Alma Mater Studiorum – Università di Bologna
In collaborazione con LAST-JD consortium:
Università degli studi di Torino
Universitat Autonoma de Barcelona
Mykolas Romeris University
Tilburg University

DOTTORATO DI RICERCA IN

Erasmus Mundus Joint International Doctoral Degree in Law,

Science and Technology

Ciclo 30–A.Y. 2014/2015

Settore Concorsuale di afferenza: 12H3

Settore Scientifico Disciplinare: IUS/20

mHealth apps and Right to Data Portability: Law and Reality

Presentata da: Andrijana Nikchevska

Coordinatore Dottorato **Supervisore**

Prof. Giovanni Sartor **Prof. Giovanni Sartor**

Esame finale anno 2019

Alma Mater Studiorum – Università di Bologna
In partnership with LAST-JD consortium:
Università degli studi di Torino
Universitat Autonoma de Barcelona
Mykolas Romeris University
Tilburg University

PhD Programme in

Erasmus Mundus Joint International Doctoral Degree in Law,

Science and Technology

Cycle 30–A.Y. 2014/2015

Settore Concorsuale di afferenza: 12H3

Settore Scientifico Disciplinare: IUS/20

mHealth apps and Right to Data Portability: Law and Reality

Submitted by: Andrijana Nikchevska

The PhD Programme Coordinator **Supervisor**

Prof. Giovanni Sartor **Prof. Giovanni Sartor**

Year 2019

Alma Mater Studiorum,

Università di Bologna

DISSERTATION Presented

on 28-29/03/2019 in Bologna

to obtain the degree of

DOTTORATO DI RICERCA

IN LAW, SCIENCE AND TECHNOLOGY

by

Andrijana Nikchevska,

Born on 2 August 1981 in Skopje, Macedonia

Dissertation defence committee:

To my son Ian and my family, for their unconditional support on this journey

Abstract

Il soggetto di questo studio, come indicato dal titolo, è il diritto alla portabilità dei dati nel contesto delle mHealth apps- o applicazioni su dispositivi mobili per monitorare lo stato di salute, nell'Unione Europea. La domanda principale oggetto di ricerca è se il nuovo diritto alla portabilità dei dati rafforzerà o comprometterà il controllo sui dati personali degli utenti di applicazioni di sanità mobile, incontrando sfide che sorgono dall'interoperabilità tra mHealth apps. La domanda principale implica due sotto-domande. La prima è cos'è il diritto alla portabilità dei dati. La seconda è se e fino a che punto il diritto alla portabilità dei dati sia possibile da un punto di vista tecnico (interoperabilità) tra mHealth apps, e se così fosse, quali siano i rischi alla privacy.

Ai fini di questa tesi, il diritto alla portabilità verrà discusso come uno strumento che dovrebbe consentire agli utenti un maggior controllo sui loro dati personali per proteggere i fondamentali diritti umani alla protezione dei dati e alla privacy.

Questa ricerca contribuisce alla letteratura nel dominio della sanità mobile e della protezione dei dati. In modo pragmatico, questa ricerca contribuirà in maniera significativa a chiarire lacune legali esistenti e future nell'implementazione del diritto alla portabilità dei dati nel settore della sanità mobile.

Abstract

The subject of this study, as the title indicates, is the right to data portability (RDP) in the context of the mHealth apps i.e. applications on mobile devices used to monitor health, in the European Union. The main research question is whether the new right to data portability will strengthen or undermine the control over personal data of mHealth apps users, encountering challenges arising from interoperability between mHealth apps. The central question entails two sub-questions. The first one is what RDP is. The second one is if and to what extent the right to data portability is possible from technical point of view (interoperability) between mHealth apps, and if so, what are the privacy risks.

For the purpose of this thesis, RDP will be discussed as an instrument that should give users greater control over their personal data to protect the fundamental human rights to data protection and privacy.

This research contributes to the literature in the domain of mHealth apps and data protection. Pragmatically, this research may make a valuable contribution in clarifying existing and future legal gaps in implementation of the right to data portability in the mHealth sector.

Table of Contents

Chapter 1: INTRODUCTION 15

1. The subject of the study 15

2. Context 15

3. What this thesis is about 18

4. Perspective 20

4.1. European Perspective 20

4.2. Legal Perspective 20

5. Methodology 21

6. Scientific value 22

7. Structure of the thesis 24

CHAPTER 2: mHEALTH 27

1. Introduction 27

2. Definition of mHealth 27

2.1. mHealth and eHealth 31

2.2. mHealth and Telemedicine 34

3. Taxonomy of mHealth apps 36

4. What is a mHealth app? 47

4.1. How do mHealth apps function? 51

4.2. Collecting, storing and processing data 53

a) Data provided by the user 56

b) Data provided by the smartphone 57

c) Usage of data 57

d) Sharing of data 58

4. Why do people care about data generated from mHealth apps? 58

5. Conclusion 59

CHAPTER 3: PERSONAL DATA, DATA PROTECTION, PRIVACY AND mHEALTH APPS 62

1. Introduction 62

2. The concept of personal data in the EU 64

2.1. Are data from lifestyle and wellbeing apps personal data? 76

(1) 'Any information' 76

(2) 'Relating to' 77

(3) '…identified or identifiable' 78

(4) 'Natural person' 79

2.2. Are data from lifestyle and wellbeing apps health data? 81

a) Inherently/clearly medical data 85

b) Raw sensor data 85

c) Health status or health risk conclusions 86

3. Exceptions for processing data from lifestyle and wellbeing apps 88

3.1 Exceptions for processing personal data 88

a) The technical way of processing 88

b) Activities out of the scope of Union Law and public security 89

c) Household exception 89

3.2 Exceptions for processing health data 92

4. The relationship between data protection and privacy 95

4.1. The right to data protection 95

4.2. The right to privacy 99

4.3. Privacy as a concept 103

4.3.1. Privacy as control 107

5. Conclusion 110

CHAPTER 4: RIGHT TO DATA PORTABILITY AND mHEALTH APPS 113

1. Introduction 113

2. Right to data portability 114

2.1 Right to data portability as control over data 116

2.2 Right to data portability as a competitive element 120

3. The right to data portability and mHealth apps 125

4. Limitations on exercising the right to data portability 132

4.1. Legal limitations 133

4.1.1 Personal data provided by the data subject 133

4.1.1.1 Data concerning the user 133

a) Non-identifiable or Anonymised data 133

b) Identifiable or Pseudonymous data 135

c) Identified data 140

d) Multi-data subjects 141

4.1.1.2 Provided data 142

a) Observed data 143

b) Inferred data 144

4.1.2 Legal grounds for processing data 145

a) Processing based on Consent 146

b) Processing based on Contract 157

4.1.3 Rights and freedom of other users 158

5.1 Technical limitations 161

5.1.1 Processing carried out by automated means 161

5.1.2 Structured, commonly used, machine-readable and interoperable 162

4 Conclusion 165

CHAPTER 5: INTEROPERABILITY OF mHEALTH APPS IN DATA-DRIVEN ECONOMY 168

1. Introduction 168

2. The Digital Economy 169

2.1 The Data-driven economy 169

2.2 Personal data and economic interests 172

2.3 Data ownership issue 174

3. Interoperability in data-driven economy 176

3.1 Levels of interoperability 179

3.3 Privacy issues 184

4. Interoperability of mHealth app operating systems 185

5. Conclusion 186

CHAPTER 6: CONCLUSION 189

1. Introduction 189

2. Problems and Answers 189

BIBLIOGRAPHY 194

Chapter 1: INTRODUCTION

1. The subject of the study

The subject of this study, as the title indicates, is the right to data portability (RDP) and mHealth apps, i.e. applications on mobile devices used to monitor health. The central research question examines, whether and to what extent, the new right to data portability as promulgated in the European Union, will strengthen the control[1] of mHealth apps users over their personal data, as well as the challenges arising from interoperability between mHealth apps. Control in the context of this thesis is seen as the possibility to receive and transfer personal data from one mHealth app to other.

The central question entails two sub-questions. The first one attempts to answer what are the legal requirements for exercising the right to data portability. The second one is whether and to what extent the right to data portability is possible from a technical point of view (i.e. interoperability) between mHealth apps, and if so, what are the risks. For the purpose of this thesis, RDP will be discussed as an instrument that should give users greater control[2] over their personal data to protect two fundamental human rights: the right to data protection and privacy. In this chapter, I will introduce the problem in the context of mHealth apps and some basic definitions that will be discussed in the following chapters. After this, the perspective of the study, the methodology used in the research and the structure of the thesis will be introduced.

2. Context

Nowadays people can wake up gently at a time carefully selected by a smart phone, which monitors their sleep patterns after drawing on weeks of stored data. Then they can

---

[1] General Data Protection Regulation (GDPR), Recital 7: '...Developments require a strong and more coherent data protection framework in the Union, backed by strong enforcement, given the importance of creating the trust that will allow the digital economy to develop across the internal market. Natural persons should have control of their own personal data. Legal and practical certainty for natural persons, economic operators and public authorities should be enhanced'

[2] *Id.* 1

go to the bathroom and step on to the smart scale, connected to the smart phone, which measures their weight and helps them to determine their workout and diet routines. After that, during their breakfast they can log in the calorie intake or scan the product calories to check if the calorie intake is within the advised limits. During the day, they use the smart phone to count how many steps they have made or how many kilometres they have run. Additionally, people with chronic diseases can use them to measure their heart rate or blood pressure.

All of these functions on the smartphones are possible due to the installation and use of different kinds of applications ('apps'). A number of these apps allow users to conduct self-diagnoses, to measure vital signs such as heart rate, blood glucose level, blood pressure; to measure the progress of physical activities such as running or walking; and to provide fitness and dietary recommendations. Apps that are used in the medical or health context are called mobile health applications or 'mHealth apps' and are generally classified into two groups: (1) medical apps, for the purpose of prevention, diagnosis and treatment of diseases; and (2) for lifestyle apps, i.e. fitness and wellbeing apps.

All these apps and the devices on which they are installed form the mobile health (mHealth) concept, defined as a sub-segment of eHealth (i.e. any health application available on a computerised device) that covers medical and public health practice supported by mobile devices. It also includes the use of mobile devices for health and well-being services and information purposes as well as mobile health applications.[3]

The first group of mHealth apps support patient-centred[4] care models and give patients opportunity for self-management of personal diseases and chronic conditions as well as the opportunity to live more independently. As a matter of fact, they empower patients and citizens to be more mobile and adopt healthy behaviour, to improve their well-being

[3] See e.g. mHealth Digital Agenda for Europe – https://ec.europa.eu/digital-agenda/en/mhealth last visited 03.06.2015

[4] From patient centred to people powered: autonomy on the rise, Dave de Bronkart *speaker, policy adviser, and co-chair, BMJ* 2015; 350:h148 doi: 10.1136/bmj.h148 (published 10 February 2015).

and to perform self-diagnosis[5] and self-monitoring. They are part of the highly regulated medical sector and will be excluded from the scope of this thesis.

The second group of mHealth apps (lifestyle and wellbeing apps) allow users to monitor their progress toward fitness, health and wellbeing goals for a prolonged period and ultimately to make more informed decisions about their health and lifestyles. In other words, these apps are considered as tools to enable users to eat healthier, move more and become aware of 'sustainable' lifestyles.[6] To clarify, the right to data portability, in this thesis will be discuss solely in the context of this second group of mHealth apps.

These benefits provided by the mHealth apps are result of collecting, storing and processing of data, mostly personal data. Therefore, it is important users to have control over their data and be able to transfer their data from one app to other. In fact, much of the data collected concern the user of the app or owner of the smartphone. These data allow a person to be directly or indirectly identified. Hence, they fall within the scope of the definition of personal (health) data. Consequently, the data protection law applies. The newly adopted General Data Protection Regulation (GDPR) has introduced a few new rights that aim to strengthen user control over their personal data and to respond to the new technological challenges. One of them is the right to data portability. This new right should give mHealth apps users the possibility of transferring their data from one app to other in a structured, machine-readable and interoperable format.

The right to data portability should respond to the concerns of mHealth apps users. Recent studies have shown that users are worried about being locked-in to dominant platforms[7] and losing control over their health data, even though they are aware of the benefits and are willing to share their health data. This lock-in to dominant platforms is

---

[5] For example self-diagnoses apps allow users to enter symptoms, which will be checked against a database to determine potential medical causes.

[6] The lifestylisation of healthcare? 'Consumer genomics' and mobile health as technologies for healthy lifestyle - Applied &Translational Genomics, Volume 4, March 2015, pages 44–49, Federica Lucivero, , Barbara Prainsack http://dx.doi.org/10.1016/j.atg.2015.02.001.

[7] Driving Innovation in Health Systems through an Apps-Based Information Economy - Mandel et al., published online 2015 June 11. doi: 10.1016/j.cels.2015.05.001. http://europepmc.org/articles/PMC4556429#R2

usually caused by because data usually reside in silos, and in most cases, according to Mandi et al.,[8] these data streams will initially remain confined to their respective platforms. For example, data generated by apps in the Apple store will be stored on their server (or cloud).

Therefore, this thesis will try to answer whether, and to what extent, the new right to data portability will strengthen the control[9] of the mHealth apps users over their personal (health) data, and how the challenges arising from interoperability between mHealth apps can be dealt with.

3. What this thesis is about

This thesis will be discussed only in the context of the second groups of apps (lifestyle and wellbeing), defined in the previous section. The reasoning behind this is that the first group are considered a task carried out in the public interest, and thus are excluded from the scope of the right to data portability.[10] More precisely, Article 20 Para. 3 states that:

> the right shall not apply to processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. Public interest refers to processing personal data in the field of employment law, social protection law including pensions and for health security, monitoring and alert purposes, the prevention or control of communicable diseases and other serious threats to health. It includes public health and the management of health-care services, especially in order to ensure the quality and cost-effectiveness of the procedures used for settling claims for

---

8 Driving Innovation in Health Systems through an Apps-Based Information Economy, Kenneth D. Mandl, Joshua C. Mandel,and Isaac S. Kohane, published online 2015 June 11. doi: 10.1016/j.cels.2015.05.001, http://europepmc.org/articles/PMC4556429

9 GDPR, Recital 7: '...Developments require a strong and more coherent data protection framework in the Union, backed by strong enforcement, given the importance of creating the trust that will allow the digital economy to develop across the internal market. Natural persons should have control of their own personal data. Legal and practical certainty for natural persons, economic operators and public authorities should be enhanced'

10 GDPR Article 20, Para. 3: the '…right shall not apply to processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

> benefits and services in the health insurance system, or for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.[11]

Additionally, the first group of apps are legally and organisationally quite different, and fall into the highly regulated medical domain.[12]

The right to data portability is the right of the data subject to receive personal data concerning him or her that he or she has provided to a controller and that has been processed by automated means based on consent or on a contract, in a structured, commonly used and machine-readable format. Thus, data subjects have the right to transmit such data to another controller without hindrance from the original controller to which the personal data have been provided. Yet, the problem is that the data subject's right to transmit or receive personal data concerning him or her should not create an obligation for the controllers to adopt or maintain processing systems which are technically compatible.[13] They are only encouraged to develop interoperable formats that enable data portability.[14] In fact, this, besides the legal interpretation of the right to data portability, might be a second major obstacle for exercising the right and strengthening users control over their data.

Encouraging development of interoperable formats would require quite complex systems to work together. This stems from the fact that interoperability consists of four layers: (1) technical interoperability or the ability of hardware and codes to connect; (2) data interoperability or the ability of interconnected systems to understand each other; (3) legal interoperability, requiring legal systems to work with one another towards establishing an international order that can accommodate the interconnected nature of the world in

---

[11] GDPR, Recital 52

[12] The lifestylisation of healthcare? 'Consumer genomics' and mobile health as technologies for healthy lifestyle - Applied &Translational Genomics, Volume 4, March 2015, pages 44–49, Federica Lucivero, , Barbara Prainsack http://dx.doi.org/10.1016/j.atg.2015.02.001

[13] GDPR, Recital 68

[14] *Id.* Recital 68

which we live;[15] and (4) human interoperability or ability of humans to understand and act on the data that exchange. The focus of this thesis will be only challenges arising from the first two, technical and data interoperability.

4. Perspective

4.1. European Perspective

Even though mHealth apps are a global phenomenon, this thesis approaches the issue from a European perspective. It will refer only to regulations of the European Union, more precisely to its data protection laws, relevant norms from the European Convention of Human Rights and the Charter of Fundamental Rights of the European Union, as well as related case law. It will also include the relevant opinions by the Article 29 Working Party (WP).[16] This study does not intend to give an overview of all data protection provisions that might be relevant for the mHealth apps.

The main focus is on the right to data portability, as one of the newly introduced rights in the GDPR, which will be applicable for all controllers and processors offering services and goods to the EU citizens.

4.2. Legal Perspective

The right to data portability can be approached from the economic, legal, and social perspectives. The economic approach might analyse the benefits and drawbacks encountered by the industry in implementing this right. This topic might also benefit if is approached from a social perspective, emphasising the interconnectedness of society by focusing on how each part influences and is influenced by other parts.

However, considering the legal background of the author and the limited period for writing the PhD thesis, it will be approached only from the legal perspective. Further, the

---

[15] Interoperability Case Study – The European Union as an Institutional Design for Legal Interoperability, Félix Tréguer 2012 The Berkman Center for Internet & Society at Harvard University

[16] The Article 29 Working Party has advisory status and acts independently. It is composed of: a representative of the supervisory authority (ies) designated by each EU country; a representative of the authority (ies) established for the EU institutions and bodies; and a representative of the European Commission.

topic from a legal perspective could be studied from the viewpoints of intellectual property law or competition law.[17] Yet, the main focus of this study will be on the data protection law.

5. Methodology

The study is based on an analytical and descriptive method. The analytical method is used to analyse the application of data protection regulation to the concepts of mHealth. The descriptive method is used to answer the questions of what is the right to data portability and what is the interoperability between mHealth apps.

However, in order to understand the problems created by mHealth apps and to discuss the relevant legal aspects, a general understanding of the technical aspects of mHealth apps and interoperability is essential. These technical aspects will be explained based on a review of the technical papers, literature and reports and based on my non-technical experience.

Data protection law is an important tool that regulates the informational privacy if personal data is processed. For the reason that we use RDP as an instrument, which should give users greater control over their personal data to protect their right to privacy, we define privacy as a control. Privacy as control is defined by many scholars but we use the one of Alan Westin. He defines privacy in terms of control by stating that 'Privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others.'

The review of the mHealth concept that follows is based on research of websites, books, online journals, papers, etc. in the field. I used references provided in relevant books and papers in order: 1) to capture the definitions of Telemedicine, eHealth and mHealth, 2) to analyse the changes in providing medical and health care under influence of the ICT, and 3) the taxonomy of mHealth apps.

---

[17] Graef, Inge and Verschakelen, Jeroen and Valcke, Peggy, Putting the Right to Data Portability into a Competition Law Perspective (2013). Law: The Journal of the Higher School of Economics, Annual Review, 2013, pp. 53-63. Available at SSRN: https://ssrn.com/abstract=2416537

6. Scientific value

This study contributes to the literature regarding the right to data portability and the challenges arising from the interoperability between mHealth apps.

The right to data portability, as a new right in the EU but also worldwide, in the context of mHealth apps is a topic relatively unexplored in the literature. Papers that are addressing this new provision in the GDPR exist, but they approach the issue from other aspects: 'Why the Right to Data Portability Likely Reduces Consumer Welfare: Antitrust and Privacy Critique',[18] 'Putting the right to data portability into a competition law perspective',[19] 'Mandating portability and interoperability in online social network's: regulatory and competition issues in the European Union',[20] 'Data Portability and Data Control: Lessons for an Emerging Concept in EU Law',[21] 'The right to Data portability in the context of the EU data protection reform',[22] 'The right to data porta-

[18] Swire, Peter and Lagos, Yianni, Why the Right to Data Portability Likely Reduces Consumer Welfare: Antitrust and Privacy Critique (May 31, 2013). 72 Maryland Law Review 335 (2013); Ohio State Public Law Working Paper 204. Available at SSRN: https://ssrn.com/abstract=2159157 or http://dx.doi.org/10.2139/ssrn.2159157

[19] Graef, Inge and Verschakelen, Jeroen and Valcke, Peggy, Putting the Right to Data Portability into a Competition Law Perspective (2013). Law: The Journal of the Higher School of Economics, Annual Review, 2013, pp. 53-63. Available at SSRN: https://ssrn.com/abstract=2416537

[20] Mandating portability and interoperability in online social networks: Regulatory and competition law issues in the European Union, Inge Graef, Telecommunications Policy Volume 39, Issue 6, July 2015, Pages 502–514

[21] Graef, Inge and Husovec, Martin and Purtova, Nadezhda, Data Portability and Data Control: Lessons for an Emerging Concept in EU Law (December 15, 2017). TILEC Discussion Paper No. 2017-041; Tilburg Law School Research Paper No. 2017/22. Available at SSRN: https://ssrn.com/abstract=3071875 or http://dx.doi.org/10.2139/ssrn.3071875

[22] The right to Data portability in the context of the EU data protection reform, Gabriela Zanfir, International Data Privacy Law, Advance Access, published May 11, 2012

bility in the GDPR: Towards user-centric interoperability of digital services',[23] 'Is the GDPR and Its Right to Data Portability a Major Enabler of Citizen Science?'[24]

On the other hand, a number of articles and studies have examined the potential and challenges of mHealth but from different aspects such as regulatory control and certification of apps,[25] safety and quality,[26] ethical and social aspects,[27] and the use of wellness apps in the employment context.[28] Data protection is addressed by Purtova, Kosta, and Koops,[29] but their discussion is based on the Data Protection Directive. Mantovani and Quinn[30] address consent in the context of mHealth, as a legal requirement for processing medical data based on the (then) proposed GDPR.

---

[23] The right to data portability in the GDPR: Towards user-centric interoperability of digital services, Paul De Hert,Vagelis Papakonstantinou, Gianclaudio Malgieri, Laurent Beslay, Ignacio Sanchez, Computer Law & Security Review, Volume 34, Issue 2, April 2018, Pages 193–203

[24] Is the GDPR and Its Right to Data Portability a Major Enabler of Citizen Science? Paul Quinn, Published June 2018 Global Jurist, DOI: 10.1515/gj-2018-0021, https://www.researchgate.net/publication/325635784_Is_the_GDPR_and_Its_Right_to_Data_Portability_a_Major_Enabler_of_Citizen_Science

[25] Mobile medical and health apps: state of the art, concerns, regulatory control and certification, Maged N. Kamel Boulos, Ann C. Brewer, Chante Karimkhani, David B. Buller, and Robert P. Dellavalle, Online J Public Health Inform. 2014; 5(3): 229 http://www.ncbi.nlm.nih.gov/pmc/articles/PMC3959919/

[26] 'Trust but verify' - five approaches to verify safety medical apps, September 2015-BMC Medicine 13(1):205, DOI: 10.1186/s12916-015-0451-z, LicenseCC BY 4.0, Paul Wick and Emil Chiazzi

[27] Lupton, Deborah. 2012. 'M-Health and Health Promotion: The Digital Cyborg and Surveillance Society.' Social Theory & Health, http://www.palgrave-journals.com/sth/journal/v10/n3/full/sth20126a.html

[28] eHealth and Privacy in U.S. Employer Wellness Programs, Anna Slomovic May 2015, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2613452

[29] Purtova, N., E. Kosta, and B.J. Koops. 2014. 'Laws and Reputation for Digital Health.' In Requirements Engineering for Digital Health and Care.

[30] Mantovani, Eugenio, and Paul Quinn. 2014. 'mHealth and Data Protection–the Letter and the Spirit of Consent Legal Requirements.' International Review of Law, Computers & Technology

7. Structure of the thesis

In this chapter, the research question was introduced: 'will the new right to data portability strengthen the control[31] of the mHealth apps users over their personal data, and how will challenges arising from interoperability between mHealth apps be addressed?' Furthermore, I introduced some basic definitions that will be discussed in the following chapters.

Chapter 2 will discuss what is mHealth, how it works and why people care about data generated by mHealth apps. We will define 'mHealth', for the reason that the lifestyle and wellbeing apps included as part of the definition will play a central role in our analysis and research for an appropriate legal framework. Second, we will provide a taxonomy of mHealth apps and explain why only lifestyle and wellbeing apps will be included in our analyses. Third, in order to study the legal issues regarding lifestyle and wellbeing apps, we need to understand their technical and functional aspects. Therefore, further in the chapter, we will explain what apps are and how they work. An important part of the discussion is why users of lifestyle and wellbeing apps care about and need to have control over their health data, in terms of the possibility to transfer the data from one app to another. The conclusions from Chapter 2 factually establish the basis on which our further discussion will be built on.

