rules must be fulfilled. Firstly, at least one condition of the six different bases to legitimise the processing of personal data must be satisfied. Consent is one of those bases and is most used. However, several requirements apply to obtaining consent and in cases of sensitive personal data these standards are even higher. When the consent is asked for processing in mHealth, different aspects come up that must be solved in order to determine the true validity of consent.

Secondly, the principles concerning the data quality must be all fulfilled in order for the data processing to be in accordance with the data protection rules. There are six principles in the DPD and the GDPR, but only two of them will be analysed. The purpose limitation principle and data minimisation principle are the principles which have come up the most in the literature as the principles which are the most important but at the same time most criticised during the age of internet and processing of large amounts of data.

The aim of this chapter is to analyse how the mHealth relates to the general data protection requirements in order to answer the question whether the traditional data protection requirements provide efficient protection of personal data in mHealth.

2.2 The Notion of Consent

2.2.1 The Elements of Consent

Pursuant to Art 7 (a) of the DPD, consent is one of the basis for making processing of personal data legitimate. Although consent is often used to legitimate the processing of personal data, especially in cases of sensitive data, it might be a weak basis and lose its value when it is stretched or curtailed to make it fit to situations it was never intended to be used in. If it is used in circumstances where it is not appropriate, because the elements that constitute valid consent are unlikely to be present, this would lead to great vulnerability and, in practice,

this would weaken the position of data subjects in practice.[75] The European Data Protection Supervisor has stated in particular that 'it is not always clear what constitutes true, unambiguous consent. Some data controllers exploit this uncertainty by relying on methods not suitable to deliver true, unambiguous consent'.[76] In the same line, the Working Party has observed that 'complexity of data collection practices, business models, vendor relationships and technological applications in many cases outstrips the individual's ability or willingness to make decisions to control the use and sharing of information through active choice'.[77] Therefore, it is important to clarify the limits of consent and determine what the applicable conditions of valid consent mean.

In the DPD, Art 2 (h) defines that the data subject's consent shall mean 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. In addition, Art 7 (a) states that consent must be unambiguous. The GDPR assembles these requirements into one article and therefore, according to Art 4 (8) of the GDPR, the consent must fulfil those conditions: freely given, specific, informed and unambiguous.

According to the definition in Art 2 (h) of the DPD, a consent can be expressed by 'any … indication of his wishes … signifying'. This shows that a consent does not require a certain form, it just needs to be an indication. The fact that the indication can be of 'any' kind, opens the possibility of a wide understanding of the scope of such an indication. The minimum expression of an indication could be any kind of signal, sufficiently clear to be capable of indicating a data subject's wishes, and to be understandable by the data controller. The notion of 'indication' is wide, but it seems to imply a need for action. Other elements of the definition of consent, and the additional requirement in Article 7 (a) for consent to be unambiguous, support this interpretation. The requirement that the data subject must 'signify' his consent seems to indicate that simple inaction is insufficient and that some sort of action is required to constitute consent, although different kinds of actions, to be assessed 'in context',

[75] Article 29 Working Party, Opinion 15/2011 on the definition of consent, adopted 13 July 2011, WP187. - http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp187_en.pdf (20.03.2016), p 10.

[76] A comprehensive approach on personal data protection in the European Union. Communication from the commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions. Brussels, 4.11.2010 COM (2010) 609 final. - http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_en.pdf (15.03.2016), p 9.

[77] Article 29 Working Party, Working Party on Police and Justice, The Future of Privacy: Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data", 1 December 2009, WP 168. - http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp168_en.pdf (20.03.2016), p 17.

are possible.[78] However, the part of the definition concerning 'indication' should be read differently, when consent is needed in order to process special categories of data according to Art 8 (2) (a) of the DPD, because then consent needs to be explicit, meaning that just any indication is not enough in order to legitimise processing of data.

When relying on consent to legitimise processing of personal data, the first condition is that the consent must be freely given. The Working Party has stated that consent can only be valid if the data subject is able to exercise a real choice, and there is no risk of deception, intimidation, coercion or significant negative consequences if he or she does not consent. If the consequences of consenting undermine individuals' freedom of choice, consent would not be free.[79] The most common reason preventing consent to be free is a situation of subordination (an employment relationship), but other elements can also influence the decision of the data subject (e.g. financial, emotional or practical reasons).[80]

The second condition requires the consent to be specific. To qualify as specific, the consent must be intelligible: it should refer clearly and precisely to the scope and the consequences of the data processing. Consent must be given in relation to the different aspects of the processing which are clearly identified, it cannot apply to an open-ended set of processing activities. This means that the parties should have an understanding and knowledge of which data are processed and for which purposed.[81] It is possible that consent is given only once for different processing operations. However, in that case, those operations must fall within the reasonable expectations of the data subject and must be necessary in relation to the purpose of processing of personal data.[82]

The third condition is linked to the previous condition and requires the consent to be informed. The Working Party has stated in its opinion regarding electronic health records, that a data subject's consent must be based upon an appreciation and understanding of the facts and implication of an action. The individual concerned must be given, in a clear and understandable manner, accurate and full information of all relevant issues, in particular those specified in Articles 10 and 11 of the DPD (respectively Chapter III of GDPR), such as the

[78] Working Party, Opinion 15/2011, p 11.

[79] *Ibid*, p 13.

[80] *Ibid*, p 14.

[81] *Ibid*, p 17.

[82] Ibid.

nature of the data processed, purposes of the processing, the recipients of possible transfers, and the rights of the data subject.[83] Appropriate information has two sorts of requirements. Firstly, the quality of the information, indicating the way the information is given. Secondly, the accessibility and visibility of information, which means that the information must be given directly to individuals. It is not enough for information to be 'available' somewhere.[84]

Finally, for consent to be legitimate, it has to fulfil the unambiguity requirement. In the DPD, unambiguity was stipulated separately from the definition of the consent and it was part of Art 7 (a), which listed consent as one of the grounds for making processing of personal data legitimate. However, in the GDPR, unambiguity was brought to the definition of the consent in Art 4 (8). The consent is unambiguous, when the indication by which the data subject signifies his agreement leaves no room for doubt regarding his or her intent. If there is a reasonable doubt about the individual's intention, there is ambiguity. This means that data controllers must create robust procedures for individuals to deliver their consent; namely either to seek clear express consent or to rely on certain types of procedures that deliver individuals' clearly inferred consent.[85]

As discussed before, consent is one of the six grounds for legitimising processing of personal data (Art 7 (a) of the DPD, Art 6 (1) (a) of the GDPR). However, consent can also be used in order to process special categories of data, which according to Art 8 (1) of DPD is in general prohibited. But in order to use consent as a basis in that case, the consent must be explicit (Art 8 (2) (a)). Explicit consent has the same meaning as express consent, meaning that it encompasses all situations where individuals are presented with a proposal to agree or disagree to a particular use or disclosure of their personal information and they respond actively to the question, orally or in writing.[86] Also, the Working Party has expressed that consent is not explicit if there is only a possibility to opt out from processing of special categories of personal data.[87]

[83] Article 29 Working Party, Working Document on the processing of personal data relating to health in electronic health records, adopted on 15 February 2007, WP131. - http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2007/wp131_en.pdf (23.03.2016), p 9.

[84] Working Party, Opinion 15/2011, p 20.

[85] *Ibid*, p 21.

[86] *Ibid*, p 25.

[87] Working Party, WP131, p 9.

Although the elements of consent have remained the same in the art 7 (2) of the GDPR, the data controllers will now have an increased burden to present declarations authorising the processing of personal data to a data subject in a distinguishable manner. In addition, Art 7 (2) of the GDPR requires that request for consent must be presented in an intelligible and easily accessible form, using clear and plain language. This provision is necessary in order to avoid that declarations of consent could be hidden amongst pages of terms and conditions, which is a particular issue given the ubiquitous nature of computing in the modern information-dense world.[88] Furthermore, Art 7 (4) of the GDPR emphasises that while assessing the 'freely given' condition of the consent, it is important that the performance of a contract, including the provision of a service, is not conditional on consent to the processing of personal data that is not necessary for the performance of that contract. In the previous version of the draft of the GDPR[89], the condition in Art 7 (4) was that consent will not be sufficient to allow the processing of an individual's personal data where there is a significant imbalance between the position of the data subject and the controller. Although the specific condition has changed, the underlying idea remains the same. A data subject should not feel pressured to consent to data processing. All of the additional conditions of consent included in Art 7 of the GDPR seek to improve the situation where most people do not feel that they are in control of their personal data.[90]

2.2.2 Consent in mHealth

During the last decades, the medical field has already grown accustomed to requiring formal forms of consent in order to meet the requirements concerning the provision of health services. The formalisation of consent is arguably related to the reduction of everyday, one-to-one, face-to-face relations, tacit understandings between doctors and patients.[91] Therefore, patients are usually asked for a formal consent before the provision of health services and if that is not possible or has not been done, there is extensive practice as to the interpretation of

[88] L. Danagher, An Assessment of the Draft Data Protection Regulation: Does it Effectively Protect Data? - European Journal of Law and Technology, Vol. 3, No. 3, 2012.

[89] Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) [first reading] Analysis of the final compromise text with a view to agreement. Brussels, 15 December 2015. - http://statewatch.org/news/2015/dec/eu-council-dp-reg-draft-final-compromise-15039-15.pdf (15 February 2016).

[90] Special Eurobarometer 359. Attitudes on Data Protection and Electronic Identity in the European Union. June 2011. - http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf (23.03.2016)

[91] E. Mantovani, P. Quinn. mHealth and data protection – the letter and the spirit of consent legal requirements. International Review of Law, Computers & Technology, 28:2, 222-236, p 223.

person's will and whether it could be counted as valid consent. Mobile technologies for health and the possibility of entering into medical treatment relationships independent of geographic location are causing further changes. These changes relate to the form of consent and the value that individuals and societies will attribute to it.[92] In addition, the change in the medical field means change for the processing of medical data, which brings new challenges to the formal requirements of giving consent for legitimate processing. Some scholars have even posed the question whether social and technological developments will offer the possibility to express genuine informed consent consistent with what is intended in the data protection regulations.[93]

As described before, there are different legitimate basis for processing health data: the existence of the treatment relationship between a doctor and a patient; or the individual consent given by data subject. Scholars and drafters of the regulations have different opinions on which of those should be preferred when seeking the legitimacy of processing in the field of mHealth or eHealth in general. In order to allow individuals to be able to give a truly informed consent, it should be possible to know what data and processing is actually required. However, in the light of the complexity of the information society, the drafters of the GDPR recognise that it is 'difficult for an individual to know and understand if personal data are being collected, by whom, and for what purpose'.[94] In the past years, the healthcare sector has been criticised for over relying on the use of consent to legitimise the processing of personal data. Probably, that is why, the GDPR will recognise that reliance on consent under the circumstances of today's information society is less and less realistic as an option. Therefore, when is not clear to the data subject whether the data processing is actually 'required', consent should not be invoked and some other basis, such as treatment relationship should be sought.[95] However, when consent is still needed, the GDPR describes the need for 'negotiating imbalances' (Article 7) and about taking into account the situation of dependency (Recital 34). It is suggested that one should not be attributed choices he or she is unable to make, since this would impair the right to defend themselves.[96]

[92] E. Mantovani, P. Quinn, p 223.

[93] *Ibid*, p 224.

[94] COM (2010) 609, p 9.

[95] E. Mantovani, P. Quinn, p 227.

[96] *Ibid*, p 227.

2.2.3 Application of Requirements of Consent in mHealth

In the next paragraphs the formal requirements of consent will be placed into the context of mHealth through analysing problems that could potentially occur and assessing whether the proposed changes in the GDPR could possibly solve them. In order to specify the analysis and better understand the arising problems, the requirements will be examined through the example of a certain mHealth application, created for people suffering from diabetes to help them collect and monitor the level of glycose in their blood. At the moment, there are many apps available on the app stores which allow users to insert their glycose level.[97] In the near future we will likely see wearable devices that can measure the glycose level with the help of a new non-invasive technology, which will use electricity or ultrasound to measure glycose through the skin. Other technologies may use special light that shines through the skin using a spectroscope to measure glucose level.[98] This means that persons do not even have to insert the data themselves, but it will be automatically collected upon wearing the device. Although wearable devices that collect data about person's activities are already widely used in the present day (for example activity monitors), the data collected may or may not fall under the category of health data. Therefore, the example of monitoring glycose level will be used, because glycose level is without a doubt health data.

As demonstrated above, consent allowing the processing of health data must be explicit. Accordingly, only the schemes that utilise consent in an opt in, and not opt out (silence or inactivity) manner are deemed lawful.[99] Therefore, in the context of mHealth, users should have a specific way of consenting to the processing of the health data. Taking the example of the glycose level monitoring device and an app processing such data, the best way to obtain legitimate data would be presenting the user a question whether he or she agrees with the processing of data collected while using this device. The consent should be asked before the user starts using the device and it should be presented in a clear and specific form, where the user him or herself can make an active choice of consenting. This could, for example, be a sentence after which the user ticks a box, which is presented in the user interface of an accompanying app.

---

[97] E. Carey, K. Cherney. The Best Diabetes iPhone and Android Apps of 2015. - http://www.healthline.com/health/diabetes/top-iphone-android-apps#2 (4.04.2016)

[98] S. Lones. Next generation of diabetes wearables. - http://www.diabeticconnect.com/diabetes-information-articles/general/1032-next-generations-of-diabetes-wearables (4.04.2016)

[99] E. Mantovani, P. Quinn, p 227.

Under the GDPR, explicit consent must be provided in written form. The specification that consent to medical data processing must be written is a positive innovation of the proposed regulation. Under the current regime, there is a lack of clarity about the form of consent and the issue has been solved differently in the EU member states. For example, in Belgium, explicit consent must be written, in other countries, the requirement of written consent is not mandatory. Recital 32 and Article 7 (1) of the GDPR now require that 'where processing is based on the data subject's consent, the controller shall be able to demonstrate that consent was given by the data subject to the processing of their personal data'. Therefore, the controller of data bears the burden of proof in a matter when the giving of consent is under question. In order to be able to prove the consent, a record should be kept, arguably in written form.[100] Also, according to Art 7 (2) of the GDPR, the request for consent must be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. This would also apply to the glycose level device and app. The previously described option in which the person ticks a box after a sentence, would satisfy the needs of written consent when the data processor keeps record of the action of ticking the box and is able to prove it and this sentence which indicates consent is construed in a clear and plain language, clearly distinguishable from the rest of the terms and conditions.

Another requirement of great importance in the field of mHealth is the notion of specific consent. The users need to have a specific understanding of what they consent to. When taking the example of the glycose level device and app, then the users should have exact knowledge of the categories of data collected, as well as their manner of processing and destination of transfer. For example, in addition to the mere numbers of glycose level, the app could also ask the user to insert body weight and height, combine it with the heart rate that the device is able to monitor and collect, and therefore, analyse a person's health status. It would not be sufficient if the person just consents to the processing of its glycose level, but he or she also needs to consent to the combination of the processing of data that the device and app carry out.

While the previously described 'tick-box' consent might fulfil the majority of the requirements for legitimate data processing, it also entails problems, especially concerning the requirement of informed consent.[101] In order to make an informed decision, the data subject

[100] E. Mantovani, P. Quinn, p 227.

[101] *Ibid*, p 234.

must have the necessary information at his disposal to form an accurate judgement.[102] The specific obligation to inform the users in the context of apps has been explained by Article 29 Working Party in its opinion on apps on smart devices.[103] As the Working Party argues, the requirement of informed consent is only fulfilled if the person has duly and correctly been informed about the key elements of the data processing. They bring out four requirements. Firstly, the information must be provided before the processing (which often starts during installation), otherwise it is not deemed sufficient and is legally invalid. Secondly, it must be told what data are being processed, which is particularly important given the broad access apps generally have to sensors and data structures on the device. Thirdly, the users need to know who is legally responsible for the processing of their personal data and how that controller can be contacted, otherwise they cannot exercise their rights, such as the right to access data stored about them. Due to the fragmented nature of the app landscape, it is crucial that every app has a single point of contact, taking responsibility for all the data processing that takes place via the app. It must not be left to the end user to research the relations between app developers and other parties processing personal data through the app. Fourthly, end users must be adequately informed which data are collected about them and why. Users should also be made aware in clear and plain language whether the data may be reused by other parties, and if so, for what purposes.[104]

As the information that must be provided prior the processing is relatively wide, it cannot be narrowed down to one sentence. This becomes problematic, as in order to fulfil the requirement of informed consent, the app developer must provide a variety of information which is hard to present on a small screen. The Working Party has offered a solution of layered notices.[105] This means that the initial notice to the user contains the minimum information required by the EU legal framework, and further information is available through links to the whole privacy policy. The information should be presented directly on screen, easily accessible and highly visible. Next to comprehensive information suitable for the small screen of mobile devices, users must be able to link through to more extensive explanations, for example in the privacy policy, how the app uses personal data, who the data controller is

[102] Working Party, Opinion 15/2011, p 19.

[103] Working Party, Opininon on apps on smart devices, p 22.

[104] Ibid.

[105] Article 29 Working Party. Opinion 10/2004 on More Harmonised Information Provisions, Adopted on 25th November 2004, WP 100. - http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2004/wp100_en.pdf (3.04.2016), p 6.

and where a user can exercise his rights.[106] However, the author of this thesis finds that the solution of layered notices might actually diminish the value of the consent that the users are giving. When the consent is given for the first time, there is a greater chance that the users are paying attention to what they are consenting to, so there is a possibility that they might even open the additional links provided in the app and actually read the information given. Nevertheless, when such consent is asked for several times, the users may not pay attention to the request anymore and are likely to just 'tick the box' in order to proceed with the activities the application or device is providing. When this happens, then the 'ticking of the box' by users cannot be considered as giving informed consent any more. Even though relevant information might be available to the data subject, the likelihood that he will actually access it and form its decision based on that information is relatively low. What is more, once the consent is given for one purpose, it should be asked again for any other processing activity which is slightly different from the previous one. When this is done for the processing which happens in the context of the app or device that the data subject has already used before, the value of the new consent asked from him has definitely a weaker value in the context of informed decisions. That is because the data subject will not delve into the details of the information given once again and therefore he or she will likely just tick the box. At the same time, the information provided, as well as the purposes and other relevant information regarding the processing might have substantially changed after the user has given his or her initial consent.

2.3 Relevant Data Protection Principles

2.3.1 About the Principles

In order to analyse the main data protection principles and understand which problems arise in the field of mHealth, the substance and structure of those principles must be clarified. At first sight, there seems to be a difference in the current data protection legislation, the DPD, and the proposed GDPR. In the DPD, Section 1 is titled as 'Principles relating to data quality' and this section encompasses only one article – Art 6, which lists five conditions that all must be fulfilled when processing personal data. These conditions are generally accepted as data protection principles, which act as the starting point for more detailed provisions in the subsequent articles of the DPD. Moreover, all later data protection legislation at the EU level must comply with these principles and they must be kept in mind when interpreting such

[106] Working Party. Opinion 10/2004, p 6.

legislation.[107] In the GDPR, the structure of the articles has changed and it might be asked whether also the substance and meaning of principles has changed. In the GDPR, the whole Chapter II has been titled as 'Principles' and this chapter encompasses Articles 5 – 10 which in addition to listing the traditional data protection principles in Art 5, also include the conditions of lawfulness of processing, conditions for consent, processing of special categories of data and the processing not requiring identification. It might seem that all the conditions set out in those articles must now be considered as principles of data protection and must all be adhered to. However, the author of this thesis believes this not to be the intention of the drafters of the GDPR. Article 6 is titled as 'lawfulness of processing' and in principle has stayed the same as Art 7 of the DPD, which sets the criteria for making data processing legitimate. As previously explained, only one condition from this list must be fulfilled in order to make the data processing legitimate. Therefore, Art 6 of the GDPR should not be viewed as a general principle of data protection. What is more, the following articles stipulate the rules for special circumstances, for example, Art 7 establishes the rules that the consent must be in accordance with, when consent is used as a basis for legitimate processing. In addition, Art 5 of the GDPR is titled as 'principles relating to personal data processing'. Therefore, the analysis of this chapter will be guided by the assumption that the principles of data protection are the rules stipulated in Art 6 of the DPD and Art 5 of the GDPR.

Although the adoption of the GDPR is regarded as a substantial change in many aspects of the European data protection, there are no considerable changes in the underlying principles. Even the wordings of Art 6 of the DPD and Art 5 of the GDPR have remained almost unchanged. Positively, the 'names' of the principles have been added in the end of the clauses in Art 5 (1), clarifying the main idea of each condition and how a principle should be called. Therefore, the main principles as named in the GDPR are: lawfulness, fairness and transparency; purpose limitation; data minimisation; accuracy; storage limitation; integrity and confidentiality; accountability.[108] Out of these, the fundamental principles underlying data

[107] Handbook on European Data Protection Law, p 62.

[108] GDPR, Art 5 Principles relating to personal data processing
1. Personal data must be:
(a) processed lawfully, fairly and in a transparent manner in relation to the data subject ("lawfulness, fairness and transparency");
(b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes; further processing of personal data for archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes shall, in accordance with Article 83(1), not be considered incompatible with the initial purposes; ("purpose limitation");
(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ("data minimisation");

protection are purpose limitation and data minimisation principles.[109] These two principles are also the most relevant in the field of mHealth, but they also cause the most problems while applying. That is why, the principles of purpose limitation and data minimisation will be analysed in depth in the following sections.