In Chapter 3, we discuss the application of the General Data Protection Regulation, Article 8 of the European Convention of Human Rights as well as Articles 7 and 8 of the Charter of Fundamental Rights of the European Union to the processing of data from lifestyle and wellbeing apps. Nonetheless, to start the discussion regarding the application of the above-mentioned instruments, we will first need to clarify when and whether the data process from lifestyle and wellbeing apps are personal data, and when the data can be categorised as sensitive (health) data. In line with this reasoning, we will further clarify the exceptions for processing health data and whether the household ex-

[31] GDPR, Recital 7: '...Developments require a strong and more coherent data protection framework in the Union, backed by strong enforcement, given the importance of creating the trust that will allow the digital economy to develop across the internal market. Natural persons should have control of their own personal data. Legal and practical certainty for natural persons, economic operators and public authorities should be enhanced'.

ception applies in the context of mHealth apps. An inevitable aspect of the data protection discussion is privacy. Basically, the issues concerning collecting, storing and processing a user's data from lifestyle and wellbeing apps tackle different aspects of the user life that are deemed private, hence, we will define privacy as 'control' for the purpose of this thesis. We intend to show why it is important for the users of lifestyle and wellbeing apps to have greater control[32] over their data. The focus will be on the aspects of information privacy in relation to data protection law. In fact, data protection law is an important tool that regulates the issue, if personal data is processed by the application. In addition, in this chapter, we will explain the relationship between data protection law and privacy.

Chapter 4 will discuss the new right to data portability (RDP) in the context of lifestyle and wellbeing apps. The RDP was for the first time introduced by the Commission in Article 20 of the GDPR as an instrument to restore the trust in online services and to give users more control over personal data held by service providers.[33] As written, it should strengthen user control over personal data by empowering data subjects 'to receive the personal data concerning him or her, which they have provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided'. In line with this reasoning and for the purpose of this thesis, control over personal data is seen as an instrument to allow users to transfer their data from one app to other which is better, cheaper or more privacy-friendly. This will prevent app users to be locked-in to the particular mHealth app. Therefore, the aim of this chapter is

---

[32] GDPR, Recital 7: '...Developments require a strong and more coherent data protection framework in the Union, backed by strong enforcement, given the importance of creating the trust that will allow the digital economy to develop across the internal market. Natural persons should have control of their own personal data. Legal and practical certainty for natural persons, economic operators and public authorities should be enhanced'.

[33] Commission staff working paper – Impact Assessment Accompanying the document 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) and Directive of the European Parliament and of the Council on the prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data. SEC (2012) 72 final, page 43

to examine to what extent RDP will actually provide app users with control over their data, confronted with the current legal interpretation of Article 20.

Chapter 5 is devoted to the question of what is interoperability and if interoperability is possible, from a technical point of view, between mHealth apps. The discussion revolves around the data-driven economy and tackles some of the obstacles for achieving interoperability, such as economic interest vs. right to data protection, as well as the data ownership issue.

Chapter 6 will summarise the findings from the previous chapters and provide answers to the research question. This research shows that, in fact, right to data portability will not strengthen the control of mHealth app users over their personal data. And the major problem is not interoperability but, the currently very limited legal interpretation of the right.

CHAPTER 2: mHEALTH

1. Introduction

This chapter will discuss mHealth, how it works and why people care about data generated by mHealth apps. First, we will attempt to provide a definition of mHealth, because the reason that lifestyle and wellbeing apps are part of the definition will play a central role in our analysis and research for an appropriate legal framework. Second, we will provide a taxonomy of mHealth apps and explain why only lifestyle and wellbeing apps will be included in our analysis. Third, in order to study the legal issues regarding lifestyle and wellbeing apps, we need to understand their technical and functional aspects. Therefore, further in the chapter, we will explain what apps are and how they work. Fourth, we will discuss why users of lifestyle and wellbeing apps care about their health data and need control over them, in terms of the possibility to transfer them from one app to other.

The chapter is organised as follows: 1) Definition of mHealth, 2) Taxonomy of mHealth apps, 3) What is an app and how does it function, and 4) Conclusion.

2. Definition of mHealth

The proliferation of connectivity embedded in smart devices allows people to install and use different kinds of applications (i.e. 'apps'). Some of these apps allow users to conduct self-diagnoses, to measure vital signs such as heart rate, blood glucose level, blood pressure and to measure physical activities such as running and walking, and can also make fitness and dietary recommendations.

In fact, apps used in the medical or health context are called mobile health applications 'mHealth apps' and are generally[34] classified in two groups: (1) apps for the purpose of prevention, diagnosis and treatment of diseases (or medical apps); and (2) lifestyle, fitness and well-being apps. The taxonomy of mHealth apps will be explained in detail in

[34] There are different classifications of mHealth apps in the literature and in the app stores. For the purpose of this paper we will adopt the abovementioned classification.

Section 1.3. All these apps and the devices on which they are installed form the mobile health (mHealth) concept.

The concept of mHealth is still new, dynamic and expanding. It is constantly changing and its boundaries being explored, meaning that there is still no consensus on a generally applicable definition of the term.[35] One author defines it as 'the use of mobile computing and communication technologies in health care and public health'.[36] Another defines it as the

> intersection between electronic Health (eHealth) and smartphone technology, that covers the acquisition, manipulation, classification, and transmission of health-related information from biomedical sensors usually attached to the user's body. Whereas, the sensory information is collected by portable devices with relevant applications running on them and information bits are transmitted through wireless and cloud networks.[37]

Another defines it as the 'component of eHealth that use mobile phones, patient monitoring devices, personal digital assistants (PDAs), and other wireless devices in medical and public health practices'.[38] However, none of the abovementioned definitions captures the notion of mHealth necessary for our further discussion. Some of them can be characterised as too broad, whereas some are too narrow.

Therefore, for this thesis, we have adopted as a working definition of the one from the Digital Agenda of EU, which defines mobile Health (mHealth) as:

---

[35] Chances and Risks of Mobile Health Apps (CHARISMHA) – Albrecht, Urs-Vito, Hannover Medical School, 2016. http://www.digibib.tu-bs.de/?docid=00060023 p.14.

[36] Mapping mHealth Research: A Decade of Evolution, Maddalena Fiordelli, Nicola Diviani,Peter J Schulz –Institute of Communication and Health, Faculty of Communication Sciences, University of Lugano, Switzerland, Pub. online 2013 May 21. doi: 10.2196/jmir.2430 http://www.ncbi.nlm.nih.gov/pmc/articles/PMC3668610/.

[37] Mobile Health – A technology Road Map, Sasan Adibi Editor – Faculty of Science Engineering & Built Environment School of Information Technology Burwood, Victoria Australia, Springer Series in Bio-/Neuroinformatics Volume 5-2015.

[38] WHO - Global Observatory of eHealth services, mHealth: New horizons for health through mobile technologies 2011, http://www.who.int/goe/publications/ehealth_series_vol3/en/.

> a sub-segment of eHealth that 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'[39]

We adopted this definition because it offers a suitably comprehensive framework to capture the notion of mHealth, for the following reasons:

First, it defines the ICT that falls within the scope on which this thesis will be built upon. It includes mobile devices or smart phones that can be characterised by powerful computing capability, various kinds of sensors, capacious memories, and open operating systems that encourage application development.[40] In fact, these devices are multifunctional with storage and processing power that exceeds by far the specifications of the Apollo Guidance Computer used on the first mission to the Moon.[41] Significantly, they comprise half of the mobile connections globally, and are predicted to reach 5.7 billion users by 2020.[42] Indeed, their storage and computational power has grown exponentially, as their price decreases. Additionally, they can capture increasing quantities of personal data, collected by a wide variety of sensors embedded in them. Another fact is that smartphones are now also serving as the 'gateways' to a variety of other devices such as fitness trackers, smart watches, connected home devices and virtual reality devices that

---

[39] mHealth Digital Agenda for Europe –mHealth https://ec.europa.eu/digital-agenda/en/mhealth last visited 03.06.2015

[40] How smartphones are changing the face of mobile and participatory healthcare: an overview, with example from eCAALYX. Boulos MN, Wheeler S, Tavares C, Jones R. 2011. Biomed Online. 10,24. .10.1186/1475-925X-10-24 http://europepmc.org/articles/PMC3959919;jsessionid=8weYDTr gw1gGUrWyma29.0#r2

[41] Health 4.0: How Virtualization and Big Data are Revolutionizing Healthcare, edited by Christoph Thuemmler, Chunxue Ba, Springer 2017 (DOI 10.1007/978-3-319-47617-9), page 14 https://books.google.de/books?id=DxHcDQAAQBAJ&pg=PA22&lpg=PA22&dq=mhealth+dortmund&source=bl&ots=yubcUCW3-M&sig=ghhWYAypSEuu5hLS7EwB7pPrYSI&hl=en&sa=X&ved=0ahUKEwjdi9j8ksXWAhUJnRQKHZEvAq0Q6AEIcjAJ#v=onepage&q=mhealth%20dortmund&f=false.

[42] Lower cost smartphones from local manufacturers such as Huawei, Oppo, OnePlus and Xiaomi in China, Micromax in India, and now AfriOne in Nigeria, are helping to address the affordability barrier. See more, GSMA Intelligence, Definitive data and analysis of the mobile industry, Global Mobile Trends 2017, page 14, https://www.gsmaintelligence.com/research/?file=3df1b7d57b1e63a0cbc3d585feb82dc2&download.

rely on smartphones for control, connectivity and processing power.[43] Data captured by the smart phones could be further processed by the provider's datacentres allowing extraordinary computing capacity. This combination of ubiquitous use and connectivity of mostly free mHealth mobile apps together with Big Data and data mining plays a central role in the building of a so-called quantified self.[44]

In spite of their technical capacity for ordinary people, the crucial feature is that they allow communication to be personalised and enable users to customise their phones to suit their personal preferences. Most importantly, they allow the downloading of apps. Apps or application programs refer to pieces of software coded for a specific purpose and usually optimised to run on a mobile device. They typically are available through application distribution platforms operated by the owner of the mobile operating system. In the context of mHealth, this would mean smart phones on which apps are installed that are intended to diagnose, monitor or prevent disease, for social and elderly care, clinical study, as well as lifestyle and wellness. They have direct access to many different sensors (microphones, cameras, GPS, accelerometers, ambient light sensors, etc). Therefore, they can track movements, take measurements and record information such as sleep patterns, mood, energy, steps, exercise, blood pressure and other indicators of health, data that are almost always connected to the owner of the device.[45]

Second, in line with the chosen mHealth definition, the EU Green paper on mobile health[46] provides a further explanation that lifestyle and wellbeing apps also fall within the scope of the definition. This study will discuss only these types of apps, and in Section 1.3, we will elaborate on the reasons for our choice.

---

[43] GSMA Intelligence, Definitive data and analysis of the mobile industry, Global Mobile Trends 2017, page 17, https://www.gsmaintelligence.com/research/?file=3df1b7d57b1e63a0cbc3d585feb82dc2&download.

[44] European Data Protection Supervisor, Opinion 1/2015 Mobile Health Reconciling technological innovation with data protection, 21 May 2015.

[45] ICO Privacy in mobile apps. Guidelines for app developers, December 2013, https://ico.org.uk/media/for-organisations/documents/1596/privacy-in-mobile-apps-dp-guidance.pdf.

[46] The Green Paper is available at: http://ec.europa.eu/digital-agenda/en/news/green-paper-mobile-health-mhealth, p.4

Third, this definition is in line with the European perspective of this study.

Fourth, it provides ground to explain the complex position of mHealth in the EU, in terms of its relationship with eHealth and telemedicine. For that reason, in the next section, we will discuss mHealth as sub-segment of eHealth, and the relationship between mHealth and telemedicine. Clarifying these issues is necessary to delimit what falls within the scope of this study.

2.1. mHealth and eHealth

Bearing in mind the European perspective of this study, as well as the adopted working definition, we consider mHealth as sub-segment of eHealth. In the EU, eHealth emerged in the 1990s as a result of promises that internet, computers and telecommunication have opened to the medical and healthcare sector.[47] It has been defined as:

> cover[ing] the interaction between patients and health-services providers, institution-to-institution transmissions of data, or peer-to-peer communication between patients and/or health professionals; it can also include health informational networks, electronic health records, telemedicine services, and personal wearable and portable communicable systems for monitoring and supporting patients.[48]

Analysing the definition one can conclude that actually it reflects all the possibilities enabled by e-commerce on the internet, solely in the context of the medical and health sector such as (1) allowing online interaction with systems, (2) possibilities for institution-to-institution transmissions of data, and (3) new possibilities for peer-to-peer communication.[49] In addition, it also includes personal wearable and portable communicable systems. Thus, even though mHealth is not explicitly mentioned in the definition, it is con-

---

[47] What is e-health? Gunther Eysenbach, J Med Internet Res. 2001 Apr-Jun; 3(2): e20. http://www.ncbi.nlm.nih.gov/pmc/articles/PMC1761894/

[48] eHealth: Legal, Ethical and Governance Challenges, Carlisle George – Diane Whitehouse-Penny Duquenoy

[49] What is e-health? Gunther Eysenbach, J Med Internet Res. 2001 Apr–Jun; 3(2): e20. http://www.ncbi.nlm.nih.gov/pmc/articles/PMC1761894/

sidered as sub-segment of eHealth, together with health informational networks, electronic health records, and telemedicine.

As a matter of fact, use of the ICT in the medical and health sector has stemmed from the promotion of an open and competitive digital economy in the EU based on ICT, which has aimed to improve quality, efficiency and effectiveness of this sector.[50] Consequently, we have seen a proliferation of health and medical websites offering details about illnesses, diseases, health promotion and healthcare, as well as online discussion groups, blogs and social media, allowing patients, citizens and doctors to share images, videos and information about their health and medical experiences.[51] Lastly, we see mHealth apps (robots, AI).

Another consequence of this development is that it has opened the medical and healthcare sector not only for registered medical doctors or subjects with a medical background and well-known health companies but also for start-up software companies (national and international). For example, manufacturers of mHealth apps come from varied backgrounds. The spectrum of developers and providers ranges from private individuals through privately organised companies and institutions to (health) insurance companies.[52] Subsequently, mHealth apps echo the complexities of the balance between medicine as a business, as a service to individuals, and as a science. Since it combines business, treatment, and research, it is often difficult to draw clear lines delineating where information collected for one of these purposes slips into being used for another, as well as the difficulty of determining the line between what should be private and what can be disclosed (and with whom and for what purposes such sharing can take place).[53]

---

[50] Book eHealth: Legal, Ethical and Governance Challenges, Carlisle George – Diane Whitehouse-Penny Duquenoy

[51] Apps as Artifacts: Towards a Critical Perspective on Mobile Health and Medical Apps - Deborah Lupton , Societies 2014, 4(4), 606–622; doi:10.3390/soc4040606, http://www.mdpi.com/2075-4698/4/4/606/htm

[52] Chances and Risks of Mobile Health Apps (CHARISMHA) – Albrecht, Urs-Vito, Hannover Medical School, 2016. http://www.digibib.tu-bs.de/?docid=00060023, p.15

[53] Engaging Privacy and Information Technology in a Digital Age, James Waldo, Herbert S. Lin, and Lynette I. Millett, editors, 2007.

However, the medical and health sector benefits from mHealth apps for the reason that they: (1) allow easier online access to medical care and information, for example by enabling doctors to remotely monitor patients, (2) are used to decrease the budget expenditure due to the ageing population,[54] (3) are used to assist in a steady decline in the number of health personnel,[55] (4) can answer to the growing demands and expectations from citizens for higher quality services and social care, (5) decrease hospitalisation costs, (6) deliver more personalised 'citizen-centric' healthcare, which is more targeted, effective and efficient,[56] and (7) for disease prevention.

Patient and users of mHealth apps, on the other hand, benefit, because they decentralise, demystify, and democratise the medical and health sector.[57] They support patient-centred[58] care models and give a patient opportunity for self-management of personal diseases and chronic conditions, as well as the opportunity to live more independently. As a matter of fact, they empower patients and citizens to be more portable and adopt healthy behaviour, to improve their well-being and to perform self-diagnosis[59] and self-monitoring.[60]However, despite being aware of the benefit of mHealth apps and willing-

---

[54] Ageing Report 2012: Economic and budgetary projections for the 27 EU Member States (2010–2060), Chapter 3, https://ec.europa.eu/digital-agenda/en/news/ehealth-action-plan-2012-2020-innovative-healthcare-21st-century.

[55] Green Paper on the European Workforce for Health COM (2008) 725 final of 10.12.2008 http://ec.europa.eu/health/ph_systems/docs/workforce_gp_en.pdf.

[56] See Vision on eHealth European Interoperability Framework – A study prepared for the European Commission DG Connect, 2013.

[57] Cortez, Nathan, The Mobile Health Revolution? (June 24, 2013). UC Davis Law Review, Vol. 47, 2104; SMU Dedman School of Law Legal Studies Research Paper No. 128. Available at SSRN: http://ssrn.com/abstract=2284448 or http://dx.doi.org/10.2139/ssrn.2284448, p.25.

[58] From patient centred to people powered: autonomy on the rise, Dave de Bronkart *speaker, policy adviser, and co-chair, BMJ* 2015;350:h148 doi: 10.1136/bmj.h148 (Published 10 February 2015).

[59] For example, self-diagnosis apps allow users to enter symptoms, which are checked against a database to determine potential medical causes.

[60] The digitally engaged patient: Self-monitoring and self-care in the digital health era, Debora Lupton, Social Theory & Health (2013) 11, 256–270.

ness to share their health data users are worried about being locked-in to dominant platforms[61] or losing control over their health data.

For example, an athlete, called 'Sportiest', is using the running app available on one of the dominant app stores, to prepare for the Olympic Games. Data collected from the running apps is necessary to measure and analyse his performances in order to further improve himself and win a medal. One month before the games the company owning the app announces that due to financial trouble the app will be switched off the following week. Sportiest has asked the app to provide him with all the data generated by the app in order to transfer them to other apps and continue with measuring, analysing and comparing his running performances. Even though, based on the new right to data portability, Sportiest has the right to receive or transmit his personal health data, which he has provided to a controller in a structured, commonly used, machine-readable and interoperable format[62] this, unfortunately, will be not possible, because the two operating systems are not interoperable. The issues around data portability and interoperability will be analysed and more details clarified in Chapters 4 and 5.

In this Chapter, we will further clarify the position of mHealth. Telemedicine and mHealth, as sub-segments of eHealth, are closely related. The reasoning behind this is that some of the mHealth apps are used to collect, store, analyse and transmit real-time health data necessary for diagnosis, prevention and treatment when patient and health professionals are in different locations. In fact, this is also the main characteristic of telemedicine. Consequently, in the next section, we will discuss their relationship, as well as what will be included and excluded further in this study.

2.2. mHealth and Telemedicine

The idea to transmit medical and health information for prevention, diagnosis and treatment, when doctor and patient are in different locations is not new. For example, in ancient times 'people used light reflections and smoke signals to relay messages to distant

---

[61] Driving Innovation in Health Systems through an Apps-Based Information Economy - Mandel et al., Published online 2015 June 11. doi: 10.1016/j.cels.2015.05.001. http://europepmc.org/articles/PMC4556429#R2

[62] GDPR, Recital 68, April 2016.

compatriots or neighbouring communities about plagues and health events.'[63] In the Middle Ages, wealthy families sent urine samples to their doctor for a diagnosis. A few centuries later, the advent telecommunication technologies such as radio, phone, fax and telegraph have been used for the same purpose. In cases when passengers on a plane or boat were facing some health issue, radio has been used to communicate with a doctor to provide diagnoses and instruction for treatment.

In the twentieth century, advancement of computers and telecommunication technology have resulted in accessibility and extensive use of personal computers and the internet in the medical and health sector. This has led to the blooming of telemedicine in the EU. The reason for this flourishing is that has allowed new ways of collecting, storing and analysing medical and health data, necessary for prevention, diagnoses and treatment when patient and doctor are in different locations. Especially for patients living in remote or rural areas, it allowed them to have access to a specialist not available locally as well as reduced travel time and costs. Telemedicine in the EU is defined as:

> provision of healthcare services, through use of ICT, in situations where the health professional and the patient (or two health professionals) are not in the same location. It involves the secure transmission of medical data and information, through text, sound, images or other forms needed for the prevention, diagnosis, treatment and follow-up of patients.[64]

mHealth is closely related with telemedicine, even is considered as 'extension'[65] of telemedicine. Actually, one of the key elements of mHealth is its potential to allow the establishment of treatment relationships between a patient and a physician that are not

---

[63] History of Telemedicine Evolution, Context, and Transformation, Rashid L. Bashshur, Ann Arbor, Michigan, Gary W. Shannon 2009, Print ISBN: 1-934854-11-5

[64] Commission staff working document on the applicability of the existing EU legal framework to telemedicine services Communication from the commission to the European parliament, the council, the European economic and social committee and the committee of the eHealth Action Plan 2012-2020 – innovative healthcare for the 21st century, Brussels, 6.12.2012

[65] Widespread Deployment of Telemedicine Services in Europe Report of the eHealth Stakeholder Group on implementing the Digital Agenda for Europe Key Action 13/2 'Telemedicine' Version 1.0 final (12 March 2014)

dependent on the geographical location. This treatment relationship, as explained above, falls under the notion of telemedicine and will be not analysed in this study, which focusses on another aspect of mHealth, the situation when health data is collected through the apps so that the user can improve his wellbeing and stay fit. To further delimit mHealth from telemedicine, we will provide a taxonomy of apps. The discussion in the next section will clarify which mHealth apps are considered as part of telemedicine and thus why they are not within the scope of this thesis.

3. Taxonomy of mHealth apps

The market for mHealth apps has been growing steadily over the years. In 2017 there were 325,000 mHealth apps or more than 78,000 new health apps released over the previous year. Remarkably this growth has mostly results from an increase of Android apps compared to other app stores and platforms. Android has seen a growth rate of 50 % from 2016 to 2017 in comparison to 20% growth rate of iOS health apps.[66]

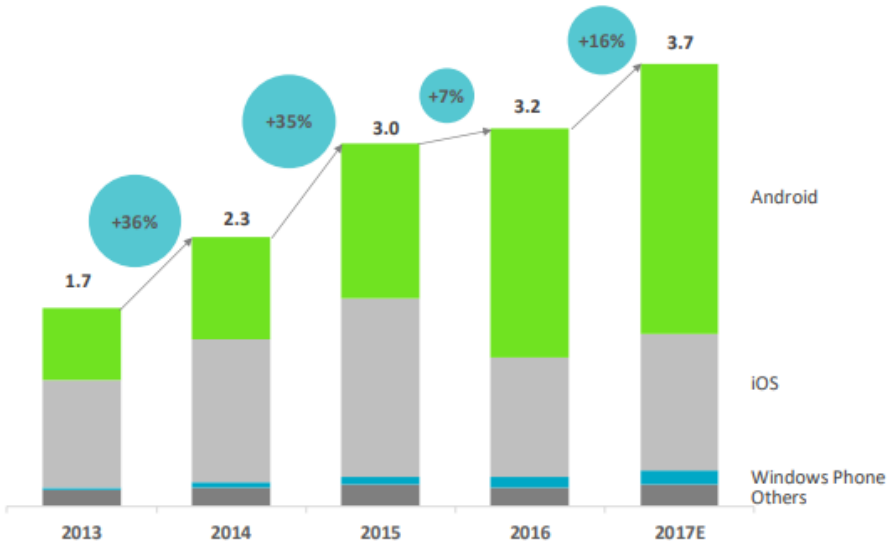

Figure 1. Growth in mHealth apps by platform. Source: Research2Guidance-mHealth App Developer Economics study 2017

[66] Statistics in this paragraph from mHealth App Economics 2017, Current Status and Future Trends in Mobile Health-How digital intruders are taking over the healthcare market, Research 2Guidance, Published November 2017, page 10

Figure 1 shows that Android is the number one platform for mHealth apps and has the greatest number of mHealth apps compared to iOS and other app stores and platforms.

Varieties of medical, lifestyle and wellness-related apps are available in the app stores. These apps are either interactive, requiring that the user participates in a program or are informational, for instance, mobile magazine subscriptions for medical, health and lifestyle publications. Another feature of these apps is the social networking element, whereby users may share their medical, health and well-being information either within the app's own network or with users of Facebook or other social networks.[67]

In the available literature, some authors conceptualise apps, based on their functionalities, as patient-consumer apps or provider apps.[68] Others discussing them as either (a) patient care and monitoring apps, (b) health apps for the layperson, (c) communication, education and research apps, and (d) physician or student reference apps.[69] Nonetheless, any taxonomy of mHealth apps will be suggestive rather than definitive, since these apps are subject to frequent updates and changes.[70]

Yet, based on the existing taxonomies for the purpose of this thesis the types of apps will be classified in two main groups (1) apps for the purpose of prevention, diagnosis and treatment of diseases (or medical apps); and (2) for lifestyle, fitness and well-being apps. This taxonomy allows us to elucidate the existing apps in two main groups, and moreover to emphasise the crucial difference between them, and why we build our analysis only on the second type of app. Nonetheless, as noted above, we must admit that delimiting clear line between these two groups of apps, in reality, is difficult.

---

[67] PRIVACY AND MHEALTH: HOW MOBILE HEALTH 'APPS' FIT INTO A PRIVACY FRAMEWORK NOT LIMITED TO HIPAA, 2014, Anne Marie Helm, Daniel Georgatos, University of California-Hastings College of the Law

[68] *Id.*

[69] A Taxonomy of mHealth Apps – Security and Privacy Concerns, 2015, 48th Hawaii International Conference on System Sciences. Miloslava Plachkinova, Steven Andrés and Samir Chatterjee, Claremont Graduate University.

[70] Cortez, Nathan, The Mobile Health Revolution? (June 24, 2013). UC Davis Law Review, Vol. 47, 2104; SMU Dedman School of Law Legal Studies Research Paper No. 128. Available at SSRN: http://ssrn.com/abstract=2284448 or http://dx.doi.org/10.2139/ssrn.2284448, p.18.

The first group entails medical apps or ones targeted to healthcare workers (physicians, nurses and assistants). These apps are generally more sophisticated, with medical terminology and functions and are not easily navigable by non-health professionals. Into this group fall:

- Drug-referencing apps.[71] These allow health care providers to reach databases featuring timely, in-depth information on drugs, natural products, interaction, medical calculations and more, whether in the hospital or on the go.
- Clinical decision-support apps are able to analyse data and to help health care providers to make clinical decisions. These apps run a patient's symptoms, personal characteristics and risk factors against a diagnostic database and other point-of-care applications like medication dosing calculators that calculate dosages based on entered weights and ages. These apps are designed to facilitate the efficient treatment of patients by allowing healthcare providers to quickly check a diagnosis.[72]
- Medical education and training apps are devoted to health and medical news as well as information from medical textbooks and journals.[73] For example, new trainee doctors use this app as a portable electronic library, providing them with a wealth of information when senior or attending physicians are not available and thus enhance patient care.[74]
- Symptom checker apps[75] provide information to patient and citizens about diseases, symptoms and give advice on how to take drugs or what to do in case of

---

[71] See more at http://www.epocrates.com/products/features

[72] See more on http://www.medscape.com/public/medpulseapp?src=mbl_stm_mbl3?src=mbl_stm_mbl2

[73] See page 61 of the Manual on borderline and classification in the community regulatory framework for medical devices Version 1.16 (07-2014)
http://ec.europa.eu/health/medicaldevices/files/wg_minutes_member_lists/borderline_manual_ol_en.pdf.

[74] Mobile technology supporting trainee doctors' workplace learning and patient care: an evaluation.Hardyman W, Bullock A, Brown A, Carter-Ingram S, Stacey M. 2013. BMC Med Educ. 13, 6 10.1186/1472-6920-13-6, http://europepmc.org/articles/PMC3552772/.

[75] See more on Android Symptom checker
https://play.google.com/store/apps/details?id=com.senstore.alice.harvard&hl=en

experiencing pain. They allow users to enter symptoms, which will be checked against a database to determine potential medical causes. Some apps allow users to submit smartphone photos of moles for analysis by an algorithm, and if necessary they refer users to local physicians.

The four abovementioned apps do not collect personal (health) data. Their purpose is purely informative or educational. Other types of medical apps do collect these data:

- Electronic Health Records apps allow health providers to access and update patient electronic health records, prescribe medication, and view test results.
- Patient Health Record apps allow users to access their health records. These apps have a long but not very successful history. Google Health and Microsoft's HealthVault are two of them, however, they have never managed to obtain widespread adoption or move the needle on interoperability. In January 2018, Apple updated the Health Records section within their Health app (see Figure 2). Thus, it succeeds where others have failed. It manages to allow users to easily see their available medical data from multiple providers whenever they choose. Thus, users will have medical information from various institutions organised into one view covering allergies, conditions, immunisations, lab results, medications, procedures and vitals, and will receive notifications when their data is updated.[76] This way they have control over their own health records. Still, availability of this app is limited only for users of the iPhone (iOS 11.3) and solely if the user is a patient at a participating hospital. Interestingly, the health data exchange is facilitated through Fast Healthcare Interoperability Resources, a standard for transferring electronic medical data. It enables greater interoperability of patient data from provider to provider. In terms of privacy and security, as announced the user's data will be encrypted and stored on the iPhone itself, not in the cloud, so Apple will not have access to this information.

---

[76] Apple announces effortless solution bringing health records to iPhone, 24th January 2018, https://www.apple.com/newsroom/2018/01/apple-announces-effortless-solution-bringing-health-records-to-iPhone/ last visited 29.01.2018

Figure 2. Apple's Health App. Source: https://www.apple.com/newsroom/2018/01/apple-announces-effortless-solution-bringing-health-records-to-iPhone/

- Clinical study apps allow researchers to design and administer app-based studies in order to have an easier time recruiting users to collect and share their data as part of large-scale clinical studies.[77] In March 2015, Apple launched such an app on their platform called Research Kit. This platform has been used by researchers at Duke University to develop an app for autistic children using the iPhone's camera to analyse the child's expressions, for example.[78] It provides parents with the option of sending the recorded video of their child along with the encoded data to researchers, or they can just send the analysed data without the full video recording.

Other medical apps are tailored for specific diseases. For example:

---

[77] Smartphones set to boost large-scale health studies, International weekly journal of science 'Nature' http://www.nature.com/news/smartphones-set-to-boost-large-scale-health-studies-1.17083, last visited 20.03.2015.

[78] Apple: ResearchKit is a pipeline for future diagnostic medical apps, October 15, 2015 http://mobihealthnews.com/47611/apple-researchkit-is-a-pipeline-for-future-diagnostic-medical-apps/.

- Medical Device apps are designed for the medical purposes and are used in healthcare[79] by the healthcare professionals.[80] Examples of medical device apps are those that gather data from the human body, such as body temperature, weight, pulse, oxygen and ECG for medical purposes such as diagnoses, treatment and prevention. The requirement in the EU legal framework for a mobile app to be considered as the medical device[81] is: to fall within the scope of Article 1, 2(a) of the current Directive 93/42/EEC as software intended[82] by its manufacturer to be used specifically for:
    - 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

---

[79] Directive 2011/24/EU on the application of patients' rights in cross-border healthcare. See Article 3 (a): 'healthcare' means health services provided by health professionals to patients to assess, maintain or restore their state of health, including the prescription, dispensation and provision of medicinal products and medical devices.

[80] Directive 2011/24/EU on the application of patients' rights in cross-border healthcare. See Article 3 (f): 'health professional' means a doctor of medicine, a nurse responsible for general care, a dental practitioner, a midwife or a pharmacist within the meaning of Directive 2005/36/EC, or another professional exercising activities in the healthcare sector which are restricted to a regulated profession as defined in Article 3(1)(a) of Directive 2005/36/EC, or a person considered to be a health professional according to the legislation of the Member State of treatment.

[81] 'medical device' means any instrument, apparatus, appliance, software, material or other article, whether used alone or in combination, 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;

[82] Directive 93/42/EEC concerning medical devices Article 1 (2) 'intended purpose' means the use for which the device is intended according to the data supplied by the manufacturer on the labelling, in the instructions and/or in promotional materials;

For example, acute stroke care is made portable and accessible to non-urban centres via real-time video on smartphones. The 'i-Stroke'[83] system was developed to transfer clinical data, computed tomography (CT), magnetic resonance imaging (MRI), angiographic and intraoperative images, as well as expert opinion, all in real time.[84]

- Patient-citizen self-management apps are designed for patient self-management of personal diseases and chronic conditions. These apps track, display and share user´s health parameters, medication intake, feelings, behaviour or provide information on a specific health condition, e.g. diabetes, obesity, or heart failure. Another feature of these apps is that it allows users to send information about their condition directly to their healthcare provider; the patient logs fasting blood sugars, daily eating behaviours, medication compliance, physical activity and emotions into a mobile online diary. A remote therapist with access to these diaries would then formulate personalised feedback to the patient.[85] One example is

---

[83] It is free software and it is already available at the Apple store. The system comprises a transmitting server and receiving Smartphones and allows the following functions: (1) stroke call function: informing participating medical staff involved in all aspects of patient management of an expected admission; (2) time-bar function for monitoring patients' management course; (3) image viewing function ; medical images virtually identical to those displayed in the hospital); (4) static and 3-dimensional video images available to off-site users , tick-box functions for input/displaying data (consciousness level and neurological findings), and automatic calculation of intravenous medication dose (including tissue-type plasminogen activator) from body weight, diagnosis confirmation from clinical history, and findings using checklists; National Institutes of Health Stroke Scale/Glasgow Coma Scale stroke scales, and others) incorporating diagnostic and treatment functions ; (5) real-time video streaming of microsurgical and diagnostic images from diagnostic and operating rooms (Figure 3C); (6) Tweeting to fellow specialists (exchanging opinions on the spot); and (7) inter-hospital exchange of images and other information, allowing consultations for patients at other hospitals. To protect personal information, all patient information has been blindly coded by the VPN system. Therefore, only patient age and gender are provided as identification. After 24 hours of stroke call initiation, all i-Stroke data for the patient are erased automatically.

[84] A new support system using a mobile device (smartphone) for diagnostic image display and treatment of stroke. Takao H, Murayama Y, Ishibashi T, Karagiozov KL, Abe T. 2012. Stroke. 43(1), 236-39 10.1161/STRO

[85] The development and feasibility of a web-based intervention with diaries and situational feedback via smartphone to support self-management in patients with diabetes type 2. Nes AA, van Dulmen S, Eide E, Finset A, Kristjansdottir OB, et al. 2012. Diabetes Res Clin Pract. 97(3), 385-93 10.1016/j.diabres.2012.04.019 http://europepmc.org/abstract/MED/22578890

> the app developed for patients with dementia, iWander,[86] which runs on several Android-based devices with GPS and communication capabilities. It allows caregivers to assist patients with daily living if they begin to wander by providing audible prompts offering to direct the patient home, sending notifications and GPS coordinates to caretakers.

The functioning of these apps is based on collection, storing and analysing data necessary for diagnosing, prevention and treatment, for social and elderly care and for research. Such data might be provided by the users, collected via sensors or through different monitoring devices that transfer the data to the apps. However, this group of apps will be not included in our further analysis.

The reason is that they are legally and organisationally quite different. As Lucivero has pointed out, the first group falls in the highly regulated medical domain and the second group, discussed below, in the less regulated consumer market.[87] Second, the consent requirement is stricter,[88] arising from other EU fundamental rights frameworks.[89] More specifically, consent in this context is not seen only as a possibility to process personal data but as part of the confidential patient-doctor relationship. It presents an instrument

---

[86] iWander: An Android application for dementia patients. Sposaro F, Danielson J, Tyson G, Conf Proc IEEE Eng Med Biol Soc 2010, 2010:3875-3878 http://europepmc.org/abstract/MED/21097072

[87] The lifestylisation of healthcare? 'Consumer genomics' and mobile health as technologies for healthy lifestyle - Applied &Translational Genomics, Volume 4, March 2015, pages 44-49, Federica Lucivero, , Barbara Prainsack http://dx.doi.org/10.1016/j.atg.2015.02.001.

[88] See more, Eugenio Mantovani, Paul Quinn, mHealth and data protection – the letter and the spirit of consent legal requirements, Article in International Review of Law Computers & Technology March 2013, DOI: 10.1080/13600869.2013.801581
https://www.researchgate.net/publication/255825921_mHealth_and_data_protection_-_the_letter_and_the_spirit_of_consent_legal_requirements.

[89] Helsinki Declaration 1964, article 8 'Respect for the Individual', 'Right to Self-Determination' and the 'Right to Make Informed Decisions Regarding Participation in Research' detailed in Articles 20, 21 and 22. Oviedo Convention on Human Rights and Biomedicine No. 164, Oviedo, 4.4.1997. Article 5 states that'[a]n intervention in the health field may only be carried out after the person concerned has given free and informed'. The Universal Declaration on Bioethics and Human Rights of 2005, in Article 6 states that 'any preventive, diagnostic and therapeutic medical intervention is only to be carried out with the prior, free and informed consent of the person concerned, based on adequate information.'

for balancing the responsibility of the doctor and the person concerned. The latter has the right to be consulted and to consent before any medical intervention takes place. In both situations, as some argue, the notion of consent lies at the heart of individual autonomy.[90] Third, this group of apps does not provide a solid basis to discuss and clarify the second research question, 'whether data from mHealth apps is health data'.

The second group, which is of particular interest to this study, are apps for lifestyle and wellbeing management. Into this group fall:

- Personal Medical Record apps, which allow patients to access their personal electronic health records and update those records with information about their health history[91] and if necessary to share them with health professionals. In this sector Google and the maker of smartwatches and wearables, Fitbit, in April 2018 announced a collaboration.[92] This follows after Fitbit's recent acquisition of Twine Health.[93] It is also not clear if this service will be available to all users, or limited only to the US citizens, as well only for the users of Apple devices.

  As part of the collaboration with Google, Fitbit 'intends to use Google's new Cloud Healthcare API to help the company integrate further into the healthcare system, such as by connecting user health and fitness data with electronic medi-

---

[90] For more, see Eugenio Mantovani, Paul Quinn, mHealth and data protection – the letter and the spirit of consent legal requirements, Article in International Review of Law Computers & Technology March 2013, DOI: 10.1080/13600869.2013.801581, page 12
https://www.researchgate.net/publication/255825921_mHealth_and_data_protection_-_the_letter_and_the_spirit_of_consent_legal_requirements.

[91] See more information on https://account.healthvault.co.uk/it/it-IT/Directory

[92] Fitbit and Google Announce Collaboration to Accelerate Innovation in Digital Health and Wearables - Fitbit to leverage Google Cloud to increase operational efficiency, agility and speed to market, Press release, 04/30/2018 https://investor.fitbit.com/press/press-releases/press-release-details/2018/Fitbit-and-Google-Announce-Collaboration-to-Accelerate-Innovation-in-Digital-Health-and-Wearables/default.aspx

[93] Fitbit, Inc. to Acquire Twine Health - Acquisition brings Fitbit's leading brand and community of millions together with Twine Health's clinically proven health coaching platform to drive better health outcomes and ultimately, lower healthcare costs, Press release 13.02. 2018
https://investor.fitbit.com/press/press-releases/press-release-details/2018/Fitbit-Inc-to-Acquire-Twine-Health/default.aspx

cal records (EMR)'. Combining Fitbit data with EMRs by using Google's AI and machine learning capabilities as well as new predictive analytic algorithms may provide patients and clinicians with a more comprehensive view of the patient profile, leading to more personalised care, especially to better manage chronic conditions like diabetes and hypertension.[94] This collaboration aims to organise health data in a way that is accessible and interoperable.[95]

Actually, interoperability is a major problem when it comes to managing health data. Therefore, to address this interoperability challenge, Google has launched a new Cloud Healthcare Application Programming Interface (API) that allows clients to absorb and manage multiple types of medical data on one platform.

This news from the two major players, Apple and Google lead us to conclude that despite their intention for providing better healthcare for the users, in fact, it is a battle for capturing a bigger piece of health data in the digital economy.

- Lifestyle and wellbeing apps involve but are not limited to activities: like counting calories, monitoring daily exercise, and providing information about nutritional supplements. These apps reflect a targeted and personalised approach to help consumers monitor their progress toward fitness, health and wellbeing goals and ultimately to make more informed decisions about their health and lifestyles. For example, nutrition and diet apps use the built-in camera, standard in today's smartphones, which allows users to take a photo (or scan the barcode) or record food intakes, which is instantly converted to nutrient intake and compared with calculated nutrition goals. Nutrition goals are then calculated based on a diet app

[94] Fitbit and Google Announce Collaboration to Accelerate Innovation in Digital Health and Wearables - Fitbit to leverage Google Cloud to increase operational efficiency, agility and speed to market, Press release, 04/30/2018 https://investor.fitbit.com/press/press-releases/press-release-details/2018/Fitbit-and-Google-Announce-Collaboration-to-Accelerate-Innovation-in-Digital-Health-and-Wearables/default.aspx

[95] Google Cloud - New collaboration with Fitbit to drive positive health outcomes, Google blog, Published 30.04.2018 https://blog.google/topics/google-cloud/new-collaboration-fitbit-drive-positive-health-outcomes/

user's sex, weight, weight goals, and activity level. Food entries and weight progress can be shared with a dietician in real time.[96]

- Fitness apps typically use GPS tracking allowing users to record physical activities, such as walking, jogging, and cycling. They also accurately record duration, frequency, and intensity of activities through an integrated gyroscope and/or accelerometer. In addition, it calculates calorie expenditure, summarises performance trends overtime periods, and allows users to share their performance with friends on social networks.[97] The latest trend in many fitness apps is gamification or turning exercise into something more interesting. Some of these apps transforms the real world into a 'game map' or playground due to the GPS-enabled smartphones and the power of sharing through online social networks. For example, Zombies Run[98] combines audiobook storytelling and running, putting users into a fictional world where running really matters. It requires users to sprint away from danger at top speed while been tracked via the GPS in the smartphone.

  The Optimized[99] app, for example, allows users to track everyday activities, visited places and people they met as well as to log their mood, stress level, health status, quality of sleep, weight, symptoms, period and other custom parameters. Moreover, Optimized automatically tracks users steps and active minutes, weather, temperature and moon phase. In combination with the free activity tracker Moves (moves-app.com), Optimized automatically tracks running, cy-

---

[96] Diet App Use by Sports Dietitians: A Survey in Five Countries, Jospe MR, Fairbairn KA, Green P, Perry TL, JMIR mHealth uHealth 2015;3(1):e7, http://mhealth.jmir.org/2015/1/e7/.

[97] Diet and Physical Activity Apps: Perceived Effectiveness by App Users, Wang Q, Egelandsdal B, Amdam GV, Almli VL, Oostindjer M JMIR mHealth uHealth 2016;4(2):e33, DOI: 10.2196/mhealth.5114, http://mhealth.jmir.org/2016/2/e33/.

[98] See app Zombie's Run https://zombiesrungame.com/

[99] Optimized - Lifelogging and Quantified Self Improvement App https://itunes.apple.com/us/app/optimized-lifelogging-quantified/id785042895?mt=8

cling, walking, steps, calories and locations. It also can integrate with Fitbit, Jawbone UP and any apps and devices connected to Apple's Health app.

The virtual life coach Ari translates all lifelogging and quantified self-data by automatically mining correlations, into answers: How does walking affect your sleep? How your time does spend at work influence your health? How do other people affect your mood? In fact, the more you track, the more insights you will get - and the more accurate they will be. As pointed out by Optimized, its goal is to help users discover more about their life, health and fitness, to improve their productivity and get decision support and motivation in their everyday life.

All of the benefits of these apps are based on the collection, storing and analysis of personal (health) data necessary for the users on prolong period to monitor their progress toward fitness, health and wellbeing goals and ultimately to make more informed decisions about their health and lifestyles. In the next section, we will explain how these benefits are provided. In other words, how these lifestyle and wellbeing apps function.

4. What is a mHealth app?

As we clarified in the previous section, an app is defined as a software program designed to run on smartphones, tablets and other wireless devices. They typically are available through application distribution platforms operated by the owner of the mobile operating system such as the Apple Store (iOS), Google Play (Android), Windows Phone Store, and BlackBerry App World.

The first mobile applications date back from the end of the twentieth century.[100] At that time, these applications were integrated into the cell phones by the manufacturer as games,[101] ringtones, calculators and calendars. In fact, manufacturers used to develop the phone software in-house because they did not want to expose the secrets of their phones to others due to the tough competition.

---

[100] History of Mobile Applications, Theory and Practice of Mobile Applications Professor John F. Clark

[101] Nokia was famous for putting the game Snake on some of its earliest phones. Other were adding games like Pong, Tetris, and Tic-Tac-Toe

However, the beginning of the new millennium saw a rapid evolution of smart technology and different customer expectations, which were some of the reasons operating systems of smartphones became open to third-party software developers. This allowed users of the smart device to download different apps besides the ones already installed by the manufacturer. At present smartphones are almost always connected to the internet and are equipped with a variety of sensors, including, but not limited to, temperature/humidity sensors,[102] touchscreens, accelerometers,[103] barometers,[104] RGB sensors,[105] gesture sensors,[106] face recognition,[107] finger hovering,[108] gyroscopes,[109] geomagnetic sensors,[110] proximity sensors,[111] voice recognition, GPS, cameras and

---

[102] Identifies temperature and humidity levels in the surrounding environment through a small hole located at the base of the smartphone. It then visually displays what the optimal comfort levels are for the user on the S Health screen. See more on http://global.samsungtomorrow.com/what-you-may-not-know-about-galaxy-s4-innovative-techonology/

[103] measures the smartphone's movement and is used as a Walking Mate, serving as a passometer that counts the number of steps a user has taken See more on http://global.samsungtomorrow.com/what-you-may-not-know-about-galaxy-s4-innovative-techonology/

[104] Ascertains the atmospheric pressure of a user's current location and determines the altitude. This is especially handy when the user is walking on inclined planes, such as a hill or mountain, because the barometer can accurately calculate how many calories are burned according to the atmosphere pressure and altitude. See more on http://global.samsungtomorrow.com/what-you-may-not-know-about-galaxy-s4-innovative-techonology/.

[105] Measures the intensity of light. See more http://global.samsungtomorrow.com/what-you-may-not-know-about-galaxy-s4-innovative-techonology/.

[106] Recognizes hand movements by detecting infrared rays that are reflected from the user's palm. This sensor allows users to accept a call, change songs, or scroll a web page up and down all with a wave of their hand. See more on http://global.samsungtomorrow.com/what-you-may-not-know-about-galaxy-s4-innovative-techonology/.

[107] Used to pauses a video when the user looks away and resumes when the user returns. This sensor also allows the user to scroll up and down without touching the screen.

[108] Technology activated by measuring electric currents that change when the user's hand is in close proximity to the touch screen. See more on http://global.samsungtomorrow.com/what-you-may-not-know-about-galaxy-s4innovative-techonology/.

[109] Detects the mobile phone rotation state based on the three axes rotation.

[110] Detects magnetic field intensity based on three axes. See more at http://global.samsungtomorrow.com/what-you-may-not-know-about-galaxy-s4innovative-techonology/.

fingerprint sensors. They have powerful onboard computing capability, capacious memories, large screens and open operating systems that encourage application development.[112] Hence, these hardware capabilities and the operating system allow app developers to develop apps with an astonishing range of purposes. Similarly, they allow communication to be personalised and enable users to customise their smartphones to suit their personal preferences.

Functioning of mHealth apps is possible only as part of the processing of data between many players in the app development landscape. Therefore, to better understand the functioning of the mHealth app we will first briefly describe the mHealth ecosystem. Understanding who the actors are, what their roles are and how they interact in the processing of personal data will provide answers in respect of who is a data controller, data processor and third party. For the purpose of this thesis we will make a distinction between four players:

- Manufacturers of the operating systems (OSs) and devices (smartphones, wearables, tablet computers, portable computers).[113] They process data necessary for smooth running of the device and security but also data generated by the users as well as data automatically generated by the device or personal data processed by the OS or device manufacturer resulting from the installation or use of apps.[114]

---

111 Recognizes situations where the user places the smartphone close to his or her face. See more on http://global.samsungtomorrow.com/what-you-may-not-know-about-galaxy-s4-innovative-techonology/.

112 How smartphones are changing the face of mobile and participatory healthcare: an overview, with example from eCAALYX. Boulos MN, Wheeler S, Tavares C, Jones R. 2011. Biomed Online. 10, 24. .10.1186/1475-925X-10-24. http://europepmc.org/articles/PMC3959919;jsessionid=8weYDTrgw1gGUrWyma29.0#r2

113 FDA Mobile Medical Applications - Guidelines for Industry and Food and Drug Administration Staff, September 2013 http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM263366.pdf.

114 Article 29 WP, Opinion 02/2013 on apps on smart devices, WP 202, Adopted on 27 February 2013, page 10.

- Distributors of the apps or app stores. Each of the OSs that produces smart devices has its own store such as 'Google Play,' 'iTunes App store,' 'Window phone store'. These app stores process data necessary for downloading the apps which require registration of the user's name, address, and payment detail if the app should be purchased or if later require in-app purchases. Data processed by the app stores can reveal purchase history as well as interests of the user.
- App developers and manufacturers.[115] There is a major difference between them. The 'author' who initiated and developed the specifications and purpose for the app is considered a 'manufacturer' of the mHealth app.[116] The developer designs and develops the mHealth app and makes it available to the end user. It can be an employee of a company or a private person. It is worth noting that to some extent they decide which categories of personal data the app will access and process on the device or through other app developers or third parties.[117] Thus, the app developers can be affected by the data protection law depending on their design choices when the app was created.[118] For instance, the responsibilities of the app developer will be significantly limited if they do not process personal data or make them available outside the device, or if the app developer has taken appropriate technical and organisational measures to ensure that data are irreversibly anonymised and aggregated on the device itself, prior to any data leaving the device.[119]

---

115 Article 1, paragraph 2f, COUNCIL DIRECTIVE 93/42/EEC of 14 June 1993 concerning medical devices.

116 FDA Mobile Medical Applications - Guidelines for Industry and Food and Drug Administration Staff, September 2013.

117 Article 29 WP, Opinion 02/2013 on apps on smart devices, WP 202, adopted on 27 Feb 2013, page 9.

118 Draft Code of Conduct on privacy for mobile health applications, 2015, page 3.

119 Article 29 WP, Opinion 02/2013 on apps on smart devices, WP 202, adopted on 27 Feb 2013, page 9.

- Third parties are involved in the processing of data through the use of the app. To briefly mention a few: services or infrastructure (internet service providers, cloud hosting services, application hosting services), wireless carriers [120] or analytical providers.