2.3.2 Purpose Limitation Principle

Purpose limitation is an essential principle in the system of data protection, because it contributes to transparency, legal certainty and predictability while aiming to protect the data subject by setting limits on how the data controllers can process their data.[110] In essence, the principle of purpose specification means that the legitimacy of processing personal data will depend on the purpose of the processing. The purpose must have been specified and made manifest by the controller before the processing of data starts. The processing of personal data for undefined and/or unlimited purposes is unlawful. Every new purpose for processing data must have its own particular legal basis and cannot rely on the fact that the data were initially acquired or processed for another legitimate purpose. In turn, legitimate processing is limited to its initially specified purpose and any new purpose of processing will require a separate new legal basis. Disclosure of data to third parties will have to be considered especially carefully, as disclosure will usually constitute a new purpose and therefore require a legal basis, distinct from the one for collecting the data.[111]

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ("accuracy");
(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the data will be processed solely for archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes in accordance with Article 83(1) subject to implementation of the appropriate technical and organisational measures required by the Regulation in order to safeguard the rights and freedoms of the data subject ("storage limitation");
(eb) processed in a way that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ("integrity and confidentiality").
2. The controller shall be responsible for and be able to demonstrate compliance with paragraph 1 ("accountability").

[109] Working Party, Opininon on apps on smart devices, p 17.

[110] Article 29 Working Party. Opinion 03/2013 on purpose limitation. Adopted on 2 April 2013. WP 203. - http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf (18.03.2016), p 11.

[111] Handbook on European Data Protection Law, p 68.

The concept of purpose limitation consists of two parts: 'purpose specification' and 'compatible use'. The first part means that the data should be collected only for the 'specified, explicit and legitimate purposes'.[112] The condition of specified purpose lies at the core of the legal framework established for the protection of personal data. It sets the limits on the purposes for which the personal data could be used by the data controller. Therefore, it is extremely important that the purpose is determined already before the collection of data and is clearly and specifically identified. For example, 'marketing purposes' or 'future research' would not fulfil the requirement of specific purpose. At the same time, it must be kept in mind that overly detailed specifications can also be counter-productive as they are complicated to understand.[113] Here, the Working Party has also offered the solution of 'layered notice', where basic information is provided in a concise manner just before the processing starts and there is a reference to where more detailed information could be found.[114]

The purpose must also be explicit in a sense that it is clearly revealed, explained or expressed in some intelligible form. It is important in order to ensure that there is no vagueness or ambiguity to the meaning of the purpose and that the data subject understands it the same way as the data controller and processor.[115]

The requirement of legitimacy extends to Art 7 of the DPD or Art 6 of the GDPR, which outline the criteria for making data processing legitimate by listing six different legal grounds. Therefore, for the purposes to be legitimate, the processing must be based on at least one of those legal grounds. In addition, the purposes must be in accordance with all provisions of applicable data protection law, as well as other applicable laws.[116]

The second part of the purpose limitation principles is the notion of 'compatible use', more precisely that the personal data shall not be further processed in a way incompatible with initial purposes.[117] Here, the term 'further' should be understood as differentiating the very first processing operation, which is collection, and all other subsequent processing activities. The fact that further processing cannot be incompatible (not that it must be compatible)

[112] DPD, Art 6 (1) (b); GDPR, Art 5 (1) (b)

[113] Working Party. Opinion 03/2013, p 16.

[114] Working Party. Opinion 10/2004, p 6.

[115] Working Party. Opinion 03/2013, p 17.

[116] *Ibid*, p 20.

[117] DPD, Art 6 (1) (b); GDPR, Art 5 (1) (b)

indicates some flexibility to further use. The fact that further processing has a different purpose does not necessarily mean that it is incompatible.[118]

2.3.3 Data Minimisation Principle

The data minimisation principle is closely tied with the purpose limitation principle. The wording of the article itself refers to the purposes in order to determine whether this principle has been fulfilled. Although the data minimisation principle is listed together with other data protection principles in Art 6 of the DPD (Art 5 of the GDPR), some experts have not given it the status of a principle equal to the other ones in Art 6. For example, Serge Gutwirth has found that data minimisation is something that in essence mandates that all processing is both adequate for and limited to a specific purpose, therefore, the data minimisation is much more than just a principle. Its existence ensures the omnipresence of the fair information principles of adequacy, purpose limitation, duration, etc. in data processing, thus making it a basis for all other principles.[119] However, others have found that data minimisation is not so much a principle, but a technical mean of ensuring that all other principles are adhered to.[120] This thesis is written from the perspective that data minimisation is a principle like all other principles named in Art 6 of the DPD and Art 5 of the GDPR and needs to be followed while processing personal data.

A short overview of the amended wording of this principles should be given. In the DPD, the principle of data minimisation states that the processing must be 'adequate, relevant and not excessive in relation to the purpose for which they are collected and/or further processed'.[121] In the GDPR, the wording has been slightly changed to 'adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed'.[122] The biggest difference is in the third element of the principle – 'not excessive in relation' versus 'limited to what is necessary'. It is unknown whether by changing this wording, the drafters of the legislation were trying to change the substance of the principle. However, the author of this thesis argues that the change can have a substantial meaning while interpreting this principle. While the wording of the DPD uses negation, it gives it more flexible meaning. The

[118] Working Party. Opinion 03/2013, p 21.; See chapter 3.2.4 of this thesis.

[119] S. Gutwirth. Short Statement about the role of consent in the European Data Protection Directive. 2012. - https://works.bepress.com/serge_gutwirth/80/ (10.04.2016)

[120] Working Party, Annex, p 6.

[121] DPD, Art (6) (1) (c)

[122] GDPR, Art 5 (1) (c)

processing must rise to the threshold of being clearly excessive in order for the principle to be violated. However, the GDPR uses affirmative wording, which makes the interpretation of this principle less flexible. The data processed must be clearly limited to what is necessary, meaning that the threshold of the boundaries of minimal data is much lower and it is easier to come to a situation when data is processed unnecessarily.

2.3.4 Purpose Limitation and Data Minimisation in mHealth

These two principles offer the data subject the most protection from the data controller or processor. At the same time, they also conflict the most with the notion and substance of what mHealth is – a way of collecting large amounts of health data from a person in order to forward and/or analyse it for the benefit of the person.

From the context of the apps, the purpose limitation principle enables users to make a deliberate choice to trust a party with their personal data. Importantly, they will learn how their data are being used, and will be able to rely on the limitative purpose description to understand for what purposes their data will be used. The purposes of the data processing therefore need to be well-defined and comprehensible for an average user without expert legal or technical knowledge. At the same time, purpose limitation requires that app developers have a good overview of their business case before they start collecting personal data from users.[123] However, the purpose limitation principle does not consider sudden changes in the data processing activities. For example, if an app originally carried a purpose to monitor a person's daily activities (for example activity tracking apps on smart watches which count the steps), but the developer decides to change its business model and merge these data with the location data of the person and find out in which locations the person is the most active. In such cases, the respective data controllers would have to individually approach all users and ask for their prior unambiguous consent for the new purpose of their personal data processing.[124]

The view of the Working Party brought out in the last sentences of the previous paragraph seems to rather depreciate the purpose limitation principle and favour the app developers who wish to use the data collect for other purposes for which it was collected. The author of this thesis is in the opinion that although the asking of additional consent from the data subjects

[123] Working Party, Opininon on apps on smart devices, p 22.

[124] *Ibid*, p 17.

might need some extra time and resource, it should still be done in order to comply with the purpose limitation principle. Another possibility to use data for further processing without the consent of the data subject derives from the DPD, but this will be discussed in chapters 3.2.3 and 3.2.4.

In order to comply with the principle of data minimisation and prevent unnecessary and potentially unlawful data processing, app developers in the field of mHealth must carefully consider which data are strictly necessary to perform the desired functions. Apps can obtain access to many of the functions in the device, and are therefore capable to execute a variety of operations, such as sending an SMS, or accessing images and the entire address book. Many app stores support (semi) automated updates where the app developer can integrate new features and make those available with little or no interaction by the end user. Access to the underlying data on the device through the APIs gives operation system and device manufacturers and app stores an opportunity to enforce specific rules and offer appropriate information to end users. For example, operation system and device manufacturers should offer an API with precise controls to differentiate each type of these data and ensure that app developers can request access to only those data that are strictly necessary for the (lawful) functionality of their app. The types of data requested by the app developer can then be clearly displayed in the app store to inform the user prior to installation.[125]

The following example illustrates what can be understood by data minimisation: when designing a mobile app with the purpose of helping fight obesity, developers should ensure that it only collects the personal data necessary for that purpose. In that respect, although it might sometimes facilitate calorie tracking (e.g. by allowing users to scan the bar code of food they buy), further use by the operator of the information about users' preferences on product brands goes beyond the primary purpose of the app and thus would be excessive.[126]

The drafters of the Code of Conduct for mHealth[127] have advised the actors of mHealth on how to comply with the purpose limitation principle. They state that the mHealth app must be designed only to collect and process data concerning health for specific and legitimate purposes. These purposes must be clearly defined before any data processing takes place, and

[125] Working Party, Opininon on apps on smart devices, p 17.

[126] EDPS Opinion, p 10.

[127] Initiative of the European Commission to develop a code of conduct for app developers during the meetings of the stakeholders. See: https://ec.europa.eu/digital-single-market/en/news/mhealth-green-paper-next-steps

must bear a meaningful relationship to the functionality of the app. Once the purposes have been decided and clearly communicated to the user, the app may only process the data for compatible purposes – with the consent of the user and as required for the functionality of the app – as long as the assessment of the compatibility is done on a case by case basis consideration:

- the relationship between the initial purpose and the purpose for further compatible processing;
- the context of collection and the expectation of the user;
- the sensitivity of the data and the impact on user of the further processing;
- the safeguards that the developer has implemented to prevent any undue impact on the user.

For example, a developer providing an app that monitors blood sugar concentration levels to assist diabetes patients in dispensing medication is not allowed to sell this information to vendors of medication. The commercial exploitation of data concerning health by third parties is not compatible with the original purpose of providing assistance to diabetes patients. If the personal data is to be used for a purpose other than the initial or compatible purpose of collection, the personal data must either be completely anonymised before re-using it (removing any possibility to identify an individual on the basis of the data), or alternatively, free, informed and explicit consent of the users with the new use must be obtained.[128]

Such advice is clearly valuable to app developers and other actors in the field of mHealth, but the ultimate purpose of this advice is and shall be protection of personal data. Although the principles of purpose limitation and data minimisation may seem too burdensome for some, especially in the field of mHealth, where large amounts of data are processed. However, by complying with these principles, the app developer gain users' trust and will eventually benefit more from the usage of their apps.