4.1. How do mHealth apps function?

Platforms or operating system providers offer app developers and others access to substantial amounts of user data from mobile devices (e.g., geolocation information, contact lists, calendar information, photos, etc.) through their application programming interfaces (APIs). Mobile applications are also able to exchange information via many network interfaces with other connected devices such as via Wi-Fi, Bluetooth, and NFC.[121]

Technically speaking, the functioning of mHealth apps depends on a permanent and smooth data flow between apps (software) and the OS[122] of the smart device (hardware). The data flow is possible through an interface called an Application Programming Interface (API). APIs are also mentioned in the PSI Directive as one of the conditions for re-using of data:

> In order to get access to the data opened for re-use by this Directive, the use of suitable and well-designed Application Programming Interfaces (APIs) is needed. An API describes the kind of data can be retrieved, how to do this and the format in which the data will be received. It has different levels of complexity and can mean a simple link to a database to retrieve specific datasets, a web interface, or more complex set-ups. There is general value in re-using and sharing data via a suitable use of APIs as this will help de-

---

120 FDA Mobile Medical Applications - Guidelines for Industry and Food and Drug Administration Staff, September 2013.
http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM263366.pdf.

121 European Data protection Supervisor, Guidelines on the protection of personal data processed by mobile applications provided by European Union institutions, November 2016, page 3.

122 App developers can develop apps for different operating systems (Android, iOS, Windows etc). In any case they will need to sign a license agreement. For example, the Android License agreement states '*You agree to use the Preview and write applications only for purposes that are permitted by (a) the License Agreement, and (b) any applicable law, regulation or generally accepted practices or guidelines in the relevant jurisdictions (including any laws regarding the export of data or software to and from the United States or other relevant countries)'.* See point 4.2 at https://developer.android.com/preview/license.html.

> velopers and start-ups to create new services and products. It is also a crucial ingredient of creating valuable ecosystems around data assets that are often unused. The set-up and use of API need to be based on several principles: stability, maintenance over the lifecycle, uniformity of use and standards, user-friendliness as well as security. For dynamic data, meaning frequently updated data, often in real time, public sector bodies and public undertakings shall make this available for re-use immediately after collection by ways of suitable APIs.[123]

Actually, the operating system (OS) and device manufacturers are the entities responsible for installing the API.[124] The API interface that is built into devices enables apps to access data collected by or stored in the device. Consequently, the app developer will be able to access data that the OS and device manufacturers make available through the API.[125]

To elucidate, API is a code that allows two software programs to communicate with each other. Just as any piece of hardware requires the right kinds of cables and wiring to connect to the electrical grid or other hardware devices, the software requires a set of code lets and protocols to interface with other pieces of software.[126] It is a software intermediary that makes it possible for application programs to interact with each other and to import or export data in order to enrich the customer value of their apps. APIs are released to third-party developers as part of a software development kit (SDK) or as an open API.[127]

---

123 Article 28, Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the re-use of public sector information (recast), Brussels, 25.4.2018, COM(2018) 234 final, 2018/0111(COD)

124 Article 29 WP, Opinion 02/2013 on apps on smart devices, WP 202, Adopted on 27 February 2013, page 10.

125 Mobile Privacy Disclosures FTC Staff Report | February 2013 # Building Trust Through Transparency, page 15

126 Cabello, F., Franco, M. G. & Haché, A. (2013). The social web beyond 'walled gardens': interoperability, federation and the case of Lorea/N-1. PsychNology Journal, 11(1), 43–65, from www.psychnology.org, page 46

127 'Opening an API to an application creates opportunities for external innovation. Giving third-party developers programmatic access to an application allows them to add value in unanticipated ways and adds re-

The latest trends in this sector are API aggregators or companies that enable and facilitate app–app or app–sensor connections. These companies provide 'one-stop connecting' models for (health) data API. Thus, they allow the collection of mHealth apps in one place. On the other hand, API Managed Services players provide the technical infrastructure to facilitate the connection of apps, sensors and medical databases.[128] The APIs might be the key player that will enable transferring personal health data, generated by one lifestyle and wellbeing app to another.

4.2. Collecting, storing and processing data

Smartphones on which lifestyle and well-being apps are installed are almost always linked to the owner of the device and can be characterised as personal, portable, frequently used and commonly always on.[129] They have direct access to many different sensors and to data coming from the built-in applications such as email, contacts, calendars messages or apps. For example:

- GPS or location data[130] can reveal the habits and patterns of the owner of a mobile device. Consequently, the sleeping place, regular travel pattern in the morning, the location of an employer may be deduced, as well as places that reveal sensitive data such as a visit to a hospital, religious places, or political institutions.
- Biometric data used for biometric recognition methods such as fingerprints, iris and facial recognition. In this case, the mobile device can be used only by the person that has provided the biometric data.

---

sources to your development effort that you would not otherwise have access to. This is what Google does when it gives users access to its vast computing infrastructure when providing such services as Google Maps, or any of its other'.

[128] mHealth App Developer Economic 2014 – The State of the Art of mHealth App Publishing.

[129] ICO Privacy in mobile apps. Guidelines for app developers December 2013 https://ico.org.uk/media/for-organisations/documents/1596/privacy-in-mobile-apps-dp-guidance.pdf.

[130] Article 29 WP, Opinion 13/2011 on Geolocation services on smart mobile devices, WP 185, 16 May 2011, page 5.

- Audio data with voice recordings also represent data, since voice matching can uniquely identify the person to whom the audio data is to be assigned to.
- App usage information, for example, which app was and when used by the user.
- They most probably know the identity of data subject for example if the user uses the mobile device with his own name.

Additionally, the correct management of a network requires the transfer of certain information elements relating to each device on the network. For example, a Wi-Fi access point that manages the connection between wireless devices and a wired network will process unique and non-unique information elements such as the MAC address and channel in order to correctly maintain connections and correctly route data packets.[131] On the other hand, some data can be automatically generated by the device, on the basis of features pre-determined by the OS, the device manufacturer or by the relevant mobile telephony provider such as:

IMEI: International Mobile Equipment Identity

UDID: Unique Device ID (=device number of an iOS device)

IMSI: International Mobile Subscriber Identity (card number)

MAC-address: Media Access Control-Address (the Hardware-Address of a network adapter)

MSISDN: Mobile Subscriber ISDN-Number (the mobile telephone number).

Unique device and card identifiers that are permanently connected to a device or card can be routinely assigned to a person. Some of the identifiers are sometimes stored by the network operators together with the name of a person or the identifiers are assigned in connection with a registration of the registered person.

Many of these identifiers cannot be deleted or changed by users, since they are generated by the operating system (such as IMEI, IMSI, MSISDN and specific unique device iden-

---

[131] Article 29 WP, Opinion 9/2014 on the application of Directive 2002/58/EC to device fingerprinting WP 224, Adopted on 25 November 2014.

tifiers added). Third parties often access unique identifiers to single out (groups of) users and serve them with targeted advertisements. Consequently, third parties have the potential to process significant amounts of data without the end user being in control or agreeing to it.[132] The IP address is necessarily required for mHealth apps for internet communication.

Furthermore, lifestyle and wellbeing apps are able to collect large quantities of real-time data provided by the user. This data is then processed in order to provide new and innovative services to the user. However, these same data can be further processed, typically to provide a revenue stream, in a manner which may be unknown or unwanted by the end user.[133]

Additionally, they are capable of collecting data without the user's knowledge, for example when user data is linked with an external data source (payment with Credit card) or by using a third-party site or service to provide a login (login to Facebook or Twitter accounts from the app). Moreover, data can be also collected by third-party advertisers while the users are using an app.[134]

Collected data is often stored on the mobile device in an app's 'documents directory' (sandbox)[135]. This sandbox can reveal a user's data history such as a cache of all viewed ads and searches (URLs about health conditions and drug information). In fact, data can be also stored on the mobile device's SD card or on the developer's website. Beside the

---

132 Article 29 WP Opinion 02/2013 on apps on smart devices, WP 202, Adopted on 27 February 2013, page 13.

133 Opinion 02/2013 on apps on smart devices, Article 29 WP, February 2013, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp202_en.pdf.

134 Technical Analysis of the Data Practices and Privacy Risks of 43 Popular Mobile Health and Fitness Applications, Craig Michael Lie Njie, released August 12, 2013, http://www.privacyrights.org/mobile-medical-apps-privacy-technologist-research-report.pdf.

135 Opinion 02/2013 on apps on smart devices, Article 29 WP, February 2013, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp202_en.pdf.

users data being stored on the device, often there are cookies and other tracking identifiers stored locally as well.[136]

Data collected from the app is transmitted by use of all network communications to the app developer's websites[137] or to third parties that the developer uses to provide certain functionalities[138] (an app often uses products and services from others) and to third-party analytics and advertising sites. The business model of an app has an influence on the amount of data collected (free or paid). The free apps rely on revenue from advertising, which means apps will provide more detailed information about their users in order for advertisers to optimise their campaigns and earn more money.

To illustrate this, I will describe how Nike running app[139] collects, use and share user information by analysing their privacy policy.

a) Data provided by the user

Based on the review of their privacy policy, the Nike running app collects information given by the user or permitted by the user to be accessed. Information may include, but is not limited to, name, image, birth date, email and physical address, telephone number, gender, contact lists, social media information and profile, location (GPS) information and when necessary, credit card information. For example, they request access to the us-

---

[136] 79% of the free mobile health and fitness apps we analysed use and store cookies and other tracking identifiers locally on the device. See Technical Analysis of the Data Practices and Privacy Risks of 43 Popular Mobile Health and Fitness Applications, Craig Michael Lie Njie, released August 12, 2013, http://www.privacyrights.org/mobile-medical-apps-privacy-technologist-research-report.pdf.

[137] 78% of the free mobile health and fitness apps and 40% of the paid apps we analysed send data to the developer. See Technical Analysis of the Data Practices and Privacy Risks of 43 Popular Mobile Health and Fitness Applications, Craig Michael Lie Njie, Released August 12, 2013, http://www.privacyrights.org/mobile-medical-apps-privacy-technologist-research-report.pdf.

[138] 52% of the free mobile health and fitness apps and 40% of the paid apps we analysed send data to third-party sites as part of their core functionality. See Technical Analysis of the Data Practices and Privacy Risks of 43 Popular Mobile Health and Fitness Applications, Craig Michael Lie Njie, Released August 12, 2013, http://www.privacyrights.org/mobile-medical-apps-privacy-technologist-research-report.pdf.

[139] Nike Privacy Policy and Cookie Policy – Europe, see more on http://agreementservice.svs.nike.com/rest/agreement?agreementType=privacyPolicy&uxId=com.nike.commerce.nikedotcom.web&country=GB&language=en&requestType=redirect.

er's phone's geolocation data in order to log their run route or to their social network credentials in order to post content from an app to a social network.

Activity and performance information includes data on physical characteristics, including weight, height, and body measurements (such as estimated stride and shoe/foot measurements or bra size). They collect fitness activity data provided by the user or generated through the app such as time, duration, distance, location, and calorie count, as well as sensor data like heart rate and (GPS) location, or movement data from the device's accelerometer.

b) Data provided by the smartphone

The smartphone may automatically collect information regarding user interaction with, and use of, their products and services. Information that may be collected includes, but is not limited to, telephone number, device identifier and hardware information, IP address, browser type and language, cookie information, system type, whether they have to enable software to access certain features, access times, referring website URLs, as well as information about purchases and other information about users interactions.

c) Usage of data

The app/Nike may use the user's information to enhance, customise and personalise experiences and communications, such as running routes, race registrations, and other activities. The user's data may also be used to provide, improve and maintain products and services, including analysing user behaviour and trends, as well as for marketing purposes. For example, data from the app that tracks fitness activity or physical characteristics is collected and stored so that the user can review it in the app. As fitness activity data includes the type of activity engaged in by the user as well as data collected by his device during the course of the activity such as location data and movement data. This activity data may be used to calculate further information, such as distance run, or calories burned, so that the calculated information can be provided to the user as part of the functionality of the app.

d) Sharing of data

The app may provide the user's information to Nike's companies and affiliates, or to service providers. For example, they may handle credit card processing, shipping, data management, email distribution, market research, information analysis, and promotions management.

Despite the fact that here we explain the functioning of the Nike app, lifestyle and well-being apps function more or less the same. Thus, one can conclude that they are collecting a large amount of data that can be considered as personal (health) data. Consequently, they fall within the scope of the Data Protection Regulation, as we will discuss in Chapter 3.

4. Why do people care about data generated from mHealth apps?

Lifestyle and wellbeing apps are technically no different from other apps for any other purpose. However, the fact is that they have an impact on human lives, quality of life and associated with data that contain health information.[140] We have already pointed out that the data generated by lifestyle and wellbeing apps is necessary to be stored and accessed for a prolonged period to monitor user progress toward fitness, health and wellbeing goals and ultimately to aid users make more informed decisions about their health and lifestyles. In other words, these apps are considered as tools to enable users to eat healthier, move more and become aware of 'sustainable' lifestyles.[141]

Some studies suggest that use of health and wellbeing apps actually influences the maintenance of healthy behaviours, and also, depending on the goal, adoption of new

---

[140] What is the Internet of medical things? The Journal of mHealth, A White paper by Intersog, October 2016, p. 2.

[141] The lifestylisation of healthcare? 'Consumer genomics' and mobile health as technologies for healthy lifestyle - Applied &Translational Genomics, Volume 4, March 2015, pages 44–49, Federica Lucivero, , Barbara Prainsack http://dx.doi.org/10.1016/j.atg.2015.02.001.

behaviours.[142] There are three key components that are critical to long-term engagement with these apps: (1) habit formation (setting cues, routines, and rewards), (2) social motivation (sharing or competing for goals with others), and (3) goal reinforcement or feedback to monitor personal progress.

For example, by recording and tracking food intake and physical activities, apps provide feedback on how well users are reaching their goals, which can significantly increase user motivation. Frequent use of these apps over time can result in a positive evaluation of self-performance. This could lead to an improved attitude towards the behaviour or activity, particularly when the app has options to show users their progress over time through social networks.

As will be discussed below, it is important for users to have control over this data for a prolonged period of time and to be able to transfer their data from one app to other.

5. Conclusion

This chapter described what is mHealth, how it works, and why people care about data generated from lifestyle and wellbeing apps.

Some of the apps allow users to conduct self-diagnoses, to measure vital signs such as heart rate, blood glucose level, and blood pressure, or to measure physical activities such as running and walking, as well as provide fitness and dietary recommendations. Apps used in the medical or health context are called mobile health applications (mHealth apps) and together with the devices on which are installed form the mobile health (mHealth) concept, defined as:

> a sub-segment of eHealth that 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.

---

[142] Diet and Physical Activity Apps: Perceived Effectiveness by App Users, Wang Q, Egelandsdal B, Amdam GV, Almli VL, Oostindjer M JMIR mHealth uHealth 2016;4(2):e33 http://mhealth.jmir.org/2016/2/e33/.

Thus, mHealth is a sub-segment of eHealth and is closely related with telemedicine, even considered by some to be an 'extension'[143] of telemedicine. Actually, one of the key elements of mHealth is its potential to allow the establishment of treatment relationships between a patient and a physician that are not dependent on the geographical location. However, this treatment relationship is not included in this study.

Currently, large numbers and varieties of medical, lifestyle and wellness-related apps exist on the market. Nevertheless, for the purpose of this thesis, these types of apps will be classified in two main groups: (1) apps for the purpose of prevention, diagnosis and treatment of diseases (or medical apps); and (2) lifestyle, fitness and well-being apps. This taxonomy allows us to elucidate the crucial differences between them, and elaborate why the first group of apps are not included in our analyses.

Smartphones on which lifestyle and well-being apps are installed are almost always linked to the owner of the device and can be characterised as personal, portable, frequently used and commonly always on.[144] Hence, since the app is most commonly installed on a smart device, which is mostly used by and connected with the owner of the device, this allows the user to be identified, directly or indirectly.[145]

Furthermore, the functioning of lifestyle and wellbeing apps is based on the collection, storing and analysis of data necessary for a prolonged period to allow users to monitor their progress toward fitness, health and wellbeing goals and ultimately to make more informed decisions about their health and lifestyles. Consequently, it is important for the users to have control over this data for a long period of time and to be able to transfer their data from one app to other. This control over the data, or possibility to transfer the data from one app to other, derives from the new right to data portability introduced in

---

[143] Widespread Deployment of Telemedicine Services in Europe Report of the eHealth Stakeholder Group on implementing the Digital Agenda for Europe Key Action 13/2 'Telemedicine' Version 1.0 final (12 March 2014)

[144] ICO Privacy in mobile apps. Guidelines for app developers, December 2013, https://ico.org.uk/media/for-organisations/documents/1596/privacy-in-mobile-apps-dp-guidance.pdf.

[145] The guidelines for mobile apps (Privacy in mobile apps). A good example in the mobile environment would be a unique device identifier such as an IMEI number: even though this does not name the individual, if it is used to treat individuals differently it may fit the definition of personal data.

the Data Protection Regulation and discussed in Chapter 4. However, companies also have an interest in the data. This is the result of the data-driven economy, an issue which will be discussed in Chapter 5.

CHAPTER 3: PERSONAL DATA, DATA PROTECTION, PRIVACY AND mHEALTH APPS

1. Introduction

The aim of this Chapter is to discuss the application of the General Data Protection Regulation, Article 8 of the European Convention of Human Rights as well as Articles 7 and 8 of the Charter of Fundamental Rights of the European Union in the context of data processed by mHealth apps. As we discussed and concluded in the previous chapter, the functioning of these apps entails processing of data that relate to identified or identifiable natural persons,[146] or data concerning the user of the app and owner of the smart phone. Indeed, as one researcher discovered, only four spatiotemporal points are needed to identify 95% of individuals[147] or users of the smart phones. Having in mind the technical functioning of the mHealth apps, analysed through the prism of the relevant legal requirement for protection of personal data, we will conclude that this data processing falls within the scope of the GDPR definition of personal data. In some cases, this data might fall in a special category of data – health data – which has long[148] been considered to be personal and deserving higher privacy protection. The reasoning behind this is that misuse of special (health) data might have long-term consequences,[149] which can lead to infringement of the right to privacy and discrimination. This could result in two

---

[146] Article 29 Working Party, Opinion 8/2014 on the on Recent Developments on the Internet of Things, adopted September 2014, WP 223 p. 4.

[147] Unique in the Crowd: The privacy bounds of human mobility, Yves-Alexandre de Montjoye, César A. Hidalgo, Michel Verleysen & Vincent D. Blondel, Published online: 25 March 2013 https://www.nature.com/articles/srep01376.

[148] Privacy has been a part of medicine since the 4th century B.C, when the importance to protect medical and health data has been recognized via the Hippocratic oath 'What I may see or hear in the course of the treatment or even outside of the treatment in regard to the life of men, which on no account one must spread abroad, I will keep to myself, holding such things shameful to be spoken about.' – Cross-Cultural perspectives of medical ethics – Robert M. Veatch, The Hippocratic oath: Text, Translation and Interpretation (Chapter 1).

[149] Article 29 Working Party Advice Paper on Special Categories of Data (sensitive data), http://ec.europa.eu/justice/dataprotection/article29/documentation/otherdocument/files/2011/2011_04_20_letter_artwp_mme_le_bail_directive_9546ec_annex1_en.pdf , p. 4.

types of concerns. The first one is a social concern – disclosure of health data potentially could lead to discrimination and being socially ostracised. Whereas the second concern is economic – disclosure of health data to third parties can lead to (a) denial of health insurance (or increase the price of such insurance), and (b) reduced access to credit if disclosed to banks.

The issues concerning collecting, storing and processing user data from the mHealth apps tackle different aspects of the user life that are deemed private. Hence, we will define privacy for the purpose of this thesis. This is in line with the objective of the rules contained in the Regulation 'to protect the fundamental rights and freedoms of individuals, in particular, their right to privacy, with regard to the processing of personal data'. Talking about privacy and data protection, one must clarify that these are two closely related but different concepts. Hence, further in the chapter, we will explain the relationship between data protection law and the right to privacy.

In terms of privacy, the focus will be on the aspects of information privacy in relation to data protection law. Actually, data protection law is an important tool that regulates what happens when personal data is processed, and grants users of mHealth apps to have greater control[150] over their personal data. To start the discussion, we will first need to clarify when and whether the data processed from mHealth apps is personal data, and when the data can be categorised as sensitive (health) data. Further, we will discuss the various exceptions for processing health data and if the household exception applies in this case. The chapter will be organised as follows: (1) discussion of the concept of personal data and health data in the EU data protection law, (2) the exceptions for processing personal data and exceptions for processing health data, (3) the relationship between the right to data protection law and right to privacy, (4) the definition of privacy – privacy as control, and (5) a conclusion.

---

[150] GDPR, Recital 7 '...Developments require a strong and more coherent data protection framework in the Union, backed by strong enforcement, given the importance of creating the trust that will allow the digital economy to develop across the internal market. Natural persons should have control of their own personal data. Legal and practical certainty for natural persons, economic operators and public authorities should be enhanced'.

2. The concept of personal data in the EU

Before we start the discussion and clarify whether the data processed from lifestyle and wellbeing apps fall within the scope of the definition of personal data, first we will outline the legal sources in the EU for data protection. Second, we will provide a historical overview of the evolution of the concept of personal data. This section aims, first, to illustrate how the concept of personal data has been evolving in parallel with technological development. Second, it will ask whether the current definition can respond to the new technological challenges, particularly the mHealth apps.

Data protection in the European Union is based on two types of law, primary and secondary. Primary law is considered to be the Treaty on European Union (TEU) and the Treaty on the Functioning of the European Union (TFEU), while secondary law is considered to be directives, regulations[151] and decisions grounded on the rights, obligations and values enshrined in the Treaties. It is worth noting that the original Treaties did not contain a reference to human rights or their protection, such as the right to privacy or protection on personal data. The reason is that the initial idea for establishing the European Economic Community (now European Union) had been economic interests and common market. The cases before the Court of Justice of the European Union (hereafter CJEU) regarding violation of human rights within the scope of the EU, have been addressed based on the interpretation of the Treaties and principles reflected in human rights protection established in national constitutions and human rights treaties, in particular the European Convention for the Protection of Human Rights and Fundamental Freedom (hereinafter the ECHR).

---

[151] Relevant in the field of data protection: (1) Regulation (EU) 2016/679 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); (2) Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications); (3) Directive (EU) 2016/680 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 (Data Protection for Police and Justice Authorities), (4) Regulation (EC) No. 45/2001 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data (EU Institutions Data Protection Regulation)

The need for the EU to have a Fundamental Rights instrument has been evident. Therefore, in 2000 in Nice, the EU Charter of Fundamental Rights was signed and has been legally binding since 2009. The core principle of the Charter has been to confirm the rights enshrined in the constitutional traditions and international obligations common to the Member States, the Treaty on European Union, the Community Treaties, the ECHR, the Social Charters adopted by the Community and by the Council of Europe and the case law of the Court of Justice and of the European Court of Human Rights (hereinafter the ECtHR). At the beginning, it has been only a political document, while, later in 2009 became a legally binding EU primary law.[152]

Additional sources for data protection are the Council of Europe (CoE) Convention No.108,[153] the only international legally binding instrument that regulates data protection issues, and is signed by all EU Member States, as well as the opinions issued by the Article 29 Working Party (hereinafter the Article 29 WP). Its opinions have a major influence between data protection practitioners and lawyers. It is composed of representatives from the national data protection authority of each EU Member State, a representative of the European Data Protection Supervisor[154] and a representative of the European Commission.

Based on the analyses of the outlined legal framework, one can conclude that the concept of personal data in EU emerged in the twentieth century. Indeed, back in the 1970s and 1980s, the technological developments or more specifically proliferation of computers that processed variety of data on EU citizens as well as novel business practices have begun to challenge the post-war conception of privacy.[155] The need for action has made it

---

[152] 1st of December 2009 is the moment when The Lisbon Treaty came into force. Article 6 (1) of this Treaty states '1. The Union recognizes the rights, freedoms and principles set out in the Charter of Fundamental Rights of the European Union of 7 December 2000, as adapted at Strasbourg, on 12 December 2007, which shall have the same legal value as the Treaties'

[153] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data.

[154] It is an independent supervisory authority that is responsible for ensuring that all EU institutions and bodies respect the right to personal data protection and privacy when processing personal data.

[155] Updating the law of Information Privacy: The new framework of the European Union, Marc Rotenberg & David Jacobs.

necessary on one hand to reconcile the fundamental values of the respect for privacy and on the other hand to answer to the free flow of information between people.[156] Consequently, in 1981, the Council of Europe[157] enacted Convention No. 108,[158] which has been recently amended.[159] This Convention has been the first binding international instrument that protects the individual against abuses arising from automatic collection and processing of personal data, and at the same time has sought to regulate the trans-frontier flow of personal data.[160]

This Convention for the first time had introduced the concept of personal data in Europe. Nonetheless, it is worth noting that this concept has been already introduced in the OECD Guidelines[161] one year earlier as well as in some of the OECD member states.

---

[156] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Jan. 28, 1981 [Convention 108], available at: http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm.

[157] The Council of Europe is leading human rights organisation. Presently it includes 47 member states, 28 of which are members of the European Union. It has produced a number of legal instruments known as Treaties (Conventions, Charter, Agreements). All Council of Europe member states have signed up to the European Convention on Human Rights, a treaty designed to protect human rights, democracy and rule of law. The Council of Europe and the European Union are separate entities that share the same fundamental values – human rights, democracy and the rule of law – they perform different, yet complementary, roles. By the mid-1970s, the Committee of Ministers of the Council of Europe adopted various resolutions on personal data protection, referring to Article 8 of the ECHR. Council of Europe, Committee of Ministers (1973), Resolution (73) 22 on the protection of the privacy of individuals vis-à-vis electronic data banks in the private sector, 26 September 1973; Council of Europe, Committee of Ministers (1974), Resolution (74) 29 on the protection of the privacy of individuals vis-à-vis electronic data banks in the public sector, 20 September 1974.See more at: http://www.coe.int/en/web/portal/european-union

[158] See *Id.*, preamble.

[159] Enhancing data protection globally: Council of Europe updates its landmark convention - Council of Europe, Elsinore (Denmark), 18 May 2018. More about reasons for the modernisation and the amendments can be found at: https://www.coe.int/en/web/portal/-/enhancing-data-protection-globally-council-of-europe-updates-its-landmark-convention

[160] See *Id.*, Summary.

[161] 'Personal data' means any information relating to an identified or identifiable individual (data subject)'; OECD Guidelines on the Protection of Privacy and Trans border Flows of Personal Data -The Recommendation was adopted and became applicable on 23 September 1980, http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm.

The Convention defined 'personal data' as *'any information relating to an identified or identifiable individual'*[162] that can be collected and processed 'fairly and lawfully'[163] stored only 'for specified and legitimate purpose,[164] be accurate and up to date,[165] to be limited to what is needed for those purposes, and to be kept only as long as is required for the purpose which the data is collected. Article 6 also defined which type of personal data will be considered a special category of personal data.[166] In fact, despite the introduction of the concept of personal data, it also introduced the key principles for processing of personal data, still valid today.

Yet, for these articles to become reality, the states that signed this Convention had a duty to pass domestic legislation that would actualise the Convention's principles. However, over the course of time, this had been seen as a weakness, for the reason that it permitted broad discrepancies among states and additionally, ratification had been slow.[167] Therefore, in order to adjust the incompatible data protection laws in the EU, in 1990 the EC (European Commission) published a draft of the Data Protection Directive. This Directive was adopted in 1995,[168] and created the first legal framework in the EU, that, on one hand, governs the movement of personal data within the EU, while, on the other hand, advocates requirements essential for secure storage, transmission, and processing

---

[162] See Article 2 (a) of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Jan. 28, 1981 [Convention 108].

[163] See *Id.*, Article 5(a).

[164] See *Id.*, Article 5(b).

[165] See *Id.*, Article 5(c).

[166] 'Personal data revealing racial origin, political opinions or religious or other beliefs, as well as personal data concerning health or sexual life, may not be processed automatically unless domestic law provides appropriate safeguards. The same shall apply to personal data relating to criminal convictions'. In our further analyses we will focus only on health data as a special category of personal data.

[167] Updating the law of Information Privacy: The new framework of the European Union, Marc Rotenberg &David Jacobs (page 12).

[168] 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, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML

of personal data. The Directive has mirrored the data protection principles already contained in the national laws as well as in Convention 108. But it also expanded them by adding instruments of protection, such as independent supervision and the Data Protection Authority.

At this point in time, data protection had been introduced into the legal framework of the European Union as an internal market issue with two goals. The first one had been to promote the internal market, and the second one had been to set clear standards for data transfers and at the same time protecting a fundamental human right. The nature of the Directive as a general legal framework allows complementation by specific regimes for data protection for specific sectors.[169]

The Directive, compared with the Convention, defined personal data more broadly 'in order to cover all information which may be linked to an individual'.[170] It defined personal data as:

> *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 identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity…*[171]

According to the Opinion[172] of the Article 29 Working party (Hereafter Article 29WP),[173] the definition consists of four main building blocks: 'any information', 'relat-

---

[169] For example, ePrivacy Directive and sectorial regulation. Article 29 Working party, WP 168, 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, Adopted on 1st December 2009, page 6.

[170] COM (90) 314 final, 13.9.1990, p. 19 (commentary on Article 2), http://aei.pitt.edu/3768/1/3768.pdf.

[171] Article, 2 (a), 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 , http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML.

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

[173] Article 29 Working party is composed of a representative from the national data protection authority of each EU Member State, a representative of the European Data Protection Supervisor (the independent supervisory authority that is responsible for ensuring that all EU institutions and bodies respect people's right to

ing to', 'an identified or identifiable', 'natural person' which are closely intertwined and feed on each other. Even though these four building blocks relate to the concept of personal data as defined in the Directive, they are still relevant to the definition of personal data in the Regulation. These four main parts of the definition will be analysed in the context of mHealth apps in the next section (3.1).

Since 1995, when the Directive has been adopted, numerous new technologies have changed the market in a significant way, and thus the ways personal data is processed. As a result, data sharing and collecting have increased dramatically. The new technologies have also allowed easier identification of natural persons. For example use of the internet, cloud computing, online identifiers and other technologies have presented a new challenge that the Directive was not able to answer. Another problem arose from the nature of the Directive. As a Directive member states could implement it non-uniformly, as long as they meet minimum requirements. This also has been reflected in the definition of personal data. In practice, some uncertainty and diversity existed among the Member States regarding important aspects of this concept, which affected the proper functioning of the data protection framework in different contexts.[174] Consequently, it has led to different levels of protection of the right to personal data within the EU, in particular, processing of their personal data in the context of the online activity.[175] The side effects of such a situation could be first, to prevent the free flow of personal data throughout the Union[176] and second, could lead consumers to hesitate to buy online and adopt new ser-

---

personal data protection and privacy when processing their personal data) and a representative of the European Commission.

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

[175] Comparative Study on Different Approaches to new Privacy Challenge's in Particular in the light of the technological developments - January, 2010 European Commission, DG Justice, Freedom and Security. http://ec.europa.eu/justice/policies/privacy/docs/studies/new_privacy_challenges/final_report_en.pdf.

[176] See Recital (9) General Data Protection Regulation.

vices. Overall, it could slow down the expansion of novel uses of the new technologies.[177]

Therefore, to respond to these problems the European Commission proposed the General Data Protection Regulation. The GDPR entered into force on the 24th of May 2016 and started to apply from 25th of May 2018.[178] As Regulation it is directly applicable to all EU Member States. The difference between the Directive and the Regulations is that the latter does not have to be transposed into the different national laws of the EU Member states. Yet, the 'opening clauses' in the GDPR give the Member States freedom to introduce additional national provisions and further specify the application of the GDPR. It is necessary to clarify, that, even though the directive has been replaced by the General Data Protection Regulation the pre-existing opinions and case law remains relevant and valid for the interpretation and application of EU data protection principles. For the reason, that core principles and concepts of the Data Protection Directive are retained in the GDPR. This clarification has been necessary because further in the discussion we will use the CJEU case law.

Other deference between them is the definition of personal data. In the GDPR is to some extent different compared to the one in the Directive. Article 4(1) of the GDPR defines personal data as:

> *any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier[179] or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;'*

---

[177] 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), Brussels, 25.1.2012 COM (2012) 11 final, page 1.

[178] European Commission, DG Justice, Data Protection http://ec.europa.eu/justice/data-protection/.

[179] GDPR, Recital 30 'provided by their devices, applications, tools and protocols, such as internet protocol addresses, cookie identifiers or other identifiers such as radio frequency identification tags. This may leave traces which, in particular when combined with unique identifiers and other information received by the servers, may be used to create profiles of the natural persons and identify them.

The wording reveals the intention of the regulator to endorse a definition that is wide enough to foreseen developments and catch all 'grey zones' within its scope[180] and to be technology neutral. Furthermore, the phrasing also exposes its absolute approach to identifiable persons, including the same four building blocks as the Directive. Yet, personal data is defined to some extent more broadly by adding a name, location data, online identifier and also genetic information as potential identifiers of a person.

Some argue that this definition is problematic, as it could mean that all data is potentially personal data. This stems from the fact that, data, which at one moment in time may contain no information about a specific person, may in the future be used, through advanced techniques to identify or individualise a person.[181] One possibility is through interconnecting databases, so when two or more de-identifying datasets are integrated, they may become identifying datasets.[182]

Having in mind the aim of this section, one can conclude that the way the definition is formulated responds to the current technological challenges, in particular mHealth apps. The analysis of Recital 30 provides further explanation on this issue, which refers to the online identifier:

> *provided by their devices, applications, tools and protocols, such as internet protocol addresses, cookie identifiers or other identifiers such as radio frequency identification tags. This may leave traces which, in particular when combined with unique identifiers and other information received by the servers, may be used to create profiles of the natural persons and identify them.* [183]

Even though mHealth apps are not directly mentioned, it is obvious that they fall within the definition of personal data introduced in the GDPR. This conclusion is built on two

---

180 Article 29 Working Party, Opinion 4/2007 on the concept of personal data, adopted on 20th June, WP136, page 5.

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

182 M. R. Koot, Measuring and Predicting Anonymity, Amsterdam: Informatics Institute cop., 2012, p 101 http://dare.uva.nl/document/2/107610.

183 GDPR, Recital 30.

findings. First, based on the discussion from Chapter 2, from how the app is functioning and what kind of data is collecting one can conclude that these apps are considered as online identifiers. Second, online identifiers in combination with other data can directly or indirectly identify the user of an mHealth app. To clarify once again, smart phones on which apps are installed, are portable, frequently used, commonly always on and personal. They typically have direct access to many different sensors and personal data,[184] necessary for proper functioning, such as:[185]

- the identity of the data subject, if the user uses the smart device with his real name.
- Location data or GPS[186] which can reveal the activities, lifestyles and patterns of the owner of a smart device such as a sleeping place, everyday travel track such as from home to the location of an employer. All this is considered as personal data since it can indirectly identify the user of the mHealth app. In addition, it can locate places that reveal sensitive personal data such as a visit to a hospital, religious places, or political institutions.
- Biometric data which is used as recognition methods such as fingerprint, iris and facial recognition is personal data. Since only the person that has provided the biometric data can use the smart phone.
- Audio data and voice recordings are also considered as personal data. Since they can be used to uniquely identify the person with the audio data.
- Smart phones also collect information about apps usage, in other words, which app was and when used by the user.
- Additionally, the correct management of a network requires the transfer of certain information elements relating to each smart device on the network. For example, a Wi-Fi access point which manages the connection between smart

---

184 Article 29 WP Opinion 02/2013 on apps on smart devices, WP 202, Adopted on 27 February 2013, page 8.

185 Orientierungshilfe zu den Datenschutzanforderungen an App-Entwickler und App-Anbieter, Bayerisches Landesamt für Datenschutzaufsicht, 16 June 2014, page 5.

186 Article 29 WP, Opinion 13/2011 on Geolocation services on smart mobile devices, WP 185, 16 May 2011, page 5.

phone and a wired network will process unique and non-unique information elements such as the MAC address and channel in order to correctly maintain connections and correctly route data packets.[187] On the other hand, certain data can be routinely generated by the device. For instance, that can be case (a) on the basis of features pre-determined by the OS, (b) by the manufacturer of the device, or (c) by the mobile telephony provider. The best-known identifiers are the following:

IMEI: International Mobile Equipment Identity

UDID: Unique Device ID (device number of an iOS device)

IMSI: International Mobile Subscriber Identity (card number)

MAC-address: Media Access Control Address (Hardware-Address of a network adapter)

MSISDN: Mobile Subscriber ISDN-Number (mobile telephone number)

Unique device and card identifiers are permanently connected to a device or card, which related to a user of the smart phone. For instance, some of these identifiers are sometimes stored by the network operators together with the name of the user or the identifiers are assigned in connection with a registration of the registered person when the card number is bought.

Many of these identifiers cannot be deleted or changed by users since they are generated by the operating system (such as IMEI, IMSI, MSISDN and specific unique device identifiers). Third parties often access unique identifiers to single out users and serve them with targeted advertisements. Consequently, third-parties have capability to process substantial quantities of personal data without the end user is in control.[188]

---

[187] Article 29 WP, Opinion 9/2014 on the application of Directive 2002/58/EC to device fingerprinting WP 224, adopted on 25 November 2014.

[188] Article 29 WP Opinion 02/2013 on apps on smart devices, WP 202, Adopted on 27 February 2013, page 13.

- Last on the list, is the IP address necessarily required for an app internet communication.

Accordingly, in the online world, data processed by the mHealth apps can be provided by the user of the app, collected by the sensors or as a result of linking the user with online identifiers provided by their smart devices on which the app is installed. These identifiers as explained above can be internet protocol addresses, cookie identifiers or others. The combination of all this data could lead to the creation of profiles of the mHealth app users and could most likely indirectly identify them.[189] The issue of the online identifiers, in particular, IP addresses, has been addressed by the European Court of Justice, in two different cases: the *Scarlet v Sabam* case,[190] and *Patrick Breyer v Federal Republic of Germany*. [191] In both cases, but in different connotations, the discussion revolved around the question of whether IP address can be considered as personal data or not.

In *Scarlet*, Court decided that the IP addresses of the concerned internet users were considered to be personal data because they allowed users to be precisely identified. While this Court decision refers to the situation where internet service providers carried out the collection and identification of the IP addresses of the concerned internet users, the second case is slightly different. In *Breyer*, instead of internet service providers, an online media services provider, specifically the Federal Republic of Germany, registers IP addresses of the users of a publicly accessible website. Namely, the difference was that they do not have the additional data necessary to identify the users, compared with internet service providers as in *Scarlet*. The Court explicated that these IP addresses are 'dynamic' IP addresses, in other words temporary addresses given for each internet connec-

---

[189] Opinion 05/2014 on Anonymisation Techniques, Article 29 WP Adopted on 10 April 2014, p.20.

[190] CJEU, C-70/10, Scarlet v Sabam, 24 November 2011, para. 51, The case is concerning Scarlet's refusal to install a system for filtering electronic communications which use file-sharing software ('peer-to-peer'), with a view to preventing file sharing which infringes copyright.

[191] CJEU Patrick Breyer v Federal Republic of Germany, Case C-582/14, 19 October 2016, para. 33-37 and 44 The case is concerning the registration and storage of the internet protocol address ('IP addresses) allocated to Mr Breyer when he accessed several internet sites run by German Federal institutions.

tion and replaced when later connections are made, and not 'static' IP addresses, which are consistent and allow continuous identification of the device connected to the network. Yet, the idea that data needed to identify the user of a website are not kept by the online media services provider but are kept by the user's internet service provider, according to the Court does not exclude dynamic IP addresses registered by the online media services provider falling out of the scope of the definition of personal data. However, the decision of the Court was that a

> dynamic IP address registered by an online media services provider when a person accesses a website that the provider makes accessible to the public constitutes personal data within the meaning of that provision, in relation to that provider, where the latter has the legal means which enable it to identify the data subject with additional data which the internet service provider has about that person.[192]

Consequently, the European Court of Justice found that nameless data (IP addresses) that refer to a device is personal data.

Despite the difference between the two abovementioned cases and mHealth apps, the Court decisions are relevant for two reasons. First, it contributes to the discussion whether data generated from the mHealth apps are considered personal data, under the meaning of the Regulations. Indeed, as described, the mHealth apps are collecting personal data, such as device ID, hardware information from the smart device mostly used by a single person, as well as the IP address, among others. Undeniably, one can argue that these are better identifiers in the online world than the most commonly used identifier in the 'real world', family name.[193] Consequently, this clearly indicates that certain identifiers are sufficient to achieve indirect identification of an mHealth app user without significant time and costs.

---

[192] CJEU Patrick Breyer v Federal Republic of Germany, Case C-582/14, 19 October 2016, para. 49.

[193] Article 29 WP, Opinion 4/2007 on the concept of personal data, WP 136, 20 June 2007, page 13.

In addition to these, these apps can have access to the microphone, camera, credit card payments, and browsing history together with the user's combined data including call list, email addresses, SMS messages and contacts from the address book.[194]

2.1. Are data from lifestyle and wellbeing apps personal data?

In line with the previous discussion, further, we will analyse to what extent the data collected from the mHealth apps fall in the scope of the four main building blocks, which according to Article 29 WP[195] constitute the definition of personal data.

(1) 'Any information'

The first building block 'any information' echoes the broader scope of the definition, meaning any information, which not is necessary to be true or proven. First, this information by its *nature* could be either objective (a fact about a certain person) or subjective (opinions or assessments).[196] Second, it can be in any *format*: alphabetical, numerical, graphical, photographic or acoustic, kept on paper, as well as information stored in a computer memory by means of a binary code, or on a videotape.[197] Third, the *content* of the information should contain information concerning the individual's private and family life, but also information about the types of activities undertaken by the individual[198] concerning working relations, social or economic behaviour.

In the context of mHealth apps, this would mean that they are collecting information of either an objective or subjective nature. For example, the information about the user's blood pressure is of an objective nature, whereas drawing a conclusion about his health

---

[194] Privacy in mobile apps - Guidance for app developers; ICO (Information Commissioners Office), December 2013 (page 3) https://ico.org.uk/media/for-organisations/documents/1596/privacy-in-mobile-apps-dp-guidance.pdf.

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

[196] Article 29 Working Party, Opinion 4/2007 on the concept of personal data, adopted on 20th June, WP136, p. 5.

[197] See *Id*., p.7.

[198] See *Id*., p.6.

status if the user is less physically active or has diabetes has more of a subjective nature. Furthermore, these apps collect information concerning the individual's private and family life as well as the types of activities undertaken by the individual. For example, these apps measure the physical activities of the users, such as running, walking or sleeping, to name a few.

(2) 'Relating to'

The second building block, 'relating to', is crucial to precisely identify and distinguish the relations or links that really matter. Mostly, data can be considered to 'relate to' an individual when it is about that individual. In other words, it is data that relates to a person's identity such as name and surname, physical appearance or behaviour. Besides, if such data is used to determine or influence the manner in which that person will be treated or evaluated, this is also considered as 'relating to'.[199] Consequently, data to be consider that 'relate' to an individual, one of three conditions should be present: a 'content' element, a 'purpose' element or a 'result' element.[200]

To clarify, the 'content' element means that data 'relates' to a particular person. The 'Purpose' element occurs when taking into consideration all the circumstances of a case, the data are used or most probably will be used, to evaluate, treat in a certain way or influence the position or behaviour of an individual. The 'Result' element occurs when taking into consideration all the circumstances of the case, the data is used or might be used to have an impact on a certain person's rights and interests. In any case, it is not essential that the possible consequence has an enormous influence. It is enough if the person may be treated in a different way from other persons as a consequence of the processing of the data. These three elements, content (what the data is clearly about), purpose (it will be used in a certain way) and result (it is likely to have an impact on rights and interests), basically must be taken into consideration as alternative conditions, and not as cumulative ones. In other words, that would mean if the content element ex-

---

[199] Article 29 Working Party document No WP 105: 'Working document on data protection issues related to RFID technology', adopted on 19.1.2005, p. 8

[200] Article 29 Working Party, Opinion 4/2007 on the concept of personal data, adopted on 20th June, WP136, p.10

ists, there is no need for the other elements to be present, in order for data to be considered that relates to the individual.

Then, how is this reflected in the mHealth apps situation? First, it is not obvious to determine if the information 'relates' to an individual, due to the fact that the information relates to the smart phone in the first instance, and not the user. However, this smartphone usually belongs to someone, most likely the user of the mHealth app, who can be subject to particular influence. As discussed in the previous chapter, data from mHealth apps in most cases relate to the owner of the smartphone (content element) on which the lifestyle and wellbeing app is installed, allowing indirectly to be identified.

Moreover, this data can be used to treat the user in a certain way (purpose element), for example, to increase the fee for health insurance due to the fact that the user is not enough physically active or is consuming unhealthy food. As a result, treating the user in this way leads to discrimination (result element).

(3) '…identified or identifiable'

The third building block '…identified or identifiable' refers to a natural person that can be considered as identified or identifiable, directly or indirectly, by a particular piece of information called an identifier closely linked to a particular individual, for example, name and surname, an ID number, GPS data, an online identifier or one or more aspects specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the particular individual. The individual is *'identified'* when, within a group of persons, he or she is 'distinguished' or can be singled out from all other members of the group. While, the natural person is *'identifiable'* when, although the person identified is not yet known, it is possible to do so. This, actually, is the threshold condition crucial to decide if the data fall within the scope of the third element.[201]

In order to determine whether an mHealth app user is identifiable, it should be taken into account all the means reasonably likely to be used either by the controller or by another person to identify the user directly or indirectly, for instance, by singling out. However,

---

[201] Article 29 Working Party, Opinion 4/2007 on the concept of personal data, adopted on 20th June, WP136, p. 12.

this requires a more systematic approach. First, to determine whether the means are reasonably likely, all objective factors should be taken into consideration, such as the expenses and time required for identification, as well as the current available technology and technological developments.[202] Second, it should also be taken into consideration the intended purpose, the method used for processing, the benefit estimated by the controller, the interests of the users, as well as the threat coming from company dysfunctions and technical failures.[203]

As already noted, the natural person is *'identifiable'* when, although the person's identity is not known yet, it is possible to reveal it. An app installed on a smart phone is mostly used by and connected with the owner of the device, hence it allows this user to be identified indirectly, in other words, to be 'individualised' or singled out and be treated differently from others. The notion of 'identifiable', as addressed in the Explanatory Report of the Modernised Convention 108,[204] could be done, for instance, by referring to the user or his one or more devices (computer, mobile phone, camera, gaming devices, etc.) an identification number, a pseudonym, biometric or genetic data, location data, an IP address, or other identifier.

(4) 'Natural person'

The fourth building block 'natural person' 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,[205] as defined in Article 6 of the Universal Declaration of Human Rights, according to which 'Everyone has the right to recognition everywhere as a person before the law'. Personal data processed by the mHealth apps at this point of

---

[202] GDPR Recital 26.

[203] Article 29 Working Party, Opinion 4/2007 on the concept of personal data, adopted on 20th June, WP136, p. 15.

[204] Explanatory Report of Modernised Convention 108, para. 17.

[205] Recital 2, GDPR.

time relates solely to identified or identifiable living individuals or natural person.[206] The fact that the General Data Protection Regulation is restricted solely to living natural persons[207] does not mean that legal persons cannot also protect their rights infringed as a result of processing of data. Their protection in the EU is enshrined in Article 8 of the ECHR, 'private life, home and correspondence'.

One of the cases in front of the ECtHR based on Article 8 of the ECHR was *Bernh Larsen Holding v. Norway*. [208] In this case, three Norwegian companies (i.e. 'legal persons') complained about decision of a tax authority that demanded they deliver a copy of all the data held on a computer server they used jointly to the tax auditors. The ECtHR found that imposing such an obligation on the Norwegian companies, indeed, constituted an interference with their rights to respect for 'home' and 'correspondence' under Article 8 of the ECHR, but did not constitute a violation. The decision reflects the intention of the Court to strike a fair balance between the companies' right to respect for 'home' and 'correspondence', specifically, their interest in protecting the privacy of employees,

---

[206] Even though in the EP report is pointed out that 'The current insufficient legal framework on data protection is of great concern due to the (expected massive) flow of data arising from the use of robotics and AI'. See more DRAFT REPORT with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL)). European Parliament, Committee on Legal affairs, 31.05.2016, p.21

[207] It is worth clarifying that pursuant to Recital 27 personal data from deceased persons is out of the scope of the GDPR

[208] ECtHR, Bernh Larsen Holding AS and Others v. Norway, No. 24117/08, 14 March 2013. The facts of the case are: 'The three applicant companies (and two other companies) shared a common server for their respective information technology systems. In March 2004 the regional tax authorities requested one of the applicant companies, Bernh Larsen Holding (B.L.H.), to allow tax auditors to make a copy of all data on the server. While B.L.H. agreed to grant access, it refused to supply a copy of the entire server, arguing that it was owned by the second applicant company (Kver) and was also used for information storage by other companies. When Kver in turn opposed the seizure of the entire server, the tax authorities issued a notice that it too would be audited. The two companies then agreed to hand over a backup tape of the data of the previous months, but immediately lodged a complaint with the central tax authority and requested the speedy return of the tape, which was sealed pending a decision on their complaint. After being informed by Kver that three other companies also used the server and were affected by the seizure, the tax authorities notified those companies that they would also be audited. One of them, Increased Oil Recovery (I.O.R.), subsequently lodged a complaint with the central tax authority. In June 2004 the central tax authority withdrew the notice that an audit of Kver and I.O.R. would be carried out but confirmed that B.L.H. would be audited and was obliged to give the authorities access to the server. That decision was upheld on appeal to the City Court, the High Court and ultimately the Supreme Court.

and on the other hand, the public interest in ensuring efficient inspection for tax assessment purposes.