2.4 Conclusion of the Chapter

The requirement of consent is a crucial concept in the field of mHealth. Although, for processing health data, a patient-doctor relationship is also a legitimate ground, in mHealth, this relationship usually does not exist. Therefore, in order for the processing to be allowed, a

[128] Draft of the Code of Conduct of mHealth. - https://www.bmjv.de/DE/Ministerium/Veranstaltungen/SaferInternetDay/Code_of_Conduct_SID.pdf?__blob=publicationFile&v=3 (10.01.2016), p 5.

valid consent must be asked from the data subject. The regular requirements of consent (freely given, informed, specific) must be applied when asking consent in mHealth and as shown through the example of a glycose metering app, this can be effectively done. As the data collected is health data, the consent shall also be explicit and after the adoption of the GDPR, also in a written form. These requirements fulfil the purpose of protecting the data subject from the breach of his right to privacy, because while consenting to the processing he/she shall have every possible opportunity to understand to what kind of processing he/she is consenting to.

The purpose limitation principle and data minimisation principle were analysed from the perspective of DPD and GDPR together, as there were no notable changes to these principles in the GDPR. Although the applicability of those principles has been challenged, it was found that in the view of the data protection authorities these principles are the most effective manner to protect the data subject from the unauthorised usage of their personal data by third parties and the author of this thesis agrees with it. Although, for the app developers it may be sometimes complicated to understand what obligation they have to fulfil in order to be in compliance with these principles, that should not undermine the value of these principles. In order to promote the compliance with the principles and in general with the data protection requirement, a Code of Conduct for the app developers is being drafted.

It must be concluded that the traditional data protection requirements as explained in this chapter, still remain an effective method to guarantee the protection of personal data. mHealth brings new situations and problems to the application of data protection requirements, for example how to ask for a legally valid consent on the small screen, or how to guarantee the compliance with the data minimisation principle one of the benefits of mHealth applications is their ability to analyse large sets of different data. However, the author of this thesis finds that the rising problems shall not be the reason for ignoring the data protection requirements. Instead, new solutions shall be found and advice given to the stakeholder but also to the persons on how to protect their data. Therefore, it can be concluded that the traditional data protection requirements analysed in this chapter are in general a sufficient way to protect the personal data.

3. SECONDARY USE OF HEALTH DATA COLLECTED IN mHEALTH

3.1 Introduction to Chapter

Pursuant to the purpose limitation principle, the data should only be processed for the initial purposes for which it was collected. When the data is transferred from the device, then the initial purpose will be exceeded and additional grounds for processing are needed. This is called the further processing or secondary use of data and is also regulated under the DPD and GDPR.

One of activities where further processing is used, is big data processing. Secondary use of data is becoming widespread in the age of big data. Although there are other possibilities to use the health data after the initial collection (for example, electronic health records), big data is chosen in this thesis as a basis for the analysis, because it has the most potential of violating the protection of personal data rules. When person's data are used without his/her consent and put into combination with other data, results of such big data processing might be used against the person (profiling) or the data might just be disclosed. It will be also discussed whether the data protection principles are in general justified in tha age of big data as suggested by some authors.

Although, normally each processing activity requires data subject's consent, there is an exception in the DPD and the GDPR according to which the processing for scientific, historical or statistical purposes shall be deemed to be incompatible with the initial purpose. If big data processing were to fall under this exception, big data processing could be concluded without the data subject's consent. The author of this thesis is in the opinion that when such processing would be allowed for big data, it would seriously breach the personal data protection principle. Therefore, the aim of this chapter is the answer the question whether it is possible to conclude big data processing on tha basis of the exception of scientific, historical or statistical purposes.

3.2 Big Data Processing

3.2.1 Notion of Big Data

Big data processing is defined as a practice when huge volumes of diversely sourced information are combined and analysed with the help of sophisticated algorithms. Big data relies on the increasing ability of technology to support the collection and storage of large amounts of data and also on its ability to analyse, understand and take advantage of the full value of data (in particular using analytics applications).[129] Another definition relies on the main characteristics of big data and describes it as high-volume, high-velocity and high-variety information assets that demand cost-effective, innovative forms of information processing for enhanced insight and decision making.[130] Following this definition, big data is often described in terms of the 'three Vs': volume, variety and velocity. By volume, it is meant that big data uses massive datasets, which are so large that they cannot be analysed using 'traditional' methods such as MS Excel spreadsheets, etc. By variety, it is meant that the data is brought together from different sources. Lastly, the notion of velocity stipulates that much of the big data analysis is done in high speed, sometimes even in real time.[131]

Many instances of big data processing do not involve personal data. For example, processing weather or traffic data can bring many useful insights to the climate change or organisation of cities. However, there are numerous cases of big data processing that do involve processing personal data, which triggers the application of data protection regulations. It is possible that the big data processing is the first processing activity and the data subject is giving his consent for such processing. Yet, big data processing often involves repurposing personal data that was obtained for a different purpose and in some cases by another organisation.[132] In addition, big data processing also has the potential to create new personal data. For example, social media and other data about an individual could be analysed to analyse that person's lifestyle as a factor determining whether they are at risk of developing a medical condition.[133]

---

[129] European Data Protection Supervisor. Opinion 7/2015. Meeting the challenges of big data. 19 November 2015. - https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2015/15-11-19_Big_Data_EN.pdf (25 March 2016), p 7.

[130] Gartner IT Glossary Big Data. http://www.gartner.com/it-glossary/big-data/ (25.04.2016)

[131] International Commissioner's Office. Big Data and Data Protection. - https://ico.org.uk/media/for-organisations/documents/1541/big-data-and-data-protection.pdf (25 March 2016), p 6-7.

[132] *Ibid*, p 9.

[133] *Ibid*, p 11.

Even when the data is at first anonymised, it can easily become personal data, as it is becoming increasingly convenient to infer a person's identity by combining allegedly 'anonymous' data with publicly available information such as that accessible through social media. Furthermore, with the rise of the 'Internet of Things', much of the data collected and communicated by the increasing number of personal and other devices and sensors will be personal data: the data collected can be easily related to the users of these devices whose behaviour they will monitor. These may include highly sensitive data including health information and information relating to our thinking patterns and psychological make-up.[134]

It is expected that big data may ultimately lead to better and more informed decisions. For example, big data may bring new discoveries in scientific and medical research, increase self-knowledge of individuals, enable to provide more personalised products, services and medical treatments better suited to an individual, and facilitate automated decision-making for businesses and other data processing organisations. These automated decisions, in turn, may lead to increased efficiency, with prospects of various commercial and other applications.[135] Big data will not only offer value to the society by research results, but the services and products generated from these results. Regarding health data, this value will mean better, quicker and cheaper diagnosis and treatment, as the application of big data to healthcare offers a way to accelerate research, improve treatment and reduce burden on the society overall.[136]

While big data has a potential of becoming beneficial to the society in many different ways, it has also raised serious concerns about its impact on the rights and freedoms of individuals, including privacy.[137] As previously mentioned, the main idea of big data is to gather as much data as possible for as many purposes as possible and to retain this data for as long as possible. This, however, conflicts with the basic principles of data protection, especially the principles of purpose limitation and data minimisation. Some advocates of big datahave argued that the rise of big data represents a fundamental challenge to established data protection principles and the current model based on stating purposes at the outset and obtaining consent for the processing no longer works because of the complexity of the

[134] European Data Protection Supervisor. Opinion 7/2015, p 7.

[135] *Ibid*, p 7.

[136] E. Morley-Fletcher. Healthy data? Horizon 2020 Projects: Portal. Issue 4. 30 March 2016. - http://www.horizon2020publications.com/H4/#100 (20.04.2016), p 101.

[137] European Data Protection Supervisor. Opinion 7/2015, p 7.

analytics and people's perceived lack of interest in how their data is used. Furthermore, some claim we risk losing the benefits that can be derived from big data if we attempt to confine it within an outdated framework of data protection.[138] Some even demand that derogations from the principles of purpose limitation and data minimisation should be made, because they do not take into account the propensity of big data to re-use data for different purposes.[139]

During the drafting of the GDPR, several institutions provided their views on the matters that, in their opinion, should be changed in the new regulation. While the applicability of the traditional data protection principles was brought up in the debates, most of the data protection institutions remained of the opinion that these principles carry a substance and value which could not be undermined or simply put aside. The Working Party issued a statement explaining that there is no reason to believe that the EU data protection principles are no longer valid and appropriate for the development of big data. Instead, they should be subject to further improvements to make them more effective in practice.[140]

In addition, the European Data Protection Supervisor also stated that in order to allow innovation and at the same time protect fundamental rights, the established principles of European data protection law should be preserved but applied in new ways.[141] In its Opinion 3/2015, the EDPS made clear that the current data protection principles, including necessity, proportionality, data minimisation, purpose limitation and transparency must remain as key principles. They provide the base line in order to protect the fundamental rights in a world of big data.[142] At the same time, these principles must be strengthened and applied more effectively, and in a more modern, flexible, creative, and innovative way. They must also be complemented by new principles such as accountability and data protection and privacy by design and by default. Increased transparency, powerful rights of access and data portability, and effective opt-out mechanisms may serve as preconditions to allow users more control over their data, and may also help contribute to more efficient markets for personal data, to

[138] International Commissioner's Office, p 40.

[139] European Data Protection Supervisor. Opinion 7/2015, p 8.; O. Tene, J. Polonetsky. Privacy in the age of big data: a time for big decisions. Stanford Law Review Online, Vol 64:63, February 2, 2012, p 68.

[140] Article 29 Working Party. Statement on Statement of the WP29 on the impact of the development of big data on the protection of individuals with regard to the processing of their personal data in the EU. Adopted on 16 September 2014. WP 221. - http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp221_en.pdf (18.04.2016), p 2.

[141] European Data Protection Supervisor. Opinion 7/2015, p 16.

[142] European Data Protection Supervisor. Opinion 3/2015. Europe's big opportunity. 27 July 2015. https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2015/15-07-27_GDPR_Recommendations_EN.pdf (25 March 2016), p 5.

the benefit of consumers and businesses alike.[143] UK's Information Commissioner's Office agreed with the EDPS's view in its opinion 'Big Data and Data Protection'. They stated that the data protection principles should not be seen as a barrier to progress. As the current principles have some flexibility, they could instead be used as a framework to promote privacy rights. [144]

In sum, it was generally agreed that traditional data protection principles should not be changed in order to facilitate the big data processing. Following the negotiations over the text of the GDPR, the principles did remain unchanged. However, several other changes were made in order to facilitate the use of big data processing while preserving sufficient protection of personal data.

3.2.2 Big Data in mHealth

Big data is expected to have a significant positive impact on healthcare. It allows establishing connections and extracting additional information from the sets of previously unrelated data, providing new insights for medical research, that were impossible to obtain before.[145] It will make it possible to link diseases to human behaviour, lifestyle or other causes that are characteristic of a given geographic area or group of people. Big data may also facilitate decision-making or collection of relevant information on the user side.[146]

Nonetheless, big data might also pose a risk to data subjects when the insights obtained are commercially exploited. For example, when a pharmaceutical company is able to identify the financial resources of its customers and their need for a specific drug (while combining data collected through different apps the person is using), the company might want to charge more from these customers who have better financial possibilities. In that case, big data would facilitate group discrimination. Therefore, there is a direct relationship between the availability of large sets of health data and the potential profitability of a number of industries active in the healthcare sector. Moreover, the widespread collection of sensitive health data will open the door to profiling and possible adverse selection, for example for employment or

[143] European Data Protection Supervisor. Opinion 7/2015, p 16.