Briefly, to summarise the findings of this section, and answer the question whether data processed by mHealth apps falls within the scope of personal data, yes, data collected and processed by the mHealth apps fall within the scope of the four main building blocks, which constitute the definition of personal data 'any information', 'relating to', 'an identified or identifiable', a 'natural person' .

2.2. Are data from lifestyle and wellbeing apps health data?

Some personal data processed by mHealth apps are considered a special category of data.[209] The Council Convention No.108 on automatic processing of personal data defined special personal data in Article 6 as:

> *personal data revealing racial origin, political opinions or religious or other beliefs, as well as personal data concerning health or sexual life, may not be processed automatically unless domestic law provides appropriate safeguards. The same shall apply to personal data relating to criminal convictions*'

The modernised version of the Convention, in order to respond to the new technological challenges, added ethical origin, trade-union membership as well as genetic data, and biometric data as sensitive data.[210]

Directive 95/46/EC defines special personal data in Article 8 covering the same categories as the Convention but adds 'ethnic origin', 'philosophical beliefs', 'trade-union membership' to the definition. It is worth noting that interpretation of this definition should be understood as meaning that not only data which by its nature contains sensitive

[209] GDPR, Article 9 (1)

[210] The Council of Europe's Committee of Ministers held in Elsinore, Denmark, adopted on 18 May 2018 the Protocol (CETS No. 223) amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108)

information is covered by this provision, but also data from which sensitive information with regard to an individual can be uncovered.[211]

In the GDPR, personal data that reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation are qualified as special category of personal data and granted special protection.[212]

Regulating this particular category 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 the misuse of other, 'normal' personal data.[213] In this thesis, our research will be focused only on health data as a particular type of special personal data.

As a matter of fact, health data as a special category of data has long been considered to be personal and deserving privacy protection. The Hippocratic oath require doctors to keep patient information confidential: '*What I may see or hear in the course of the treatment or even outside of the treatment in regard to the life of men, which on no account one must spread abroad, I will keep to myself, holding such things shameful to be spoken about.'* [214]

Having in mind their sensitivity, processing of this data is prohibited, pursuant to Article 9 of the GDPR, except in the cases when one of the exceptions applies. The exceptions

---

[211] Article 29 WP, Advice paper on special categories of data ('sensitive data'), 20/04/2011, p.6.

[212] Article 9, Para.1 General Data Protection Regulation.

[213] Article 29 WP, Advice paper on special categories of data ('sensitive data'), 20/04/2011, p.4.

[214] Privacy has been a part of medicine since the 4th century B.C, when the importance to protect medical and health data has been recognized via the Hippocratic oath 'What I may see or hear in the course of the treatment or even outside of the treatment in regard to the life of men, which on no account one must spread abroad, I will keep to myself, holding such things shameful to be spoken about.' - Cross-Cultural perspectives of medical ethics-Robert M. Veatch, The Hippocratic oath: Text, Translation and Interpretation, Chapter 1.

for processing health data as a special category of data will be explained and analysed further in Section 3.2.

Health data as a special category of personal data is defined as data concerning the physical or mental health of a person, as well as the provision of health care services that disclose information about health status. Moreover, Recital 35 provides a comprehensive explanation of what falls within the scope of the definition:

> 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. This includes information about the natural person collected in the course of the registration form, or the provision of, health care services as referred to in Directive 2011/24/EU of the European Parliament and of the Council () to that natural person; a number, symbol or particular assigned to a natural person to uniquely identify the natural person for health purposes; information derived from the testing or examination of a body part or bodily substance, including from genetic data and biological samples; and any information on, for example, a disease, disability, disease risk, medical history, clinical treatment or the physiological or biomedical state of the data subject independent of its source, for example from a physician or other health professional, a hospital, a medical device or an in vitro diagnostic test.

At first sight, it seems that the Recital will straightforwardly solve the question of whether data generated by mHealth apps fall within the scope. In fact, this definition is very broad.[215] It is characterised as being comprehensive but non-exhaustive,[216] and does not specifically address the question of whether and to what extent information from mHealth apps falls within the scope of health data. Therefore, the absence of a specific threshold between health data and non-health data actually complicates the attempts to qualify, regulate, and protect such data.[217]

---

[215] It reflects the technologically neutral character of the Regulation.

[216] 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, p 6.

[217] Malgieri, Gianclaudio and Comandé, Giovanni, Sensitive-By-Distance: Quasi-Health Data in the Algorithmic Era (May 2, 2017). Information, Communication and Technology Law, Issue n. 3, 2017 (Forthcoming). Available at SSRN: https://ssrn.com/abstract=3020628, page 5.

In line with this reasoning personal data generated by mHealth apps, in some situations, fall within the grey area between personal and health data. It is not obvious at first sight whether or not the processing of these data should qualify as the processing of health data.[218] In other words, they are personal data, but it is not always clear if they can be regarded as health data. The language used in the definition is understandable from the regulator's position since it reflects his intention to create a definition which can address the technological challenges.[219] On the other hand, it gives a possibility for Courts to interpret the definition in wide variety of cases. For instance, the case law suggests that the expression 'data concerning health' should be given wider interpretation *'to include information concerning all aspects, both physical and mental, of the health of an individual'*.[220]

Despite the vague definition, capturing the notion of health data collected by mHealth apps is more complex since the apps collect various kinds of data which could be in combination considered as health data. The Article 29 WP,[221] in the advice paper 'Health Data in Apps and Devices',[222] has provided some clarification on this issue. It has concluded that data generated from lifestyle and wellbeing apps is considered to be health data when it is:[223] (a) inherently/clearly medical data, (b) when raw sensor data by itself or in combination with other data can be used to draw

---

[218] Article 29 WP, ANNEX - health data in apps and devices, 2015, p. 3.

[219] Malgieri, Gianclaudio and Comandé, Giovanni, Sensitive-By-Distance: Quasi-Health Data in the Algorithmic Era (May 2, 2017). Information, Communication and Technology Law, Issue n. 3, 2017 (Forthcoming). Available at SSRN: https://ssrn.com/abstract=3020628.

[220] Judgement of the European Court of Justice, Lindqvist Case C-101/01, 6 November 2003, para.50.

[221] The Article 29 Data Protection Working Party was set up under the Directive 95/46/EC (Data Protection Directive)and consist of representatives of the supervisory authorities of each EU country of the EU institutions, bodies and European Commission. It has advisory status and acts independently.

[222] 'ANNEX-health data in apps and devices' of the Article 29 WP http://ec.europa.eu/justice/data-protection/article-29/documentation/otherdocument/files/2015/20150205_letter_art29wp_ec_health_data_after_plenary_annex_en.pdf.

[223] *Id.*, p. 5.

an assumption about the actual health status or health risk of a user, and (c) decisions can be drawn about a person's health status or health risk.

a) Inherently/clearly medical data

The general agreement is that 'medical data or data about the physical or mental health status of a data subject that is generated in a professional, medical context is health data. In particular, it entails data about diagnosis, diseases, disabilities or treatment provided by health services, medical history and clinical treatment. For example, data from an app that measures blood pressure or heart rate is considered health data, regardless of whether testing is performed by medical professionals or by apps freely available on the commercial market and irrespective of whether the app is marketed as medical devices or not. This is in line with the last part of Recital 35, stating that 'any information (…) independent of its source' that reveals past/present or future health conditions is 'health data'.

Yet, health data is a much broader term then just 'medical' data. Some argue that 'what constitutes health is more difficult to define than what constitutes illness'.[224] Thus, the definition has been interpreted that it is not always necessary that data be related with 'ill health' or 'disease risk' in order to be considered as health data. For example, the results from a blood test that is performed to diagnose health, qualify as health data no matter if the outcome of the test is within the health limits or not.

b) Raw sensor data

To decide if the raw data falls within the scope of the definition of health data, one should consider the intended purpose by itself as well in combination with other information. For example, information about user weight without any further information about age or sex does not allow the conclusion to be made about the actual or likely future health status of that person. Yet, that aspect measured over time, especially in combination with age and sex, may be used to determine a significant aspect

[224] A cross-cultural comparison of health status values, D L Patrick, Y Sittampalam, S M Somerville, W B Carter, and M Bergner , Am J Public Health. 1985 December; 75(12): 1402–1407.

of an individual's health, such as the health risks related to obesity or an illness causing a significant loss of weight. [225]

Furthermore, there has to be an obvious relationship between the raw data set and the capacity to determine a health aspect of a person, based on the raw data itself or on the data in combination with data from other sources. For example, if a diet app only counts the calories about the specific foods eaten but does not store this data, it would be unlikely to draw any meaningful conclusions about the health of that person. On contrary, if the data from diet app are combined with data from the sleeping app or activity app, the user's health condition can be assessed, regardless of the fact if the assessment is accurate or inaccurate. In such a case, when data are combined from one or more different apps, it is likely that health statues can be inferred.

c) Health status or health risk conclusions

Information about a person's obesity, blood pressure, hereditary or genetic predisposition, excessive alcohol consumption, tobacco consumption, drug use or any other information is also considered as health data if there is a scientifically proven or commonly perceived risk of possible future disease,[226] no matter whether these conclusions are correct or incorrect, legitimate or illegitimate, or otherwise sufficient or insufficient. As a result, any information that could possibly affect or predict the health status of a person, would be considered as health data. For example, data process from apps used for tracking exercise habits or diet might be considered as health data. This stems from the fact that is possible to draw a conclusion from the correlation between certain lifestyle factors and diseases. More specifically, data from an app that tracks footsteps solely as a way of measuring the user's fitness activities, will be not considered as health data if it is not stored by the app developer in order to create a profile that evaluates the user's physical fitness or health condition, nor combined with other data. On the other hand, if the app is

---

[225] ANNEX-health data in apps and devices' of the Article 29 WP, p.4

[226] 'ANNEX-health data in apps and devices' of the Article 29 WP http://ec.europa.eu/justice/data-protection/article-29/documentation/otherdocument/files/2015/20150205_letter_art29wp_ec_health_data_after_plenary_annex_en.pdf p.2

used to measure or predict health risks (heart attack) and to enable medical follow up, then these data are considered health data.[227]

The abovementioned issue has been also addressed in the Code of Conduct on Privacy for Mobile Health Applications.[228] Although, it does not provide a more detailed clarification of how to capture the notion of health data than the one already explained by the Article 29 WP. The Code provides guidance for app developers on how European data protection legislation should be applied in relation to mHealth apps.[229] In fact, it is a Privacy Impact Assessment (PIA),[230] in the form of questions intended to help app developers determine whether the main requirements of the Code are respected and whether good privacy practices are followed before making the app available.

It is evident that despite the existing law, opinions and clarifications, it is challenging to capture the notion of health data, partly due to the highly technical and complex technology used in the apps, which is also continuously developing and improving. Considering the fact that there is no simple definition of health data, some argue that it should be decided case by case.[231] In view of this, controllers or app developers should be accountable how they legally define the data from the mHealth apps, merely as personal data or as health data. The main reasoning behind is that, in most cases, they possess the crucial technical knowledge necessary to qualify such information as health data or not.[232]

---

[227] European mHealth Initiative, Draft Code of Conduct on privacy for mobile health applications, p.2 - On 7 June 2016, the Code of Conduct has been formally submitted for comments to the Article 29 Data Protection Working Party. Once approved by the Working Party, the Code will be applied in practice: App developers can sign it on a voluntary basis, thereby committing to following its rules.

[228] See *Id.*

[229] *Id.*, p.1.

[230] *Id.*, p.19.

[231] See Opinion 1/ 2015 Mobile Health, 21 May 2015, European Data Protection Supervisor; https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2015/15-05-21_Mhealth_EN.pdf, p.6.

[232] See *Id*,. p.8

The distinction between regular personal data and health data is exceptionally important, as the breaches concerning health data endanger the right to privacy in a much more substantial way. Additionally, infringement of Article 9 of the GDPR, paragraph 1, allows hefty fines[233] for the controller(s) and processor(s) of health data of up to 4 % of the total worldwide annual turnover of the preceding financial year.

3. Exceptions for processing data from lifestyle and wellbeing apps

3.1 Exceptions for processing personal data

Despite the fact that the concept of ‘processing personal data' is very broad, yet that does not mean that every situation that involves processing of personal data is subject to the Regulation. Article 2 of the GDPR provides exemptions for processing personal data, taking into account three key points. The first one is the technical way of processing, meaning, by automated means as well as manually as part of a structured system. The second are activities that fall outside of the scope of EU law and the public interest. The third is the intention of the use, e.g. for purely personal or household activities by a mHealth app user.

a) The technical way of processing

Concerning the first key point, the GDPR applies to personal data if they are solely processed partly or completely by automated means[234] as well as to completely manual processing. Regarding the latter, the personal data needs to be contained or intended to be contained in a filing system. This means that files or sets of files, as well as their cover pages, which are not structured according to specific criteria, do not fall within the scope of this Regulation.[235] Practically, this means that any processing of personal data, for ex-

---

[233] GDPR, Article 83, para.5.

[234] GDPR, Article 2, para.1.

[235] GDPR, Recital 15.

ample, through a laptop, a smart device, or wearable is considered as an automated means. Hence, data processed by mHealth apps is considered as 'carried out by automated means'. This finding is relevant for our further discussion, for the reason that users can exercise the right to data portability. In other words, the right to data portability applies only if data is processed by automated means, it does not cover data processed in paper files.[236]

b) Activities out of the scope of Union Law and public security

The main purpose of the second exemption is to provide a considerable degree of flexibility in order to balance the interests between protection of the data subject's rights and on the other side the legitimate interests of data controllers, third parties and the public security.[237] Therefore the Regulation does not apply to the processing of personal data in the course of (a) an activity which falls outside the scope of Union law,[238] (b) by the Member States when carrying out activities which fall within the scope of Chapter 2 of Title V of the TEU,[239] or (c) by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.[240] These activities are not within the scope of this thesis and will be not further discussed.

c) Household exception

The third exception deserves our attention. Based on this, regulation does not apply to the processing of personal data by a natural person in the course of a purely personal or

---

[236] Article 29 Working Party, Guidelines on the right to data portability, adopted on 13 December 2016, WP242, p.7.

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

[238] GDPR, Article 2, para. 2(a).

[239] GDPR, Article 2, para. 2(b).

[240] GDPR, Article 2, para. 2(d).

household activity,[241] and thus with no connection to a professional or commercial activity.[242] Further, Recital 18 explains that personal or household activities could include, for instance, correspondence and holding of addresses, or social networking and online activity carried out within the context of such activities. One crucial fact in considering if household exception applies or not is the number of people to whom the personal data are made available. If data is spread out to large number of people or as ruled in the *Lindqvist* case, 'made accessible to an indefinite number of people'[243] then the household exception does not apply.

Data processed by the mHealth apps in most cases can be characterised as solely used by the user, with some degree of online activity with a social networking element. The first assumption is that the data fall under the 'household exemption'. But this is not a general rule. To illustrate, if the app user creates and store personal data on their smart device and no personal data are transmitted outside the device, this processing is considered to fall under the purely personal or household exception and GDPR does not apply.[244] Therefore, the user would be exempt from the formal data protection obligations.[245]

On the contrary, when private users are processing personal data through mHealth apps and are widely sharing it on the Internet via a social network or a mailing list, then this processing would not fall within the scope of the household exception. Actually, they may become jointly responsible as controllers of the processed data. The analogy between mHealth apps and household exception can be drawn from the case law. The household exception has been addressed by the CJEU in the case of *Ryneš vs Office for Personal Data Protection.*[246] The main question in the case was 'can the operation of a

---

241 GDPR, Article 2, para. 2(c).

242 GDPR, Recital 18.

243 CJEU, C-101/01, Criminal proceedings against Bodil Lindqvist, 6 November 2003, para. 47.

244 Article 29 WP, Opinion 02/2013 on apps on smart devices, adopted February 2013, p. 9.

245 ANNEX-health data in apps and devices' of the Article 29 WP, 2015, p. 5.

246 Case C-212/13, Mr Ryneš vs Office for Personal Data Protection, judgment of the CJEU of 11.12.2014, paras. 29 and 33.

camera system installed on a family home for the purposes of the protection of the property, health and life of the owners of the home be classified as "the processing considered as a purely personal or household activity" even though such a system also monitors a public space?' The Court's answer has been that, to the extent that video surveillance processing covers, even partially, a public space it cannot be considered as an activity which falls within the purely 'personal or household' exception.

Consequently, if users are processing personal data through mHealth apps and are widely sharing it on the Internet, which in this situation can be regarded as public space, then the household exception does not apply.

Yet, as advised in EDPS Opinion 02/2013, the household exception should be narrowly applied in the mHealth apps context. In a manner that, irrespective of whether the user meets its criteria, entities involved in the design, supply and functioning of the app such as app designers, app stores, and third parties will stay accountable for the processing they carry out in pursuit of their own purposes.[247] In other words, the business model of the mHealth apps indicates that the user's data are systematically transferred to device manufacturers of the operating system and device, application developers, app stores and other third parties who are involved in the processing of the personal data, and who qualify as data controllers.[248] For example, even though the household exemption applies to a user, that does not exclude the app developer from obligations. Specifically, he would be responsible as data controller if he processes the data for his own purposes, and if the app demands access to the contacts in order to provide instant messaging, phone calls, and video calls.[249]

Additionally, the social networking element of the lifestyle and well-being apps is seen as an option to make the data public to an indefinite number of people on social net-

---

[247] European Data Protection Supervisor, Opinion 1/2015 Mobile Health Reconciling technological innovation with data protection, 21 May 2015, page 14.

[248] Article 29 WP, Opinion 02/2013 on apps on smart devices, adopted February 2013, p. 9.

[249] Article 29 WP, Opinion 02/2013 on apps on smart devices, WP 202, Adopted on 27 February 2013, page 9

works. These apps can be automatically configured to publish the data on social networks by the user of the app or developer. Yet, in this case, processing of personal data is beyond the conditions of the household exemption, since data is processed by social networks for distinct purposes which they have determined.[250] For instance, a social network may use information collected by well-being or lifestyle app to profile the user and shows them ads. Therefore, social networks qualify as data controllers in their own right under EU law.

Based on the discussion the 'household exemption' will be of limited application in the context of mHealth apps.[251] Even though in some cases processing performed on the data by the app user might fall within the scope of household activities, for the sake of this thesis, we will assume that household exception does not apply to data processed by the mHealth apps, since, the right to data portability should not apply[252] to data processed in a purely personal or household activity.

3.2 Exceptions for processing health data

As we already explained, the newly adopted GDPR qualifies health data into a special[253] category of data to which a higher level of data protection applies, whereas processing is prohibited unless one of the exceptions applies.[254]

Yet, the Regulation lays down various exceptions for processing the special category of personal data. One of them is the explicit consent of the user. In such a case, the explicit consent is given to the processing of data for one or more specific purposes, under-

---

250 Opinion 8/2014 on the on Recent Developments on the Internet of Things, Article 29 WP, Adopted on 16 September 2014, WP 223, page 12

251 Opinion 8/2014 on the on Recent Developments on the Internet of Things, Article 29 WP, Adopted on 16 September 2014, WP 223, page 13

252 Article 29 Working Party, Guidelines on the right to data portability, adopted on 13 December 2016, WP242 p.5

253 Article 9, para.1, GDPR, 6 April, 2016.

254 *Id.*, para. 2.

standably, only if Union or Member State law provides that this prohibition may not be lifted by the user.[255] This exception is highly significant for this thesis, due to the fact that the user of lifestyle and wellbeing app will be able to exercise their right to data portability only if the processing of personal or health data is based on explicit consent.[256]Another exception is when processing is necessary for exercising particular rights and obligations in the field of employment and social security and social protection law, based on Union or Member State law or a collective agreement on condition that appropriate safeguards for the fundamental rights and the interests of the data subject are respected.[257] Next on the exceptions list is when processing is necessary to protect the vital interests of the user or of another person who is physically or legally unable of giving consent[258] or the processing is carried out in the course of legitimate activities.[259]

The exemption that deserves attention is when processing relates to personal data that the user has made manifestly public.[260] The user mHealth app very often are publishing their personal health data such as steps, calories, physical activities or health parameters on social media or are sharing them with people in their community, therefore are manifestly making public and fall under this exception. The list of exceptions also include processing necessary for: exercise or defence of legal claims or whenever courts are acting in their judicial capacity,[261] reasons of significant public interest, on the basis of Union

---

[255] *Id.*, para. 2(a).

[256] *Id.*, Article 20, Para. 1(a): 'the processing is based on consent pursuant to point (a) of Article 6(1) or point (a) of Article 9(2) or on a contract pursuant to point (b) of Article 6(1)…'.

[257] Article 9, para. 2(b), GDPR.

[258] *Id.*, para. 2(c).

[259] *Id.*, Para. 2(d): 'processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects'

[260] Article 9, para. 2(e) General Data Protection Regulation

[261] *Id.*, para. 2(f).

or Member State law,[262] public interest in the area of public health,[263] archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.[264] The last exception is when processing is necessary for the purposes of preventive or occupational medicine, for the evaluation 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 or Member State law or pursuant to contract with a health professional,[265] when those data are processed by or under the responsibility of a professional subject to the obligation of professional secrecy.[266] To explicate, if the processing of health data is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller then right to data portability does not apply.[267] Data processed by lifestyle and wellbeing apps does not count as a task carried out in public interest. It is worth noting that despite the exceptions, Member States, based on the 'open clauses' can determine additional conditions as well as restrictions regarding the processing of genetic, biometric or health data.[268]

To summarise, mHealth apps fall within the scope of the definition of personal data, and in most cases, they will be considered a special category of data, health data, even if in practice it could be difficult to draw a clear line between them without the necessary

---

[262] *Id.*, para. 2(g): '…which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject'.

[263] *Id.* para. 2(i): '..such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy';

[264] *Id.*, para. 2(j).

[265] *Id.*, para. 2(h).

[266] *Id.*, para. 3.

[267] Article 20, para. 3, GDPR

[268] *Id.*, article 9, para. 4.

technical knowledge. Categorising them as special data means they deserve higher privacy protection, since their misuse could have long-term consequences and could infringe the right to privacy.

Then, what is the relationship between data protection and privacy? The right to privacy and the right to personal data protection are two closely related but different concepts. Hence, in the next section, we will explain the relationship between them.

4. The relationship between data protection and privacy

4.1. The right to data protection

The right to protection of personal data has been recognised as a fundamental human right in the Article 8 of the EU Charter on Fundamental Rights.[269] Considering the fact that is adopted after the Data Protection Directive, one must have in mind that it has embedded the pre-existing data protection law, such as key data protection principles and the need for independent authority to supervise the implementation. Article 16 of the TFEU[270] also recognised the right to data protection as an autonomous right, separate and different from the right to a private life.[271] This article is very important since it places data protection on a different basis. Previously, data protection was based on the

---

[269] OPINION 2/13 OF THE COURT (Full Court), (Opinion pursuant to Article 218(11) TFEU — Draft international agreement — Accession of the European Union to the European Convention for the Protection of Human Rights and Fundamental Freedoms — Compatibility of the draft agreement with the EU and FEU Treaties), 18 December 2014 , para. 34: 'The EU Charter of Human Rights, signed in Nice 2000 and legally binding since 2009, has the principal aim, of reaffirming 'the rights as they result, in particular, from the constitutional traditions and international obligations common to the Member States, the Treaty on European Union, the Community Treaties, the [ECHR], the Social Charters adopted by the Community and by the Council of Europe and the case-law of the [Court of Justice] and of the [ECtHR]'. Article 8 Protection of personal data: '1. Everyone has the right to the protection of personal data concerning him or her; 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified; 3. Compliance with these rules shall be subject to control by an independent authority.'
http://curia.europa.eu/juris/document/document.jsf?docid=160882&doclang=EN.

[270] Article 16 (1)TFEU ' Everyone has the right to the protection of personal data concerning them'.

[271] Article 29 Working Party, Opinion 4/2007 on the concept of personal data, adopted on 20th June, WP136, p. 7.

internal market's legal basis for the free movement of data within the EU. Besides the Charter and the TFEU, Data Protection is also part of the legislation of many countries.[272]

As some argue, positioning the protection of personal data as autonomous right 'has acquired this meaning over the last 30 years through the case law of the ECtHR and in the EU Charter on Human Right'.[273] Nevertheless, not all agree. Germany, for example, has found it difficult to draw the line between the right to data protection and the right to privacy, as the German understanding of the right to data protection is derived from the right to privacy.[274] One can argue that this is not necessarily correct. After all, not every act that involves processing of personal data could fall under the scope of the right to privacy. Apparently, this reasoning is also contrary to the logic of the ECHR. The ECHR does not recognise the right to personal data as a distinct fundamental right. Rather, it is protected under the right to respect for private life in Article 8. Therefore, if the user claims existence of illegal processing of personal data, depending on the context and facts of the particular case,[275] it first has to be determined whether a private interest or a person's private life has been compromised.

After all, the fact that in the Charter the right to data protection is enumerated immediately following the right to privacy in Article 7 demonstrates that it is closely connected

---

[272] The first laws that expressly protected information privacy were passed in Europe in the early 1970s. The West German Land of Hesse passed its Datenschutzgesetz (Data Protection Act) in 1970. Sweden's Data Act of 1973 was the first such legislation at national level. France in 1978 and Germany in 1977. Germany is the first country in the Europe where since 1977 is into force Federal Data Protection Act. http://www.bmi.bund.de/EN/Topics/Society-Constitution/Data-Protection/data-protection_node.html.

[273] The Emergence of Personal Data Protection as a Fundamental Right of the EU, ISSN 2352-1902 ISSN 2352-1910 (electronic), 2014 By Gloria González Fuster, page 92.

[274] *Id.*

[275] Handbook on European data protection law, 2018 edition, CoE: ISBN 978-92-871-9849-5, April 2018, page 37

to privacy[276] or respect for private and family life. The relationship between privacy and data protection had been reflected in Article 1(1) of the Directive 95/46/EC, as well in Recitals 10 and 11, stating that the Member States need to protect fundamental rights and freedoms of people and in particular their right to privacy concerning the processing of personal data.[277] On the contrary, the GDPR in Article 1(2) as its subject matter mentions only the right to data protection.

This issue is also addressed in the case law, particularly by the ECJ, who in a few cases confirmed that right to the protection of personal data is closely connected with the respect of private life expressed in Article 7 of the Charter,[278] but is not absolute;[279] it must be considered in relation to its function in society, as interpreted through the case law of

---

[276] A Typology of Privacy (March 24, 2016) Koops, Bert-Jaap and Newell, Bryce Clayton and Timan, Tjerk and Škorvánek, Ivan and Chokrevski, Tom and Galič, Maša,. University of Pennsylvania Journal of International Law, Forthcoming; Tilburg Law School Research Paper No. 09/2016. Available at SSRN: http://ssrn.com/abstract=2754043 p.46.

[277] 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), Brussels, 25.1.2012 COM(2012) 11 final 2012/0011 (COD), page 7

http://www.europarl.europa.eu/RegData/docs_autres_institutions/commission_europeenne/com/2012/0011/COM_COM(2012)0011_EN.pdf.

[278] Court of Justice of the EU (Grand Chamber), judgment of 9.11.2010, Joined cases C-92/09 and C-93/09. Volker und Markus Schecke GbR (C-92/09) and Hartmut Eifert (C-93/09) v Land Hessen,Judgment, [2010] ECR I-0000.

[279] Data protection is closely linked to respect for private and family life protected by Article 7 of the Charter. This is reflected by Article 1(1) of Directive 95/46/EC which provides that Member States shall protect fundamental rights and freedoms of natural persons and in particular their right to privacy with respect of the processing of personal data. Other potentially affected fundamental rights enshrined in the Charter are the following: freedom of expression (Article 11 of the Charter); freedom to conduct a business (Article 16);the right to property and in particular the protection of intellectual property (Article 17(2)); the prohibition of any discrimination against others on grounds such as race, ethnic origin, genetic features, religion or belief, political opinion or any other opinion, disability or sexual orientation (Article 21); the rights of the child (Article 24); the right to a high level of human health care (Article 35); the right of access to documents (Article 42); the right to an effective remedy and a fair trial (Article 47). See 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), Brussels, 25.1.2012, COM(2012) 11 final, p.8.

the ECtHR and the CJEU.[280] To clarify, the discussion throughout this thesis sometimes will refer to the case law of the ECtHR or CJEU; to avoid further confusion, under case law we mean cases from both Courts. Since, in their case law, the CJEU and the ECtHR often refer to each other's judgments, as part of the constant dialogue between the two courts to seek a harmonious interpretation of data protection rules. This is in line with Article 52 (3) of the EU Charter which states that:

> *rights which correspond to rights guaranteed by the Convention for the Protection of Human Rights and Fundamental Freedoms, the meaning and scope of those rights shall be the same as those laid down by the said Convention.*[281]

One must understand that the concept of private and family life is a wide-ranging one, while the rules on protection of personal data are more specific, they are applicable solely if personal data is processed.[282] For example, some situations are covered by the right to a private life, but not by data protection law. If someone is spying on a neighbour, it might be privacy infringement, but data protection law does not apply for the reason that it does not entail processing of personal data.[283] On the contrary, all processing of personal data falls within the scope of data protection law but does not necessarily mean the existence of a privacy breach. For example, processing of personal data can be considered as infringing the right to freedom of expression or access to documents.

Concerning the issue between privacy and data protection, Bygrave[284] argues that while privacy does occupy a central place in data protection law, it is misleading to characterise data protection solely or essentially concerned with protecting privacy. As some ar-

---

[280] ECJ Joined Cases C-465/00, C-138/01 and C-139/01 2003, Rechnungshof v Österreichischer Rundfunk and Others and Christa Neukomm and Joseph Lauermann v Österreichischer Rundfunk, paragraph 70; Case C-101/01 2003, Criminal proceedings against Bodil Lindqvist, Paragraph 99; Case C-73/07 Tietosuojavaltuutettu v Satakunnan Markkinapörssi Oy and Satamedia Oy 2008, paragraph 52.

[281] European Charter of Human Rights, Article 52 (3).

[282] Article 29 Working Party, Opinion 4/2007 on the concept of personal data, adopted on 20th June, WP136, p. 10.

[283] Improving Privacy Protection in the area of Behavioural Targeting, Frederik Zuiderveen Borgesius, 2014, p. 166.

[284] The place of Privacy in Data Protection law, Lee A.Bygrave, 2001

gue, it is about the reconciliation of the interest of the data subject with the legitimate interest of data controllers in processing personal data.[285]

4.2. The right to privacy

The discussion about the right to privacy, or in Europe termed 'the right to private and family life' will take 1948 as a starting point as when the right to privacy has been recognised in the international human rights law as a fundamental human right.[286] The United Nations, Universal Declaration of Human Rights[287] in Article 12 states:

> *No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation.*

Soon after, the Council of Europe also declared this right. The right to privacy has been, embedded in the Article 8 of the European Convention on Human Rights adopted 1950 in Rome, effective since 1953. It states that:

> *Everyone has the right to respect for his private and family life, his home and his correspondence.*

The right to privacy is also guaranteed in the International Covenant on Civil and Political Rights[288] (1966) and in Article 7 of the EU Charter of Fundamental Rights.[289] In

---

[285] Privacy and Data Protection Issues of Biometric Applications-A Comparative Legal Analysis, Kindt, Els J. 2013

[286] The right to privacy as some scholars argue, existed long before it was recognised as a fundamental right. The European approach of privacy protects dignity as aspect of privacy, whereas American approach protects liberty as aspect of privacy, especially liberty against the state. This is result of much older differences over basic legal values, rooted in much larger and much older differences in social and political traditions. See more The Two Western Cultures of Privacy: Dignity versus Liberty, 2014 James Q. Whitman, Yale Law School.

[287] The Universal Declaration of Human Rights (UDHR) is a milestone document in the history of human rights. Drafted by representatives with different legal and cultural backgrounds from all regions of the world, the Declaration was proclaimed by the United Nations General Assembly in Paris on 10 December 1948 General Assembly resolution 217 A as a common standard of achievements for all peoples and all nations. It sets out, for the first time, fundamental human rights to be universally protected. http://www.un.org/en/universal-declaration-human-rights/.

[288] The ICCPR is an international treaty that commits its 169 parties to respecting and ensuring the exercise of individuals' civil rights, including privacy. Article 17 1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and

particular, these provisions have established that the centre of the privacy protection in Europe is private life and its three spheres: home, family and correspondence. As a matter of fact, private life and its three spheres are actually associated with three types of privacy protection.[290] These are:

1. Physical Privacy – entails protection of people's physical bodies against invasive procedures (drug testing genetic testing) and setting limits on intrusion into the home and other physical environments.
2. Relational Privacy – protects the security and privacy of communication (email, phones, direct communication) and privacy of the relationships (personal or intimate)
3. Informational Privacy – is the protection of private information, which involves rules regarding the collection, storing and processing of personal data. As Clarke has pointed out it is the interest of the individual to have control or at least significant influence over the handling of data about them; in other words, 'interest in controlling information about oneself reflects concerns about the exercise of power by others'.[291]

'Privacy', as it is defined in these legal instruments, is considered to be vague. However, this disadvantage is beneficial in the case law. It gives the Court the possibility of applying the right to privacy to a broad range of real-life situations. It presents a living instru-

---

reputation; 2. Everyone has the right to the protection of the law against such interference or attacks http://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx

289 Article 7 Respect for private and family life 'Everyone has the right to respect for his or her private and family life, home and communications.' The Charter of Fundamental Rights of the EU brings together in a single document the fundamental rights protected in the EU. The Charter contains rights and freedoms under six titles: Dignity, Freedoms, Equality, Solidarity, Citizens' Rights, and Justice. Proclaimed in 2000, the Charter has become legally binding on the EU with the entry into force of the Treaty of Lisbon, in December 2009.

290 'Code' and Privacy or How Technology is Slowly Eroding Privacy – R. Leenes & Bert-Jaap Koops.

291 Beyond the OECD Guidelines: Privacy Protection for the 21st Century, Roger Clarke, 2000, http://www.rogerclarke.com/DV/PP21C.html

ment that must be interpreted in the light of present-day conditions,[292]specifically, the challenges that arise from the use of new technology, for instance, mHealth apps. The opinion of the ECtHR is that 'does not consider it possible or necessary to attempt an exhaustive definition of the notion of private life'.[293]

Issues about the use of mHealth apps and the right to privacy have not been challenged in front of the Courts, specifically, whether health data from mHealth apps fall within the scope of private life. Anyway, analogies can be drawn from the existing case law. There are cases which confirm that health data is deemed as part of the right to privacy. For instance, the ECtHR has specified that processing of information relating to an individual's private life falls within the scope of Article 8, para. 1, thus, health data relating to an individual undoubtedly belongs to his or her private life.[294] It further, confirmed that:

> *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 as guaranteed by Article 8 of the Convention. Respecting the confidentiality of health data is a vital principle in the legal systems of all the Contracting Parties to the Convention.[295]*

This emphasises that confidentiality of health data is crucial not only for a patients' privacy but also to preserve their confidence in the medical profession and in the health services in general. [296]

The CJEU has also addressed the issue of health data in the *Lindqvist* case,[297] confirming that 'the fact that an individual has injured her foot and is on half-time on medical

---

[292] ECHR, CASE OF TYRER v. THE UNITED KINGDOM, Application no. 5856/72,25 April 1978 para. 31.

[293] ECHR, CASE OF NIEMIETZ v. GERMANY, Application no. 13710/88,16 December 1992, para. 29.

[294] European Court of Human Rights, I. v. Finland - 20511/03, Judgment 17.7.2008, https://hudoc.echr.coe.int/eng#{%22appno%22:[%2220511/03%22],%22itemid%22:[%22001-87510%22]}.

[295] European Court of Human Rights, I. v. Finland - 20511/03, Judgment 17.7.2008, para. 38, https://hudoc.echr.coe.int/eng#{%22appno%22:[%2220511/03%22],%22itemid%22:[%22001-87510%22]}.

[296] European Court of Human Rights, I. v. Finland - 20511/03, Judgment 17.7.2008, para. 38, https://hudoc.echr.coe.int/eng#{%22appno%22:[%2220511/03%22],%22itemid%22:[%22001-87510%22]}

grounds constitutes personal data concerning health', whose processing must be balanced between freedom of movement of personal data and the protection of private life.[298]

The answer to the question of what is the relationship between right to privacy and right to data protection can be summarised by two points. First, throughout the years, data protection law has emerged as an instrument to respond to the latest information and communication technology developments in society that have presented new risks to the right to respect for private life. This development has shifted the focus of the privacy legislation from family, home, reputation and state surveillance towards protection of personal information, something that UDHR and the ECHR could not address for the reason that they recognise only a right to privacy. In response to protect the collection and use of personal information, a new concept of privacy emerged, known in some jurisdictions as 'informational privacy' and in others as the 'right to informational self-determination'.

Second, these two rights are closely related but have a different formulation and scope. They are related because both attempt to secure a personal sphere in which mHealth app users can freely develop their behaviour, body, emotions and their opinions. The difference is that the right to respect for private life consists of the general prohibition on interference, except in certain cases. While the right to personal data protection as a modern right [299] is protected by a system of checks and balances to protect individuals whenever their personal data are processed.

This section thus presents that in the context of mHealth apps, it is difficult to draw a clear line between right to privacy and right to data protection, since each processing of personal data by mHealth apps can potentially infringe user's privacy. As a result,

---

[297] CJEU, C-101/01, Criminal proceedings against Bodil Lindqvist, 6 November 2003, para. 51.

[298] CJEU, C-101/01, Criminal proceedings against Bodil Lindqvist, 6 November 2003, court ruling no. 6.

[299] Opinion on the Advocate General Sharpston described the case as involving two separate rights: the 'classic' right to the protection of privacy and a more 'modern' right, the right to data protection. See CJEU, Joined cases C-92/09 and C-93/02, Volker und Markus Schecke GbR v. Land Hessen, Opinion of Advocate General Sharpston, 17 June 2010, para. 71.

strengthening users control over their personal data could lead to better privacy protection.

4.3. Privacy as a concept

In the previous section, we discussed the relationship between data protection law and the right to privacy. This section will try to define privacy for the purpose of this thesis, since data collected from the mHealth apps tackle different aspects of the user life that are deemed private.

Privacy as a concept is very elusive and is difficult to define even though has been explored in many disciplines, including philosophy, economics and social science.[300] Philosophical approaches to privacy attempt to elucidate what is privacy and whether it is a right or a good in itself. These questions are tackled from a libertarian/individualistic and communitarian approach to liberal, republican and feminist theoretical approaches.[301] The economic approaches to privacy, attempt to explicate privacy in economic terms as a value, whereas information is needed for effective markets and as a piece of property, while sociological approaches to privacy elucidate how collected personal information has influenced the relationship between individuals, groups, and institutions within society. Regardless of the variety of legitimate theoretical approaches none of them captures or can fully capture privacy's various nuances.

Part of the problem, as Moore argues, is that 'privacy has been used to denote a wide number of interests including, personal information control, reproductive autonomy, access to places and bodies, secrecy, and personal development'.[302] In line with Moore's argument, Solove has pointed out that 'the problem is that discussion is often not well ar-

---

[300] Engaging Privacy and Information Technology in the Digital Age-James Waldo, Herbert S. Lin, and Lynette I. Millett, eds., 2007.

[301] A Typology of Privacy (March 24, 2016) Koops, Bert-Jaap and Newell, Bryce Clayton and Timan, Tjerk and Škorvánek, Ivan and Chokrevski, Tom and Galič, Maša,. University of Pennsylvania Journal of International Law, Forthcoming; Tilburg Law School Research Paper No. 09/2016. Available at SSRN: http://ssrn.com/abstract=2754043.

[302] Moore, Adam D., Privacy (2007). Library Hi Tech, Vol. 25, pp. 58-78, 2007 . Available at SSRN: http://ssrn.com/abstract=1980871 (page 1)

ticulated, and as a result, we frequently do not have a compelling account what is at stake when privacy is threatened and what precisely the law must do to solve this problem'.[303] In other words, the problem is that concepts (definitions) of privacy are centred on different aspects of life that are deemed private, such as: [304]

- The right to be let alone – which views privacy as a type of immunity or seclusion.[305] The emergence of the 'Instantaneous photographs and newspaper enterprise'[306] and their possibility to publish information relating to private and domestic life, were the main reason for future Supreme Court Justice Louis Brandeis and Boston attorney Samuel Warren to published the ground-breaking article 'The Right to Privacy'[307] in 1890. They argued that privacy was an emerging right that needed to be recognised. 'Recent inventions and business methods call attention to the next step which must be taken for the protection of the person, and for securing to the individual what Judge Cooley calls the right 'to be let alone'.[308] Instantaneous photographs and newspaper enterprises have invaded the sacred precincts of private and domestic life, and numerous mechanical devices threaten to make good the prediction that 'what is whispered in the closet shall be proclaimed from the house-tops.'[309] They defined the privacy as 'the right to be let alone',[310] based upon the principle of 'inviolate personality'.

---

303 Solove, Daniel J., Conceptualizing Privacy. California Law Review, Vol. 90, p. 1090, 2002. Available at SSRN: http://ssrn.com/abstract=313103 ;

304 See *id*.

305 Samuel D. Warren & Louis D. Brandeis, The Right to Privacy, Harvard Law Review, V. IV, No. 5, December 1890

306 *Id.*

307 *Id.*

308 Samuel D. Warren & Louis D. Brandeis, The Right to Privacy, Harvard Law Review, V. IV, No. 5, December 1890

309 *Id.*

310 This phrase was previously coined by the Judge Thomas Cooley, Solove, Daniel J., Conceptualizing Privacy. California Law Review, Vol. 90, p. 1087, 2002. Available at SSRN: http://ssrn.com/abstract=313103.

However, this definition of privacy is too broad. It does not provide maters in which people should be let alone. As Anita Allen[311] explains, privacy, defined as such might be violated by any form of offensive or harmful behaviour directed at another person.

- Limited access to the self – This views privacy as the individual desire for concealment and for being apart from other or as withdrawal from other individuals. Ruth Gavison[312] argues that privacy as limited access 'is related to our concerns over our accessibility to others: the extent to which we are known to others, the extent to which others have physical access to us, and the extent to which we are subject of others attention'. Moreover, she explains that limited access consists of secrecy, anonymity and solitude.[313] Yet her attempt to define privacy is characterised as too narrow since it excludes from the definition harassment and insulting, decisions regarding one's body (abortion), health, sexual conduct, unsolicited mail and unwanted phone calls and family life.[314]
- Secrecy – This views privacy as the secrecy of certain matters, whereas privacy is violated by the public disclosure of previously concealed information. For example, Posner defines privacy as 'an individual right to conceal discreditable facts about himself' more precisely as 'concealing true but harmful facts about oneself for one's own gain'. Still, some things that people do such as buying products or reading books are not associated with secret but nonetheless are viewed as a private matter. Therefore, this definition same as the previous one is seen as too narrow.
- Personhood – Here, privacy is seen as a form of protecting personhood, and its three aspects of self: individuality, dignity and autonomy. The term personhood was coined by Paul Freund and refers to 'those attributes of an individual which are irreducible in is selfhood'. This concept is criticised by Gavison, as she

311 Anita L. Allen, Uneasy Access: Privacy for Women in a Free Society (1988).

312 Gavison, Ruth E., Privacy and the Limits of Law (May 16, 2012). The Yale Law Journal, Vol. 89, No. 3 (Jan., 1980), pp. 423 Available at SSRN: http://ssrn.com/abstract=2060957.

313 *Id.*, p. 433

314 *Id.*, p. 436

pointed out 'there are ways to offend dignity and personality without violating the privacy'[315]

- Intimacy – Privacy is understood as a form of intimacy whereas the desired levels of intimacy for each of our varied relationships can be maintained. This concept view privacy as some form of limited access or control that locates the value of privacy in the development of personal relationships. In other words, people establish relations with diverse degrees of closeness and self-revelation, so the value of privacy is to preserve the desired level of intimacy for each of these various relations. Nevertheless, the same as the previous concepts, this one is criticised on the basis that privacy cannot be narrowed down only to one aspect, for the fact that, as DeCew pointed out, financial information is considered as private but are not intimate.
- Control over personal information – Privacy is seen as control over personal information. One of the representatives of this concept is Westin. He defines privacy as 'the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others.' This concept fails to define what is meant by 'control' over information. Still, 'control' is frequently understood as a form of ownership in information. As above, this concept is seen as problematic, first, due to the unique nature of the information, that once transmitted and known by others, cannot be eradicated and is easily transferred to others. Second, it fails to define over what type of information individuals should have control. However, these two problematical theoretical issues will be further discussed through the lens of GDPR, which has addressed these two issues. Therefore Chapter 5 will discuss the new right to data portability, as a possibility or maybe an illusion, allowing users to transfer their data to other controllers and as a tool to maintain control over their personal information.

To conclude, each of the mentioned definitions of privacy emphasises various aspects of life that are deemed private and worth protecting, and more or less are relevant for the

---

[315] *Id.* p.438

users of the lifestyle and well-being apps. The problem is that they are concentrated only to a single aspect of the private life, and do not comprise a complete conception of privacy. Only control over personal information entails (protects) all aspects of privacy. As we discussed in the previous chapter, the functioning of lifestyle and well-being apps is based on the processing of personal information. Therefore, if users have control over their personal information generated by the lifestyle and wellbeing apps, they can protect the spread of their information and will be able to guard all aspects of their privacy.

4.3.1. Privacy as control

Subsequently, despite the fact that privacy can be defined and explained in various ways, for the sake of this chapter I will adopt the one that understands privacy as instrumental value[316] and 'privacy as control'. Modern privacy theorists tend to analyse the notion of privacy in terms of controlling the flow of personal information and have coined the phrase 'informational privacy' to express this new concept.

Privacy as control is defined as such by many scholars. For example, Charles Fried[317] believes that privacy is 'not simply an absence of information about a person in the minds of others, rather it is the control that a person has over information about themselves'. Yet, this view is to some extent incomplete, for the reason that privacy can be interpreted as the control that a person has over information about themselves that they wish to keep from others. Moor, on the other hand, has proposed a restricted access view of privacy 'as a complex of situations in which information is authorised to flow to specific people, at specific times'.[318]

---

316 It is valued as a means for achieving certain other ends that are valuable. Contrary to the intrinsic value 'privacy is valuable in itself locate the source of value in a form of respect that must be provided to all rational beings'. Solove, Daniel J., Conceptualizing Privacy. California Law Review, Vol. 90, p. 1145, 2002. Available at SSRN: http://ssrn.com/abstract=313103.

317 Charles Fried, 'Privacy [a moral analysis],' in Philosophical Dimensions of Privacy: An Anthology. New York: Cambridge University Press, 1968, pp. 333–345.

318 J.H. Moor, 'Towards a theory of privacy in the information age,' ACM SIGCAS Computers and Society vol. 27, pp. 27–32, 1997.

Alan Westin is a predominant representative of this concept and our analysis will be built upon his definition of privacy. He defined privacy in terms of control stating that 'Privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others.' In order to incorporate the specific characteristics of mHealth apps, we propose an adapted version of the definition of privacy as control:

> Privacy of the users of mHealth apps is the guarantee that they maintain control when, how, to whom and to what extent information about their personal health data is communicated.

This includes the protection of data that can be inferred from sensors, added or typed in by the users, generated by the device or OS, as well as from the interaction with other users of mHealth apps. This definition implies that users continuously need to have control over data shared with the mHealth apps as well as to third parties. In other words, to have full control, when, how, to whom and to what extent the data they provided, will be transferred to other mHealth apps. The aim of the user's control is to be actively involved in pursuing the protection of their privacy and decide for themselves if they prefer to be in one or more of various 'privacy states':

- Solitude – or freedom from observation, 'the inner dialogue with mind and conscience'. According to Westin, solitude is the most complete state of privacy an individual can achieve.
- Intimacy – or closeness among a small group of people. This refers not only to the intimate relations between lovers or spouses, but also to family, friends, and work colleagues.
- Anonymity – freedom from being identified in public settings. It is a state were the individual is in public places but still seeks and finds freedom from identification and surveillance.'
- Reserve – the freedom to withdraw from communication according to Westin, expresses the individual's choice to withhold or disclose information - a 'dynamic aspect of privacy in daily interpersonal relations.'

These four states, lead to four functions of privacy, which should allow users of mHealth apps to maintain:

- Personal autonomy or the desire to avoid being manipulated, dominated, or exposed by others;
- Emotional release or the release of tensions under social restrictions like role demands, emotional states or minor deviances;
- Self-evaluation or extracting meaning from personal experiences and exerting individuality on events;
- Limited communication or setting interpersonal boundaries and protected communication that allows sharing personal information with trusted others.

Despite the fact that users been actively involved in pursuing the protection of their privacy, this ideally should be supported by applying privacy techniques, embedding them in the design and functioning of the mHealth apps. After all, taking into account the users' perspective, one might conclude, that they are often unaware of the technical details of the underlying design, resulting in an underestimation of the risks related to their privacy.[319] Therefore the mHealth app, and the multi-structured ecosystem necessary for its functioning is responsible for user's privacy protection.