[144] International Commissioner's Office, p 4.

[145] D. Boyd, K. Crawford. Six Provocations for Big Data. - Paper to be presented at Oxford Internet Institute's "A Decade in Internet Time: Symposium on the Dynamics of the Internet and Society" on September 21, 2011. - http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1926431 (20.04.2016), p.3

[146] EDPS Opinion, p 9.

insurance purposes. For example, there is a possibility that insurance companies start promoting the use of monitoring devices and genetic screenings, by giving better payment conditions to persons who monitor their health. However, if all insurance companies and private healthcare providers adopt an in-depth monitoring of personal health data as a standard practice in order to adapt their commercial offering to each customer, they may automatically refuse coverage to those who object to such disclosure or sharing, regardless of their health conditions or risk factors. As a result, the practice of sharing data will automatically result in discrimination against those who prefer not to disclose or share their health data.[147] In order to avoid the exploitation of personal data and discrimination based on data sharing, the safeguards must be used and the users must be aware of the rights they have under the data protection regulations.[148]

The last pages of the thesis will focus on the possibilities how the big data processing of health data collected through mHealth fits under the current and future rules and whether these rules provide enough protection for individual privacy.

3.2.3 Big Data Processing for Scientific, Historical or Statistical

As explained in chapter 2, the purpose of the data processing must be determined and disclosed to the data subject and processing which does not fall under the initial processing is not legitimate. Under regular circumstances, each data processing activity should be individually analysed and decided whether the personal data is processed in a way compatible with the set purposes. However, Art 6 (1) (b) of the DPD which stipulates the purpose limitation principle, also allows further processing of data for historical, statistical and scientific research purposes. This means that when data is used for these named purposes, the purpose is considered as compatible. However, in that case, appropriate safeguards must be used. It is noted in Recital 29 of the DPD that the typical purpose of the safeguards is to 'rule out' that the data will be used to support measures or decisions regarding any particular individual. The term 'rule out' suggests that the safeguards should indeed be strong enough to exclude or at least minimise any risks to the data subjects.[149] Under the current DPD framework, it is up to each member state to specify the appropriate safeguards. This specification is typically provided in legislation, which could be precise or more general. In

[147] EDPS Opinion, p 10.

[148] *Ibid*, p 9.

[149] Working Party, Opinion 03/2013, p 28.

Art 5 (1) (b) of the GDPR, instead of giving member states the right to determine relevant safeguards, reference is made to Art 89, which stipulates that the safeguards must be in accordance with the GDPR, meaning that member states do not have the discretion to determine safeguards in their national laws. While there is no definitive list of the appropriate safeguards, pseudonymisation is brought as an example. The GDPR requires that technical and organisational measures shall be in place in order to ensure respect for the principle of data minimisation.

In addition to the reference to safeguards, the provision concerning the purpose limitation principle in the GDPR sets a new exception to the purpose limitation principle. According to Art 5 (1) (b) the further processing for archiving purposes in the public interest shall not be considered as incompatible with the initial purposes. The author of this thesis finds that big data processing would not fall under this exception. Firstly, the core of the big data processing is to actively use the data, not only store it. Secondly, even when the data is stored for further big data processing, it would already exceed the limits of this exception. The author thus believes that the notion 'archiving for public interest' rather means the storage of data by state institutions.

As the provision of purpose limitation principles remains the same in the DPD and the GDPR, the following analysis of the three exceptions – scientific, historical, statistical purpose – applies to both the DPD and the GDPR. Firstly, 'statistical' purposes covers a wide range of processing activities, from commercial purposes (e.g. analytical tools of websites or big data applications aimed at market research) to public interests (e.g. statistical information produced from data collected by hospitals to determine the number of people injured as a result of road accidents).[150] Although Article 29 Working Party has categorised big data analysis under the 'statistical' purposes in its opinion on purpose limitation principle, there are different standings on whether the big data analysis falls under this exception.

Secondly, processing for 'historical' purposes can also have specific characteristics and this may require a different set of safeguards. Member states often have specific laws governing access to national archives, archives on recent history of particular interest and court files kept by the judiciary.[151] Therefore, this exception can be seen as relating to the 'archiving for

[150] Working Party. Opinion 03/2013, p 29.

[151] *Ibid*, p 29

public interest' exception. While the latter makes it possible to archive the data, the former makes it possible to process the archived data for historical purposes.

Thirdly, the 'scientific' purposes are meant for a situation when there may be a need to access different kinds of data. For example, some research may require raw microdata, which are only partially anonymised or pseudonymised. In other cases, research purposes involved can only be fulfilled if the pseudonymisation is reversible: for example, when research subjects need to be interviewed at a later stage in a longitudinal study. Further, publication of research results should, as a rule, be possible in such a way that only aggregated and/or otherwise fully anonymised data will be disclosed.[152]

A question arises whether it is possible to use the exception for scientific, historical and statistical purposes when processing health data. The Working Party has expressed an opinion that further processing of personal data concerning health (in addition to data about children, other vulnerable individuals, or other highly sensitive information) should, in principle, be permitted only with the consent of the data subject. Any exceptions to this requirement for consent should be specified in law, with appropriate safeguards, including technical and organisational measures to prevent undue impact on the data subjects (in case of doubt, the processing should be subject to prior authorisation of the competent data protection authority); exceptions should only apply with regard to research that serves an important public interest, and only if that research cannot possibly be carried out otherwise.[153] The Working Party's opinion has been also included to the GDPR by expressing the same view in Recital 53[154] and Art 9 (2) (j). Art 9 (2) (j) gives an exception to the prohibition on processing health data and allows it when processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Art 89 (1) based on the EU or member state law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and

[152] Working Party. Opinion 03/2013, p 29.

[153] *Ibid*, p 32.; See also: amendments 334-342 of the Draft report of the Committee on Civil Liberties, Justice and Home Affairs (LIBE) dated 16.1.2013 (2012/0011(COD) ('Draft LIBE Committee Report').

[154] GDPR, recital 53: Special categories of personal data which merit higher protection should be processed for health-related purposes only where necessary to achieve those purposes for the benefit of natural persons and society as a whole, in particular in the context of the management of health or social care services and systems, including processing by the management and central national health authorities of such data for the purpose of quality control, management information and the general national and local supervision of the health or social care system, and ensuring continuity of health or social care and cross-border healthcare or health security, monitoring and alert purposes, or for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, based on Union or Member State law which has to meet an objective of public interest, as well as for studies conducted in the public interest in the area of public health.

specific measures to safeguard the fundamental rights and the interests of the data subject. Therefore, in theory, it is possible to carry out big data processing with health data while relying on the scientific purpose exception. However, as Recital 53 emphasises that in such case the research should meet an objective of public interest. Also, Recital 53 points out the management and central national health authorities as the conductors of such research and other permitted activities.

It can be concluded that big data processing may fall under the exception from the purpose limitation principle, when the big data processing serves a scientific, historical or statistical purpose. However, the lawfulness of the big data processing of the data gathered in mHealth depends largely on the greater purpose of the big data processing and the processors. If the big data processing were to be carried out by state institutions in order to carry out a research for the welfare of the public, the big data processing would be lawful even without the consent of the data subjects. However, when a private company wishes to carry out big data processing for the benefit of itself or even for the benefit of, for example, users of one specific app, a separate consent would have to be asked from the data subjects.

3.2.4 Big Data Processing for Other Purposes

Concerning the safeguards to be adopted, the notion of functional separation may be of particular relevance. Functional separation means that data used for statistical purposes or other research purposes should not be available to support measures or decisions that are taken with regard to the individual data subjects concerned (unless specifically authorised by the individuals concerned). To comply with this requirement, controllers need to guarantee the security of the data, and take all other necessary technical and organisational measures to ensure functional separation.[155] The other possible safeguards include full anonymisation and partial anonymisation.[156] Directly identifiable personal data may be processed only if anonymisation or partial anonymisation is not possible without frustrating the purpose of the processing, and further provided that other appropriate and effective safeguards are in place.

When big data processing does not fall under the scientific, statistical and historical purpose exception, it must be evaluated whether there might be another ground for making such processing legitimate. The firmest ground would be asking for the consent from the data

[155] Working Party. Opinion 03/2013, p 30.

[156] *Ibid*, p 30.

subject. However, one of the virtues of the big data processing lies in the fact that while analysing large amounts of data which are gathered from different sources, it is possible to come to conclusions or discover correlations that are in the first place not even sought.[157] This means that it is nearly impossible to obtain valid consent from the data subject when at the time of asking consent even the data controllers do not know for what purposes exactly the data will be used. At the same time, the potential of big data would be wasted if there is no possibility to further process the data to discover unknown correlations. The DPD is rather strict concerning further processing of data, unless it is concluded for scientific, historical or statistical purposes. However, the Working Party has expressed an opinion that the fact the further processing is for a different purpose does not necessarily mean that it is automatically incompatible and this needs to be assessed on a case-by-case basis.[158]

According to the UK's Information Commissioner's Office, the key factor in deciding whether a new purpose is incompatible with the original purpose is whether it is fair. This means it is necessary to consider how the new purpose affects the privacy of the individuals concerned and whether it is within their reasonable expectations that their data could be used in this way.[159]

The GDPR is introducing more specific rules on factors a controller must take into account to assess whether a new processing purpose is compatible with the purpose for which the data were initially collected. Art 6 (4) of the GDPR lists the factors[160] which should be taken into account and it will be analysed how those factors should be viewed while big data processing is concluded with the health data collected in the mHealth apps.[161] The first factor includes whether there is any link between the purposes for which the personal data have been collected and the purposes of the intended further processing. The data subject is generally using the mHealth app in order to track his or her own health. The data might be just stored in the app or it might also be analysed in order to draw some conclusions from it, for example, to find out the average blood pressure during certain period of time. The author of this thesis finds that the link between tracking your own health and using this data for big data

[157] S. Barocas, H. Nissembaum. Big Data's End Run around Anonymity and Consent. – J. Lane, V. Stodden, S. Bender et al (eds.). Privacy, Big Data and the Public Good. Cambridge University Press 2014, p 60.; International Commissioner's Office, p 21.

[158] Working Party. Opinion 03/2013, p 21.

[159] International Commissioner's Office, p 22.

[160] GDPR, Art 6 (4) (a)-(e)

[161] See also GDPR, Recital 50.

processing is not strong enough in order to allow such processing without separate consent. The second factor concerns the context in which the personal data have been collected. In particular the relationship between data subjects and the controller, should be taken into account. The third factor requires to take into account the nature of the personal data, in particular whether special categories of personal data are processed or whether personal data related to criminal convictions and offences are processed. The author of this thesis is in the opinion that this clause is the biggest obstacle when trying to see big data processing as compatible with the initial purposes. Sensitive data in general and health data in particular enjoys much stricter protection and this clause shows that the stricter protection also applies to the compatibility of the further processing. The fourth factor stipulates that the possible consequences of the intended further processing for data subjects must be taken into account. The final factor requires to consider the existence of appropriate safeguards, which may include encryption or pseudonymisation. When combining the last two factors, it is possible that while using appropriate safeguards, the consequences for the data subject are not serious (the right to privacy is not breached). However, taking into account all factors above, the author concludes it is not possible that a further big data processing satisfies all the conditions and it could be considered as compatible further processing.

3.3 Conclusion of the Chapter

Due to health data's high value, it would be beneficial if this data could be used for more purposes than the initial one for which it was collected. However, this could easily conflict with the data subject's protection under the data protection rules. In the current chapter it was analysed whether it is possible to use the health data that has been collected in the mHealth apps for further processing without the consent of the data subject. Referring to the practices regarding big data, it can be concluded that such further use is not compliant with the rules of data protection, when the data subject has not given his/her consent.

Although there is a debate about the general principles of data protection initiated by some advocates of big data, it has been concluded by the data protection authorities that these principles cannot be undermined and they were also reinforced in the GDPR. Therefore, in order to legitimise big data processing without the data subject's consent, there must be special ground for it in the applicable law. The DPD and the GDPR allow further processing when it is carried out for scientific, historical or statistical purposes. While big data processing falls under the notion of statistical purposes and could be carried out when using

adequate safeguards, then the processing of health data adds even more conditions and requirements for using this exception. It stems from the Recital 53 and the Art 9 (2) (j) of the GDPR that this exception could be only used when there is public interest and by public institutions.

Working Party brought out four factors in order to evaluate whether the further use of data would be compatible with the initial purpose and therefore would allow the processing. However, the evaluation of these factors showed that while processing health data, enjoying stricter rules than 'regular' personal data, it would not be possible to legitimise big data processing without the data subject's consent or without completely anonymising the data. Therefore, the answer to the underlying question of this chapter is that the data subjects are protected from the further use of their personal data if they have not consented to it. However, as the further use of health data, especially while using the big data processing, has a potential of being beneficial to both the individuals and the whole society, a safe way of using this data should be promoted. For example, one possibility is anonymising the data, which, however, was not further discussed about as it was not the subject of the thesis.

CONCLUSION

The central question of this thesis was to determine whether the current EU data protection framework is sufficient in order to protect personal data in the field of mHealth. In addition, relevant changes to the framework were discussed in order to analyse whether there will be any changes in data protection in mHealth and whether they will strengthen the protection of personal data.

In the process of answering the first sub-question, it was concluded that personal data is being processed in the course of data processing in mHealth. Although the apps and devices of mHealth are different, it was shown on the basis of an example data set which conditions should be taken into account in determining whether personal data is processed.

Concerning health data, it was concluded that although the specific definition of health data was not included in the DPD, the content of the health data was in general same as it will be in the GDPR, because the notion of health data had been explained by courts and relevant data protection authorities.

The author argued that by adding a wording 'independent of its source' to the definition of health data, the notion of health data is broadened, thus making it independent from the provision of healthcare services. This is relevant regarding mHealth, as many apps measure health parameters but are not provided by health care professionals. Therefore, as the definition of health data explicitly says that the source of the data is not relevant when determining its status of health, data subjects can count on stricter protection of these health data that have been collected in mHealth apps.

The author of this thesis concluded that by adding the pseudonymisation tool to the GDPR, a better ground is established for the protection of personal data in mHealth. As the pseudonymisation of data does put a heavy burden on the data processors, but at the same time gives them several benefits, they are more likely willing to use the pseudonymisation tool. At the same time, individuals' rights are better protected under the data protection principles as it is more complicated to relate certain data to a specific person.

In addition, it was ascertained that regulations on medical devices also play a role in the protection of personal data. When an mHealth app or device is considered as a medical

device, specific requirements must be fulfilled to bring the product to the market which means that the compliance with the data protection rules will also be guaranteed. In addition, when a medical device is provided in the course of the provision of healthcare services, the consent of the data subject is not needed.

While answering the second sub-question, it was established that the traditional data protection requirements shall still be applicable to mHealth. The requirement of consent as a basis for making data processing legitimate was described and relevant problems were brought out through an example. The consent for health data processing should be informed, freely given and explicit. It was found that in mHealth, the most problematic requirement is the requirement of informed consent as it is complicated to give the data subject all relevant information through an app. As the data collected are health data, the consent shall also be explicit and, after the adoption of the GDPR, also in a written form. These requirements fulfil the purpose of protecting the data subject from the breach of his right to privacy, because while consenting to the processing he/she shall have every possible opportunity to understand what kind of processing he/she is consenting to.

The author reached a conclusion that while the application of traditional data protection principles as purpose limitation principle and data minimisation principle might be burdensome for the app developers, these principles are the most effective way to protect the users of an app from a situation in which their data could be harmed. In order to promote compliance with the principles and with the data protection requirement in general, a Code of Conduct for the app developers is being drafted, which the author finds to be a positive way to converge the data subjects' rights and the interests of app developers. Therefore, it was concluded that the traditional data protection requirements analysed are in general a sufficient way to protect personal data.

The final chapter analysed whether the health data collected in mHealth apps could possibly be used for further processing without the data subject's consent. As health data carries an immense value, these data could be utilized for purposes other than that initially collected for. Nevertheless, such conduct might often breach the data protection regulations protecting the data subject. Deriving from ordinary practices regarding big data, it can be established that further use of this kind violates the data protection rules if the data subject has not given his/her consent.

Despite an existing debate on general principles of data protection between some advocates of big data, the data protection authorities have concluded that these principles cannot be undermined, and a similar approach has further been reinforced in the GDPR. Thus, to legitimise big data processing without the data subject's consent, the applicable law must offer a special ground for this purpose.

The DPD and the GDPR permit further processing when it is performed for scientific, historical or statistical purposes. In case big data processing is conducted for statistical purposes and could be carried out with using adequate safeguards, the processing of health data raises even further conditions and requirements for this exception to become available. According to Recital 53 and Art 9 (2) (j) of the GDPR, this exception could only be used upon the existence of public interest and by public institutions.

Finally, it was brought out that there exists a possibility that even without the consent of the data subject, the further use might be compatible with initial purpose. Four factors brought out by the Working Party were examined and it was revealed that while processing health data, which already enjoys stricter rules than 'regular' personal data, legitimising big data processing without the data subject's consent or without completely anonymising the data would not be possible. Importantly, it can thus be concluded that the data subjects are protected from further use of their personal data if they have not consented to it. Nevertheless, as further use of health data, including big data processing carries great potential to become beneficial to both individuals and the whole society, a safe method of using such data should be promoted. One possibility would be anonymising the data – a topic, which certainly deserves further research attention.

Therefore, the answer to the thesis question must be answered that the current data protection rules are applicable to mHealth and they offer sufficient protection to personal data. It was concluded that some terms of personal data protection might be complicated to apply to the realities of mHealth or the traditional data protection principle might seem too burdensome for the use in mHealth. However, this does not mean they could not or should not be applied. In addition, the GDPR, which will enter into force in 2018, will not majorly amend the basic principles that should already now be taken into account in the field of mHealth, although it will offer some specification.

ANDMEKAITSE m-TERVISE VALDKONNAS. RESÜMEE

Tänapäeva maailmas on nutiseadmete kasutamine muutunud igapäevaelu lahutamatuks osaks ning turul on tuhandeid tarkvararakendusi, mis seadmed nö targaks teevad. Spetsiaalsed tarkvararakendused ehk äpid töötavad peamiselt andmetega. Andmed võivad sinna sisestada äppide kasutajad või need võivad tuleneda ka spetsiaalsetest seadmetest, millega äpp ühendatud on. Teatud äppe kasutatakse tervise ja meditsiini eesmärgil. Tegemist võib olla lihtsa äpiga, kuhu kasutaja saab ise oma terviseandmed sisestada, kuid tänapäeval on levinud ka erinevad seadmed, mis suudavad sensorite abil inimese terviseandmeid ise jälgida ning neid analüüsida. Kõik sellised äpid moodustavad mobiilse tervise ehk m-tervise valdkonna.

M-tervis võimaldab pakkuda tervishoiuteenuseid sõltumatu isiku ja arsti asukohast, kuid sellisel juhul on tegemist pigem telemeditsiini valdkonnaga, mida käesolev töö ei puuduta. Käesoleva töö fookuseks on andmed, mida m-tervise valdkonnas kogutakse ja töödeldakse. Kuigi suurel hulgal andmete kogumisel telefoni äppidesse on omad eelised, siis andmekaitse seisukohast võib selline tegevus pigem probleeme tekitada. Nimelt on äppides töödeldavate andmete näol üldjuhul tegemist isikuandmetega, tihtipeale ka terviseandmetega, mille töötlemise puhul tuleb kohaldada isikuandmete kaitse reegleid.

Käesolev töö võtab aluseks Euroopa Liidu andmekaitseõiguse. Nimelt on isiku õigus privaatsusele ja tema isikuandmete kaitsele olnud juba pikka aega Euroopas tunnustatud. Alates 1996. aastast reguleerib andmekaitse valdkonda Euroopa Parlamendi ja nõukogu direktiiv 95/46/EÜ üksikisikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta (edaspidi Direktiiv) ning sellest on saanud rahvusvaheline standard andmekaitseõiguse alal. Tulenevalt tehnoloogia arengust ja ühe suureneva andmete mahuga on aga alates 2010. aastast toodud esile vajadus üle-Euroopalise andmekaitsereformi järele. Pärast pikaajalisi läbirääkimisi võttis Euroopa Parlament 14. aprillil 2016 vastu Euroopa Parlamendi ja Nõukogu Määruse füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiivi 95/46/EÜ kehtetuks tunnistamise kohta (Isikuandmete kaitse üldmäärus) (edaspidi Määrus). Määruse sätteid hakatakse kohaldama 2018. aastal.

Käesoleva töö eesmärgiks on analüüsida praeguse ja tulevase Euroopa andmekaitseõiguse sobivust m-tervise valdkonnale. Nimelt on üha suurenevas andmete hulgas eriti oluline, et isikuandmed oleksid kaitstud, kuid juba 20 aastat tagasi vastu võetud Direktiiv ei pruugi

pakkuda piisavalt võimalusi ja kaitset sellise uue valdkonna nagu m-tervise jaoks. Töö hüpoteesiks on seatud, et Direktiivi sätted ei ole piisavad, et kaitsta isikuandmeid m-tervise valdkonnas ning ka uue Määruse tulemine ei muuda olukorda, sest Määruse muudatused ei ole piisavalt täpsed ja konkreetsed, et neid m-tervise valdkonnale kohaldada. Seega on töö keskseks uurimisküsimuseks, kas praegune ning tulevane Euroopa Liidu andmekaitse regulatsioon tagab piisava isikuandmete kaitse m-tervise valdkonnas. Küsimusele vastamiseks on töö jagatud kolme peatükki, mis omakorda on jagatud alapeatükkideks.

Töö kirjutamisel on kasutatud nii hetkel kehtivat Direktiivi kui uut Määrust, et teha kindlaks, millised sätted m-tervisele kohalduvad ning millised on muutused Määruses. Õigusaktide sisustamisel on kasutatud suurel hulgal erinevate andmekaitseorganisatsioonide arvamusi. Kuigi m-tervise teemat ei ole veel akadeemiliselt väga palju uuritud, on siiski kasutatud mõningaid varasemaid töid.

Esimene peatükk on pigem kirjeldava iseloomuga ning selle eesmärgiks on kaardistada andmekaitse mõisted, mis on m-tervise valdkonnas relevantsed ning nende kohaldamine m-tervisele. Andmekaitse keskseks mõisteks on isikuandmed, sest nende töötlemine toob endaga kaasa andmekaitseõiguse kohaldamise. Isikuandmed on igasugune teave tuvastatud või tuvastatava füüsilise isiku kohta. Kuna isikuandmete mõiste on võrdlemisi lai, siis toimub nutiseadmetes olevates äppides pidev isikuandmete töötlemine, sest seadmete kasutajateks on füüsilised isikud, kes üldjuhul sisestavad sinna infot enda kohta.

Isikuandmete eraldi kategooria moodustavad spetsiaalset kaitse vajavad isikuandmed, mille hulka kuuluvad ka terviseandmed. Kuna m-tervise valdkonnas töödeldakse suurel määral just tervisandmeid ning nendele on tagatud eriline kaitse, on oluline terviseandmete mõiste lahtiseletamine. Kuigi Direktiivis terviseandmete definitsiooni ei ole, siis kohtud on mitmel üksikjuhul analüüsinud, mida saab pidada terviseandmeteks. Tulenevalt aga interneti ning mobiilside levikust ei toimu enam terviseandmete vahetamine rangelt arsti ja patsiendi või näiteks töötaja ja tööandja vahel, vaid tervisandmed võivad liikuda andmesubjektilt mistahes töötlejale erinevaid viise pidi. Seega on vaja täpsemalt määratleda terviseandmete definitsioon. Määrus seda ka teeb, kuid töö autor jõudis järeldusele, et tegelikult ei sisalda siiski definitsioon midagi uut võrreldes varasema kohtupraktika ja autoriteetide arvamusega.

M-tervise valdkonnas on probleemkohaks tervisandmete eristamine nö ’heaolu andmetest’. Selle all peetakse silmas andmeid, mis võivad küll kaudselt olla seotud inimese tervisliku

seisundiga, nt füüsiline aktiivsus, tarbitud kalorite arv, alkoholitarbimine, kuid mille puhul liiga väikse andmete hulgaga järeldusi ei saa teha. Direktiivi Artikkel 29 alusel loodud töögrupi (edaspidi Töögrupp) juhistest selgub, et üldjoontes on kolm liiki andmeid, mis just m-tervise valdkonnas kujutavad endast terviseandmeid: meditsiinilised andmed; nö toored andmed, mille puhul saab teha järeldusi inimese tervise kohta, kui neid kombineerida teiste andmetega; ning inimese tervise kohta juba tehtud järeldused.

M-tervise äppide ja seadmete puhul on oluline analüüsida ka meditsiiniseadmete mõistet. Nimelt kui tegemist on meditsiiniseadmega 93/42/EMÜ direktiivi alusel, siis kohalduvad sellele spetsiaalsed reeglid, mille mõju ulatub ka andmekaitse valdkonda. Nimelt on sellisel juhul tegemist arsti-patsiendi suhtega ning terviseandmete töötlemiseks ei pea küsima eraldi nõusolekut. Samas on meditsiiniseadmete turule toomiseks spetsiifilised nõuded ning nende alla käivad ka andmekaitse põhimõtetega kooskõlas olemine.

Teise peatüki eesmärk on vastata küsimusele, kas andmekaitseõiguse peamised nõuded ja printsiibid on sobivad m-tervises kasutamiseks ning kas nende kohaldamine on võimalik. Isikuandmete töötlemisel peab olema töötlemiseks üks kuuest Direktiivi Art 7 toodud alusest. Esimene ja kõige eelistatum nendest alustest on andmesubjekti nõusolek andmete töötlemiseks. Nõusolekule kohalduvad aga teatud tingimused. Nimelt peab nõusolek olema vabatahtlik, konkreetne ja teadlik tahteavaldus. M-tervise valdkonnas pole tavaliselt probleeme vabatahtlikkuse kriteeriumiga, kuid teised kaks kriteeriumi võivad neid tekitada. Nimelt tähendab konkreetsuse kriteerium seda, et andmesubjekt saab anda kehtiva nõusoleku ainult sellisel juhul, kui nõusolek käib piiratud andmete kohta piiratud ajal ning teada on andmete töötlemise eesmärk. Selliste piirangute seadmine ei pruugi aga kasulik olla äpi arendajale, sest ta ei saa kogutud andmeid hiljem kasutada, mis võib talle väga kasulikuks osutuda.

Probleemne on ka informeerituse kriteerium, sest väikse m-tervise seadme kaudu on keeruline edasi anda kogu vajalikku infot töötlemise kohta. Kuigi Töögrupp on välja pakkunud nö kihilise nõusoleku vormi (nõusolekut küsitakse ühel äpi lehel ning enne selle andmist on võimalik tutvuda tingimustega eraldi keskkonnas või veebiaadressil), siis töö autori hinnangul vähendab see nõusoleku väärtust, sest ühel hetkel hakkavad inimesed andma nõusolekut ilma tegelikult süvenemata, millele nad nõusoleku annavad.

Tervisandmete töötlemisel peab tulenevalt Direktiivi Art 8 (2) (a) nõusolek lisaks olema selgesõnaline ning tulenevalt Määruse Art 7 (1) taas esitataval kujul. Sellised nõuded aitavad paremini tagada terviseandmete kaitse.

Teise peatüki teine osa tegeleb andmekaitse printsiipidega. Nimelt peab kogu isikuandmete töötlemine olema kooskõlas Direktiivi Art 6 (1) printsiipidega. Käesolevas töös on analüüsimiseks valitud andmete minimaalsuse printsiip ja eesmärgipärasuse printsiip, sest just need printsiibid on ühest küljest kõige olulisema isikuandmete kaitse tagamisel, kuid teisalt tekitavad probleeme m-tervise valdkonnas kohaldamisel.

Andmete minimaalsuse printsiip tähendab seda, et andmeid ei või koguda liigsetes kogustes, nt tuleviku tarbeks igaks juhuks. Kui andmete töötlemise eesmärk on lõppenud, tuleb andmed isikule tagastada. M-tervise valdkonnas tähendab see, et kuigi andmetöötlejal oleks väga kasulik hoida enda valduses kõiki andmeid, mis ta on isikutelt saanud, et neid edasi töödelda muude eesmärkide saavutamiseks, siis tegelikult ta seda teha ei tohi.

Eesmärgipärasuse printsiibi kohaselt peab iga andmetöötlus lähtuma mingist konkreetsest eesmärgist ning selles piiridest ei või väljuda. M-tervise seisukohast tähendab see, et äpi looja ei või muuta äpis kasutatavate isikuandmete töötlemise eesmärki ilma selleks enne andmesubjektilt nõusolekut küsimata.

Töö kolmas osa keskendub andmete hilisemale töötlemisele. Nimelt on teatud juhtudel võimalik töödelda isikuandmeid pärast esimese töötlemise lõppu ilma selleks isikult nõusolekut küsimata. Töö autor leiab, et kui selline võimalus rakendub ka *big data* ehk suurandmete töötlemisprotsessile, siis võib see olulisel määral kahjustada isikute privaatsusele.

Nimelt on suurandmete töötlemise puhul võimalik jõuda järeldusteni, mis võivad kahjustada isikut (profileerimine) või võivad läbi suurandmete töötlemise lekkida isikuandmed kolmandate osapoolte kätte. Üheks võimalikuks aluseks, et suurandmete töötlemine oleks seaduspärane on Direktiivi Art 6 (1) (b), mis lubab isikuandmete hilisema töötlemise juhul, kui see viiakse läbi ajaloo, statistika või teadusega seotud eesmärkidel. Kuigi Töögrupp on paigutanud suurandmete töötlemise statistika valdkonda, siis tervisandmete sellisel viisil töötlemine pole siiski lubatud.

Lisaks on Töögrupp avaldanud arvamust, et isegi kui tegemist pole ajaloo, statistika või teadusega seotud eesmärkidel töötlemisega, siis ei saa välistada, et hilisem töötlemine on siiski kooskõlas esialgse töötlemise eesmärkidega. Ka siin on välja toodud kriteeriumid, mille alusel kooskõla hinnata. Üks kriteeriumitest ütleb, et hinnata tuleb isikuandmete liiki ning fakt, et töödelda tahetakse terviseandmeid on töö autori hinnangul piisav alus sellise töötlemise mitte lubamiseks ilma andmesubjekti nõusolekuta.

Töö lõpuks jõuab autor vastupidisele seisukohale sissejuhatuses püstitatust ning lükkab hüpoteesi ümber. Nimelt selgub vastavatele uurimisküsimustele vastates, et kuigi m-tervise valdkond toob oma uudsusega kaasa mõningaid raskusi andmekaitseõiguse kohaldamisel, on tegelikult kõik peamised andmekaitse printsiibid ja nõuded sobivad ka selleks, et tagada m-tervises isikuandmete piisav kaitse.

LIST OF USED MATERIALS

Literature

1. Barocas, S., Nissembaum, H. Big Data's End Run around Anonymity and Consent. – J. Lane, V. Stodden, S. Bender et al (eds.). Privacy, Big Data and the Public Good. Cambridge University Press 2014.
2. Boyd, D., Crawford, K. Six Provocations for Big Data. - Paper to be presented at Oxford Internet Institute's "A Decade in Internet Time: Symposium on the Dynamics of the Internet and Society" on September 21, 2011. - http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1926431 (20.04.2016).
3. Buttarelli, G. The EU GDPR as a clarion call for a new global digital gold standard. – International Data Privacy Law, Guest Editorial. - http://www.oxfordjournals.org/our_journals/idpl/featured.html (28.04.2016).
4. Carey, E., Cherney, K. The Best Diabetes iPhone and Android Apps of 2015. - http://www.healthline.com/health/diabetes/top-iphone-android-apps#2 (4.04.2016).
5. Cuijpers, C., Purtova, N., Kosta, E. Data Protection Reform and the Internet: the draft Data Protection Regulation. - Tilburg Law School Research Paper 2014, No. 3. - http://ssrn.com/abstract=2373683 (05.04.2014).
6. Danagher, L., An Assessment of the Draft Data Protection Regulation: Does it Effectively Protect Data? - European Journal of Law and Technology, Vol. 3, No. 3, 2012.
7. Gutwirth, S. Short Statement about the role of consent in the European Data Protection Directive. 2012. - https://works.bepress.com/serge_gutwirth/80/ (10.04.2016).
8. Handbook on European Data Protection Law. Luxembourg: Publications Office of the European Union, 2014.
9. Koot, M. R., Measuring and Predicting Anonymity, Amsterdam: Informatics Institute cop., 2012.
10. Kotschy, W. The proposal for a new General Data Protection Regulation - problems solved? - International Data Privacy Law, 2014, Vol. 4, No. 4, p 274-281.

11. Lones, S. Next generation of diabetes wearables. - http://www.diabeticconnect.com/diabetes-information-articles/general/1032-next-generations-of-diabetes-wearables (4.04.2016).
12. Mantovani, E., Quinn, P. mHealth and data protection – the letter and the spirit of consent legal requirements. International Review of Law, Computers & Technology, 28:2, 2014, p 222-236.
13. Morley-Fletcher, E. Healthy data? Horizon 2020 Projects: Portal. Issue 4. 30 March 2016. - http://www.horizon2020publications.com/H4/#100 (20.04.2016).
14. Rubinstein, Ira S Big data. The end of privacy or a new beginning? International Data Privacy Law 25 January 2013. http://idpl.oxfordjournals.org/content/early/2013/01/24/idpl.ips036.full.pdf+html;
15. Tene, O., Polonetsky, J. Privacy in the age of big data: a time for big decisions. Stanford Law Review Online, Vol 64:63, February 2, 2012.
16. Van der Sloot, B. Do data protection rules protect the individual and should they? An assessment of the proposed General Data Protection Regulation. - International Data Privacy Law, 2014, Vol. 4, No. 4.

Legislation

1. Charter of Fundamental Rights of the European Union. - OJ C 326, 26.10.2012, p. 391–407.
2. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Council of Europe, CETS No. 108, 1981.
3. 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.
4. European Convention on Human Rights (entry into force 4.11.1950). - http://www.echr.coe.int/Documents/Convention_ENG.pdf
5. Personal Data Protection Act. - RT I 2007, 24, 127
6. The EU Charter of Fundamental Rights. Commentary. Hart Publishing: Oxford, p 253.

Case law

1. ECJ, Judgment of 6 November 2003, Case C-101/01 - Bodil Lindqvist.
2. ECtHR, I v Finland, No. 20511/03, 17 July 2008.
3. CJEU 16.10.2012, C-614/10, Commission vs Austria.

Other sources

1. A comprehensive approach on personal data protection in the European Union. Communication from the commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions. Brussels, 4.11.2010 COM (2010) 609 final. - http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_en.pdf (15.03.2016).
2. A comprehensive approach on personal data protection in the European Union. Communication from the commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions. Brussels, 4.11.2010 COM (2010) 609 final. - http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_en.pdf (15.03.2016),
3. Article 29 Working Party, Advice Paper on Special Categories of Data (sensitive data). - http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2011/2011_04_20_letter_artwp_mme_le_bail_directive_9546ec_annex1_en.pdf (20.02.2016).
4. Article 29 Working Party, Annex (Health data in apps and devices) to a Letter to European Commission in answer to Green Paper, 05.02.2015. - http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2015/20150205_letter_art29wp_ec_health_data_after_plenary_annex_en.pdf (20.02.2016)
5. Article 29 Working Party, Letter to EU Council president, Annex 2: Proposals for Amendments regarding exemption for personal or household activities, Brussels, 11 December 2013. - http://ec.europa.eu/justice/data-protection/article-

29/documentation/other-document/files/2013/20130227_statement_dp_annex2_en.pdf (20.03.2016).

6. Article 29 Working Party, Letter to Mr Jan Philipp ALBRECHT, 17 June 2015, available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2015/20150617_letter_from_the_art29_wp_on_trilogue_to_mralbrecht_en.pdf, (18 March 2016).
7. Article 29 Working Party, Letter to Mr Jan Philipp ALBRECHT, Appendix, 17 June 2015, available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2015/20150617_appendix_core_issues_plenary_en.pdf, (18 March 2016).
8. Article 29 Working Party, Opininon on apps on smart devices, adopted on 27 February 2013, WP 202. - http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp202_en.pdf (20.03.2016).
9. Article 29 Working Party, Opinion 01/2012 on the data protection reform proposals, adopted on 23 March 2012, WP 191. - http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp191_en.pdf (3.04.2016).
10. Article 29 Working Party, Opinion 05/2014 on Anonymisation Technique, adopted on 10 April 2014, WP216. - http://www.cnpd.public.lu/fr/publications/groupe-art29/wp216_en.pdf (13.02.2016).
11. Article 29 Working Party, Opinion 15/2011 on the definition of consent, adopted 13 July 2011, WP187. - http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp187_en.pdf (20.03.2016).
12. Article 29 Working Party, Opinion 4/2007 on the concept of personal data, adopted on 20th June, WP136. - http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf (10.02.2016).
13. Article 29 Working Party, Working Document on data protection issues related to RFID technology, adopted on 19.1.2005. - http://www.cnpd.public.lu/en/publications/groupe-art29/wp105_en.pdf (10.02.2016).

14. Article 29 Working Party, Working Document on the processing of personal data relating to health in electronic health records, adopted on 15 February 2007, WP131. - http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2007/wp131_en.pdf (23.03.2016)

15. Article 29 Working Party, Working Party on Police and Justice, The Future of Privacy: Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data", 1 December 2009, WP 168. - http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp168_en.pdf (20.03.2016).

16. Article 29 Working Party. Opinion 03/2013 on purpose limitation. Adopted on 2 April 2013. WP 203. - http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf (18.03.2016)

17. Article 29 Working Party. Opinion 10/2004 on More Harmonised Information Provisions, Adopted on 25th November 2004, WP 100. - http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2004/wp100_en.pdf (3.04.2016).

18. Article 29 Working Party. Statement on Statement of the WP29 on the impact of the development of big data on the protection of individuals with regard to the processing of their personal data in the EU. Adopted on 16 September 2014. WP 221. - http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp221_en.pdf (18.04.2016).

19. Commission Nationale de l'Informatique et des Libertés (CNIL), Le Corps, Nouvel Object Connecté, Chaiers IP no 2.

20. Commission proposes a comprehensive reform of data protection rules to increase users' control of their data and to cut costs for businesses. - European Commission Press Release. Brussels, 25 January 2012. - http://europa.eu/rapid/press-release_IP-12-46_en.htm?locale=en (17.04.2016).

21. Draft of the Code of Conduct of mHealth

22. Draft report of the Committee on Civil Liberties, Justice and Home Affairs (LIBE) dated 16.1.2013 (2012/0011(COD) ('Draft LIBE Committee Report').

23. European Data Protection Supervisor. Opinion 1/2015 Mobile Health, 21 May 2015. - https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2015/15-05-21_Mhealth_EN.pdf (5.03.2016).

24. European Data Protection Supervisor. Opinion 3/2015. Europe's big opportunity. 27 July 2015. https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2015/15-07-27_GDPR_Recommendations_EN.pdf (25 March 2016).

25. European Data Protection Supervisor. Opinion 7/2015. Meeting the challenges of big data. 19 November 2015. https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2015/15-11-19_Big_Data_EN.pdf (25 March 2016).

26. Gartner IT Glossary Big Data. http://www.gartner.com/it-glossary/big-data/ (25.04.2016).

27. Guidelines on the Qualification and Classification of Stand Alone Software Used in Healthcare within the Regulatory Framework of Medical Devices. European Commission, DG Health and Consumer, Directorate B, Unit B2 'Health Technology and Cosmetics'. January 2012.

28. International Commissioner's Office. Big Data and Data Protection. https://ico.org.uk/media/for-organisations/documents/1541/big-data-and-data-protection.pdf (25 March 2016).

29. International telecommunication Union. Filling the gap: Legal and Regulatory Challenges of Mobile Health (mHealth) in Europe, 2014. - https://www.itu.int/en/ITU-D/Regional-Presence/Europe/Documents/ITU%20mHealth%20Regulatory%20gaps%20Discussion%20Paper%20June2014.pdf (20.03.2016).

30. mHealth – Digital Single Market. European Commission. - https://ec.europa.eu/digital-single-market/en/mhealth (28.04.2016).

31. Mobile health app market report 2013–2017: The commercialization of mHealth. Research2Guidance. - http://www.researchandmarkets.com/reports/2497392/mobile_health_app_market_report_20132017 (5.02.2016).

32. Position of the Council at first reading with a view to the adoption of a Regulation of the European Parliament and of the Council 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). ST 5419 2016 INIT - 2012/011 (OLP). Brussel, 6 April 2016. - http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_5419_2016_INIT&from=EN (1.05.2016).

33. Position of the Council at first reading with a view to the adoption of a Directive of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA. ST 5418 2016 INIT - 2012/010 (OLP). Brussels, 6 April 2016. - http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_5418_2016_INIT&qid=1462066004286&from=EN (1.05.2016).

34. Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) [first reading] Analysis of the final compromise text with a view to agreement. Brussels, 15 December 2015. - http://statewatch.org/news/2015/dec/eu-council-dp-reg-draft-final-compromise-15039-15.pdf (15 February 2016).

35. Special Eurobarometer 359. Attitudes on Data Protection and Electronic Identity in the European Union. June 2011. - http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf (23.03.2016).

36. What is telemedicine? – American Telemedicine Association. - http://www.americantelemed.org/about-telemedicine/what-is-telemedicine#.VyUgylaLRmM (28.04.2016).

37. World Economic Forum Unlocking the value of personal data; from collection to usage. World Economic Forum February 2013 http://www3.weforum.org/docs/WEF_IT_UnlockingValuePersonalData_CollectionUsage_Report_2013.pdf

Lihtlitsents lõputöö reprodutseerimiseks ja lõputöö üldsusele kättesaadavaks tegemiseks

Mina, Kärt Raud (sünnikuupäev: 16.02.1991),

1. annan Tartu Ülikoolile tasuta loa (lihtlitsentsi) enda loodud teose „Data Protection in mHealth," mille juhendajateks on Dr. Helen Eenmaa-Dimitrieva ja Mati Kaalep,

1.1. reprodutseerimiseks säilitamise ja üldsusele kättesaadavaks tegemise eesmärgil, sealhulgas digitaalarhiivi DSpace-is lisamise eesmärgil kuni autoriõiguse kehtivuse tähtaja lõppemiseni;

1.2. üldsusele kättesaadavaks tegemiseks Tartu Ülikooli veebikeskkonna kaudu, sealhulgas digitaalarhiivi DSpace i kaudu kuni autoriõiguse kehtivuse tähtaja lõppemiseni.

2. olen teadlik, et punktis 1 nimetatud õigused jäävad alles ka autorile.

3. kinnitan, et lihtlitsentsi andmisega ei rikuta teiste isikute intellektuaalomandi ega isikuandmete kaitse seadusest tulenevaid õigusi.

Tartu, 02.05.2016.a