Privacy as control is also recognised in legal practice, for example as 'right to informational self-determination' in the famous *Census* case from 1983. The background of this ground-breaking decision was a census planned for 1983, to include the entire German population and to be conducted by electronic data processing. Yet, the idea was not very well accepted and resulted in more than 1,600 complaints filed at the Federal Constitutional Court against the census law. While the law had been specifically approved by the German parliament, the final outcome of this case, in December 1983, was that the Ger-

[319] Delphine Christin, Andreas Reinhardt, Salil S. Kanhere, Matthias Hollick: A Survey on Privacy in Mobile Participatory Sensing Applications. In: Elsevier Journal of Systems and Software, vol. 84, no. 11, p. 1928–1946, November 2011. Page 8.

man Federal Constitutional Court declared certain provisions of the Census Act to be unconstitutional.[320] German Constitutional Court stated that:

> A social and legal order in which the citizen can no longer know who knows what when about him and in which situation, is incompatible with the right to informational self-determination. A person who wonders whether unusual behaviour is noted each time and thereafter always kept on record, used or disseminated, will try not to come to attention in this way. A person who assumes, for instance, that participation in a meeting or citizen initiative is officially recorded, and may create risks for him, may well decide not to use the relevant fundamental rights ([as guaranteed in] Articles 8 and 9 of the Constitution). This would not only limit the possibilities for personal development of the individual, but also the common good because self-determination is an essential prerequisite for a free and democratic society that is based on the capacity and solidarity of its citizens.[321]

5. Conclusion

This chapter discusses the concept of personal data as introduced in the EU data protection law, as well as the relationship between the right to privacy and the right to data protection.

The legal historical analyses of the concept of personal data reveal that throughout the years the concept has been changing parallel with technological developments in society. The broad notion of this concept allows accommodating a wide variety of challenges within its shelter. One of them is mHealth apps. Data collected and processed by the mHealth apps fall in the scope of the four main building blocks of EU data protection law, which constitute the definition of personal data as 'any information', 'relating to', 'an identified or identifiable', 'natural person'. To illustrate, mHealth apps are installed on smart devices, which in most cases are associated with a user of the phone, meaning it 'relates to' a 'natural person'. Second, they typically have direct access to many different

---

[320] The Privacy, Data Protection and Cybersecurity Law Review - Germany, The Law Reviews Edition 4, Nikola Werry, Benjamin Kirschbaum, Jens-Marwin Koch, published December 2017.

[321] Comparative Study on Different Approaches to new Privacy Challenge's in Particular in the light of the technological developments - January, 2010 European Commission, DG Justice, Freedom and Security. http://ec.europa.eu/justice/policies/privacy/docs/studies/new_privacy_challenges/final_report_en.pdf.

sensors, data provided by the user or uniquely generated data by the device or OS, meaning there is a possibility a user to be directly or indirectly ‘identified’ or is ‘identifiable’.

Data protection law distinguishes between personal data and a special category of personal data. Health data falls within this special category of personal data, defined as data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about user health status. By its nature information collected from the mHealth apps in most cases falls within the special category of data, or health data. Having in mind the way these apps function, it is possible based on the raw sensor data used in itself or in combination with other data to draw a conclusion about the actual health status or health risks facing a user. On the other hand, if seemingly innocuous raw data is tracked over a longer period of time, it might also reveal the health status of the user.

Anyway, it is challenging to capture the notion of health data. This is part due to the highly technical and complex technology used in the apps, which is continuously developing and improving. Considering the fact that there is no simple definition of health data, some argue that whether some data are health-related should be decided case by case. In view of this, controllers or app developers should be accountable how they legally define the data from the mHealth apps, as merely personal data or as health data. The main reasoning behind is that, in most cases, they possess the crucial technical knowledge necessary to qualify such information as health data or not.

Despite the fact that the concept of ‘processing personal data' is very broad, yet that does not mean that every situation that involves ' processing of personal data' is subject to the EU Regulations. Article 2 of the GDPR provides the exemptions for processing personal data, taking into account three key points: (a) technical way of processing (by automated means, not in manual non-structured form), (b) activities that fall outside of the scope of Union law and the public interest, and (c) for purely personal or household activities by a natural person. The latter, the ‘household exemption’, will be of limited application in the context of mHealth apps. Even though in some cases processing performed on the data by the app user him or herself might fall within the scope of household activities, for the sake of this thesis, we will assume that household exception does not apply to da-

ta processed by the mHealth apps. For the reason that the right to data portability does not apply to data processed in purely personal or household activity.

Data protection law and the right to privacy are closely related but are two different rights. They attempt to protect the same values but have a different scope and form. In the context of mHealth apps, it is difficult to draw a clear line between right to privacy and the right to data protection, since each instance or type of processing of personal data by mHealth apps can potentially infringe a user's privacy. Indeed, it tackles different aspects of the user's life that are deemed private. For the purpose of this thesis, we define privacy as control, i.e. *privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others*. As a result, strengthening users' control over their personal data is an important tool that could lead to a better privacy protection. In fact, that is the aim of the right to data portability introduced in the GDPR.

In the next Chapter, the right to data portability as a tool for strengthening control over data generated from mHealth apps will be discussed based on the outline and elaboration on the choices we made.

CHAPTER 4: RIGHT TO DATA PORTABILITY AND mHEALTH APPS

1. Introduction

This chapter will discuss the right to data portability (hereafter RDP) in the context of mHealth apps. Right to data portability is one of the data subject rights enshrined in the GDPR such as: a) Right of access by the data subject[322] b) Right to rectification[323] c) Right to erasure ('right to be forgotten')[324] d) Right to restriction of processing[325] e) Right to object[326] and f) Automated individual decision-making, including profiling.[327] Nonetheless in the scope of this thesis falls only the RDP, as newly introduced right.

The RDP was introduced by the Commission in Article 20 of the General Data Protection Regulation (hereafter GDPR) as an instrument to restore the trust in online services and to give users more control over their personal data held by service providers.[328] As written, it should strengthen user control over personal data by empowering data subjects 'to receive data they have provided to a controller, in a structured, commonly used and machine-readable format and to transmit those data to another controller without hindrance'. In line with this reasoning and for the purpose of this thesis, control over personal data is seen as an instrument that empowers users to decide when, how and to

---

[322] GDPR, Article 15

[323] GDPR, Article 16

[324] GDPR, Article 17

[325] GDPR, Article 18

[326] GDPR, Article 21

[327] GDPR, Article 22

[328] Commission staff working paper- Impact Assessment Accompanying the document 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) and Directive of the European Parliament and of the Council on the prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data SEC (2012) 72 final, page 43.

whom they will transfer their personal data. This way they can prevent themselves from being locked-in on a particular mHealth app, and be able to simply transfer their data to a better, cheaper or more privacy-friendly app. The aim of this chapter is to examine to what extent RDP will actually give app users control over their data, when confronted with the current legal interpretation of Article 20.

This chapter will be organised in the following order: Section 1 will address the purposes of this right, first, as a right that should give user control over their data, and second, as a competitive element in the digital economy; Section 2 will outline the legislative history of this right from the initial idea to the final text; Section 3 will clarify if and to what extent this right applies to users of lifestyle and well-being apps taking into account its legal and technical limitations; and Section 4 will provide conclusions.

2. Right to data portability

Portability currently seems like a hot topic in the EU. Beside the introduction of this new right in the GDPR, the same idea about portability can be found in a few other EU Directives as well as in the legislation of some Member States.[329] Article 30 (as well as Recitals 40, 41 and 42) of the Universal Service Directive 2002/22/EC[330] discuss 'phone number portability' in the telecommunication sector. Portability is further mentioned in Recital 31[331] of the Directive 2002/21/EC on a common regulatory framework for electronic communications networks and services (or Framework Directive):[332]

---

329 France in October 2016 adopted legislative act on data retrial and data portability, which entered into force in May 2018. Arts. L-224-42-1 to L.224-42-4. It obliges online public communication service to allow consumer a free recovery of online data posted by the consumer, according to Article 20 (right to data portability) in the GDPR https://www.legifrance.gouv.fr/affichTexteArticle.do;jsessionid=D05F7021587B4D04A18C687F70ABEE01.tplgfr42s_2?cidTexte=JORFTEXT000033202746&idArticle=LEGIARTI000033205186&dateTexte=20180525&categorieLien=id#LEGIARTI000033205186.

330 Directive 2002/22/EC of the European Parliament and of the Council of 7 March 2002 on universal service and users' rights relating to electronic communications networks and services (Universal Service Directive).

331 Recital 31: *'…Open APIs facilitate interoperability, i.e. the portability of interactive content between delivery mechanisms, and full functionality of this content on enhanced digital television equipment…'* Di-

> *Open APIs facilitate interoperability, i.e. the portability of interactive content between delivery mechanisms, and full functionality of this content on enhanced digital television equipment.*

Payment Service Directive 2[333] in Articles 66 and 67 indirectly mention portability as a possibility for third parties to access customers account information to provide payment initiation or account information services, with the previously given consent by the account holder. The proposed Directive on certain aspects concerning contracts for the supply of digital content[334](hereafter the DCD proposal) also introduced portability. Yet, there are three major differences between the right to data portability introduced in the GDPR and the right arising from the DCD proposal. The first one is that the DCD proposal applies only after the termination of a business to consumer contract for the supply of digital content[335] and the second one is that the right to retrieve data is not limited to personal data but extends to all kinds of digital content uploaded or created by the consumer.[336] In the case of processing personal data, the implementation and application of the GDPR should be made in full compliance with its legal framework.[337] The third dif-

---

rective 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive).

[332] Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive).

[333] Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC (Text with EEA relevance)

[334] Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on certain aspects concerning contracts for the supply of digital contentCOM/2015/0634 final - 2015/0287 (COD) http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52015PC0634

[335] Article 13, Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on certain aspects concerning contracts for the supply of digital content COM/2015/0634 final - 2015/0287 (COD)

[336] Article 13, parg 2 (c), Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on certain aspects concerning contracts for the supply of digital content COM/2015/0634 final - 2015/0287 (COD)

[337] Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on certain aspects concerning contracts for the supply of digital contentCOM/2015/0634 final - 2015/0287 (COD) Recital 22 http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52015PC0634

ference is that according to the DCD proposal, companies are not encouraged to develop interoperable format as in the right to data portability. As the Directive stated they should

> make use of standards, open technical specifications, good practices and codes of conduct, including in relation to the commonly used data format for retrieving the content generated by the user or any other content provided by the consumer, whether established at the international level, the European level or at the level of a specific industry sector.[338]

Last is the Regulation on the free flow of non-personal data in the EU,[339] which in Article 6 introduced the need for service providers and professional users to develop and implement codes of conduct detailing the information on data porting conditions, pointing out technical and operational requirements that providers should make available to their professional users in a sufficiently detailed, clear and transparent manner before contract is concluded.

One may argue that 'Some synergies and even benefits to individuals may emerge between the different types of portability if they are provided in a combined approach',[340] yet as the Article 29 WP has stated, such analogies should be treated carefully. Further, the current situation might be confusing for apps (market players), in figuring out what exactly fall within the scope of portability under the GDPR and the other Directives.

2.1 Right to data portability as control over data

Before we dive into discussion what entails data portability as introduced in GDPR, we need first to clarify why data portability, alongside the other Directives was introduced in

---

[338] Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on certain aspects concerning contracts for the supply of digital contentCOM/2015/0634 final - 2015/0287 (COD) Recital 28, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52015PC0634.

[339] Proposal for a Regulation of the European Parliament and of the Council on a framework for the free flow of non-personal data in the European Union (COM(2017)495), Brussels, 13.9.2017.

[340] 'Guidelines on the right to data portability' by Article 29 Working Party, Adopted on 5 April 2017, 16/EN WP 242 rev.01, p. 4.

the Data Protection Law. Back in 2012, the European Commission in order to respond to the latest technological developments as well as to future challenges, proposed reform of the 1995 Data Protection Directive.[341] The reform was felt to be necessary to increase the effectiveness of the fundamental rights to data protection. On the contrary, free flow of personal data throughout the member States of the EU[342] could be prevented. For instance, consumers faced with uncertainty regarding their protection would hesitate to buy online and adopt new services. In the end, the overall result could slow down the development of innovative uses of new technologies in the EU.[343]

Hence, the Commission proposed general data protection regulations.[344] In fact, data protection plays an important role in building trust in the online environment, which could in fact boost the European digital economy. The proposed GDPR announced many changes and novelties, such as the enrichment of the package of data subject rights, by strengthening and detailing existing ones and introducing new ones. One of the newly introduced rights by which it sought to build trust in online services and restore the control over personal data was the right to data portability.[345] It has been identified, that due to the latest technological developments, users are of the opinion that they do not have control over the personal data they have provided. Indeed, based on the Eurobarometer survey from 2015 (Figure 3), more than eight out of ten respondents felt that they did not have complete control over their personal data, meaning, nearly a third (31%) felt that

---

[341] 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.

[342] See Recital (9), GDPR.

[343] 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), Brussels, 25.1.2012 COM(2012) 11 final, page 1.

[344] 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.

[345] Graef, Inge and Verschakelen, Jeroen and Valcke, Peggy, Putting the Right to Data Portability into a Competition Law Perspective (2013). Law: The Journal of the Higher School of Economics, Annual Review, 2013, pp. 53-63. Available at SSRN: https://ssrn.com/abstract=2416537.

they have no control at all over their personal information online, half (50%) answered that they had partial control, and just 15% of people felt they had complete control.[346]

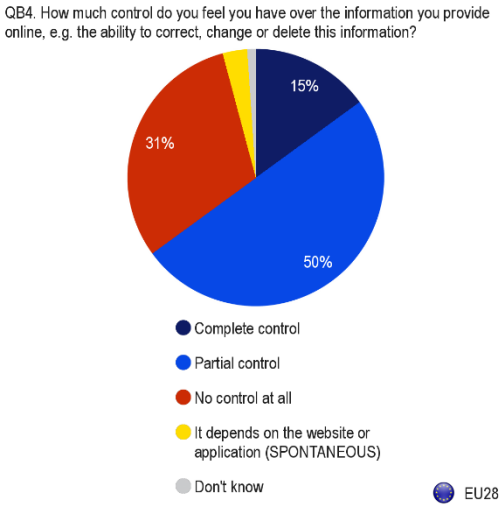

Figure 3. Eurobarometer Survey of Attitudes toward data privacy. Source: Special Eurobarometer 431, Data Protection Report, Publication: June 2015

In truth, these results are unacceptable considering the time and personal data users invest in mHealth apps and other online services.

Consequently, to respond to the current situation, the new right to data portability has two purposes, as control and as a competitive element. The first one is to strengthen users control over their own data,[347] allowing them to obtain a copy of the data, and to transfer the data from one controller to other. First, there is a practical reasoning behind the RDP. As commission stated, '…with the use of new technologies, the amount of personal data collected, becomes an obstacle for changing services, even if better,

---

[346] Data Protection Report, Special Eurobarometer 431, Fieldwork: March 2015, Publication: June 2015. This survey has been requested by the European Commission, Directorate-General for Justice and Consumers and coordinated by the Directorate-General for Communication, page 9, http://ec.europa.eu/commfrontoffice/publicopinion/archives/ebs/ebs_431_en.pdf.

[347] 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), Brussels, 25.1.2012 COM(2012) 11 final.

cheaper or more privacy friendly mHealth apps become available'.[348] Subsequently, if the user would like to change the smart phone on which the mHealth app is installed, it means loss of contacts, photos, interpersonal communications and other kinds of personally or socially relevant data, created spending hours and hours online, and which are very difficult to recreate or restore. For instance, in the context of mHealth, this would mean the loss of data regarding steps, calories, health parameters collected over a long period of time, necessary for further health improvement.

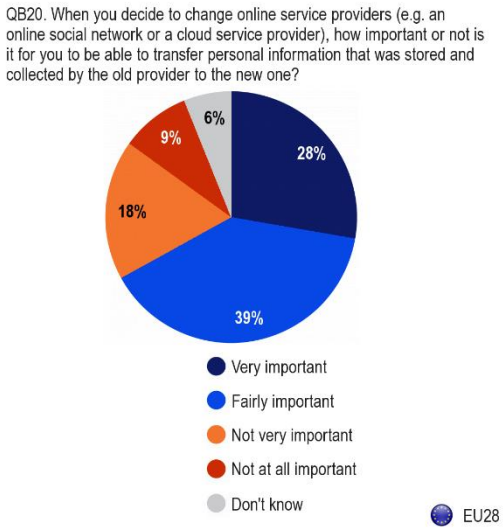

Figure 4. Eurobarometer survey on attitudes toward data portability. *Source: Special Eurobarometer 431, Data Protection Report, Publication: June 2015.*

As identified in the Data Protection Eurobarometer (Figure 4),[349] two-thirds of respondents, or 67%, answered that it is important to them to be able to transfer personal information that has been stored and collected by the old provider to the new one when they change online service providers: 28% answered this is very important, and 39% that it is

---

[348] Impact Assessment, Brussels, 25.1.2012 SEC(2012) 72 final p.28, , https://www.cr-online.de/2012_0125_EU_Commission_Impact_Assessment_to_Proposal_Data_Protection_SEC_2012-72.pdf.

[349] Data Protection Report, Special Eurobarometer 431, Fieldwork: March 2015, Publication: June 2015. This survey has been requested by the European Commission, Directorate-General for Justice and Consumers and coordinated by the Directorate-General for Communication, page 45, http://ec.europa.eu/commfrontoffice/publicopinion/archives/ebs/ebs_431_en.pdf.

fairly important. Only 27% answered it is not important to be able to transfer personal information to a new service provider.

To summarise, control over provided personal data and possibility to transfer that data to other mHealth app is crucial for the users. Not solely to prevent 'lock-in', but for further improvement of their well-being and health, which is dependent on these data.

2.2 Right to data portability as a competitive element

The second purpose, besides empowering users to prevent 'lock-in', is to foster opportunities for innovation and sharing of personal data between data controllers in a safe and secure manner under the data subject's control.[350] It has been predicted that the possibility of moving data from one service provider to another would increase competition and could mark 'data protection' as an competitive advantage, meaning users will tend to move more toward services they consider appropriate in terms of data protection.[351] For instance, an mHealth app user would not be bound to continue using an app once trusted as privacy friendly, if he or she is of the opinion that the app is not appropriate anymore in terms of data protection.[352] As envisioned, the right to data portability should enforce a healthy competitive environment in the EU, by opening the market for SME which could offer privacy friendly solutions. Subsequently, its main idea was to prevent a single dominant company that infringes privacy laws to continue gaining advantage over its competitors. Still, one cannot ignore the fact that from an economic perspective, the companies would prefer to have many users locked into their service by lowering entry costs and increasing exit costs, indeed as the case with Facebook and Google.[353] Google users can transfer their contacts onto the Facebook platform, but it has been not possible

---

[350] Article 29 WP, Guidelines on the right to data portability, Adopted on 13 December 2016, As last Revised and adopted on 5 April 2017, page 5.

[351] Impact Assessment, Brussels, 25.1.2012 SEC(2012) 72 final p.106, https://www.cr-online.de/2012_0125_EU_Commission_Impact_Assessment_to_Proposal_Data_Protection_SEC_2012-72.pdf.

[352] Impact Assessment, Brussels, 25.1.2012 SEC(2012) 72 final, p.106.

[353] Google to Facebook: You can't import our user data without reciprocity, published Nov. 5 2010 https://techcrunch.com/2010/11/04/facebook-google-contacts/.

other way around. To address this challenge, Google has changed their terms and condition, introducing reciprocity, meaning any service that would like to access and import Google contacts APIs would need to offer reciprocity.

In the opinion on purpose limitation, the Article 29 WP stated that allowing 'data portability could enable businesses and data-subjects to maximise the benefits of big data in a more balanced and transparent way. It can also help minimise unfair or discriminatory practices and reduce the risks of using inaccurate data for decision-making purposes, which would benefit both businesses and data-subjects/consumers'.[354] One may argue that data portability is considered as an 'additional safeguard' applied by data controllers, which may 'empower data subjects' and, therefore, constitutes a positive element in the balancing test between data controllers' legitimate interests and the data protection rights of subjects.[355]

As constructed, it will apply to all data controllers, irrespectively of whether they are a big company or a start-up. This idea has positive and negative aspects. The positive aspect is that it will force dominant companies to open the data market for new entrants, who are more likely to create innovative services. The negative aspects are that it might create a disproportionate burden, in terms of the necessary resources and investment, for small companies and start-ups to comply with the RDP. Second, the question is if and to what extent the dominant companies would allow data transfers, considering their investment in creating the data sets, as well as protection of their trade secrets, intellectual property and particularly, the copyrights protecting their software. Yet, the latter should not be seen as an obstacle to refuse portability, since data controllers can transmit the personal data provided by data subjects in a form that does not release information covered by trade secrets or intellectual property rights.[356] Indeed, the trade secret or intellec-

---

[354] Article 29 WP, Opinion 03/2013 on purpose limitation, WP 203, p. 47

[355] The right to data portability in the GDPR: Towards user-centric interoperability of digital services, PaulDe Hert, Vagelis Papakonstantinoua, Gianclaudio Malgieria, Laurent Beslay, Ignacio Sanchez, Computer Law & Security Review Volume 34, Issue 2, April 2018, Pages 193-203 https://www.sciencedirect.com/science/article/pii/S0267364917303333#fn0060

[356] Article 29 WP, Guidelines on the right to data portability, Adopted on 13 December 2016, As last Revised and adopted on 5 April 2017, page 12

tual properties are not really the obstacle but the battle for market share is. Tech companies benefiting from the openness of their platforms, attracting more developers and thus increasing the value of their platforms by attracting more users. In fact, they want the advantages of openness but without the risk of emergence of competing services. This is similar to free trade, in which governments embrace the benefits of free trade but strive to minimise the political instability when less-competitive industries lose.

This competitive element of RDP raises the question if this right is a matter of data protection law or competition law. Even though it was introduced in the GDPR, the Former Commissioner for Competition Almunia has said that right to data portability goes to the heart of competition policy.[357] So, it might be expected that EU Commission will take action based on competition law if a dominant company does not allow its users to exercise the right to data portability, or to transfer their data to other companies.[358] In such a case, this will be possible based on Article 102 of the Treaty on the Functioning of the EU, which prohibits abusive behaviour of dominant undertakings.[359] Competition authorities are entitled to impose duties on dominant undertakings in order to remedy the abusive behaviour.[360] If the dominant company resists transferring data to a competitor,

---

[357] Commissioner Almunia, 'Competition and personal data protection', speech given at the Privacy Platform event: Competition and Privacy in Markets of Data in Brussels on 26 November 2012, http://europa.eu/rapid/press-release_SPEECH-12-860_en.htm

[358] Graef, Inge and Verschakelen, Jeroen and Valcke, Peggy, Putting the Right to Data Portability into a Competition Law Perspective (2013). Law: The Journal of the Higher School of Economics, Annual Review, 2013, pp. 53-63. Available at SSRN: https://ssrn.com/abstract=2416537 p.6

[359] Consolidated version of the Treaty on the Functioning of the European Union'; Article 102 (ex Article 82 TEC) 'Any abuse by one or more undertakings of a dominant position within the internal market or in a substantial part of it shall be prohibited as incompatible with the internal market in so far as it may affect trade between Member States. Such abuse may, in particular, consist in: (a) directly or indirectly imposing unfair purchase or selling prices or other unfair trading conditions; (b) limiting production, markets or technical development to the; (d) making the conclusion of contracts prejudice of consumers; (c) applying dissimilar conditions to equivalent transactions with other trading parties, thereby placing them at a competitive disadvantage subject to acceptance by the other parties of supplementary obligations which, by their nature or according to commercial usage, have no connection with the subject of such contracts.'
See: http://eur-lex.europa.eu/legalcontent/EN/ALL/?uri=CELEX%3A12008E102

[360] Article 5 and 7(1) of Council Regulation 1/2003 of 16 December 2002 on the implementation of the rules on competition laid down in Articles 81 and 82 of the Treaty [2002], OJ L1/1. See more on: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32003R0001

based on the data portability request, they might be in breach of Article 102(b), 'limiting production, markets or technical development to the prejudice of consumers'.

The issue of data portability has been addressed by the EU Commission in two cases: *Google* case[361] and *Facebook/WhatsApp*.[362] In the first case, a lack of data portability on the Google platform prevented advertisers from porting and managing their search advertising campaigns across Google to the competing search advertising platforms. In October 2013, Google provided an improved commitment to the Commission, guaranteeing portability on the search advertising campaigns on competing platforms.[363] In the second case, Facebook/WhatsApp's right to data portability has been addressed in the context of merging of these two entities. To clarify, Facebook acquired the cross-platform communication app WhatsApp, which is available on more mobile operating systems, including iOS, Android, BlackBerry 7 and 10, Windows Phone, and Nokia Series 40 (Asha) and 60 (Symbian), contrary to Apple's FaceTime and iMessage, which are considered as 'proprietary apps' and are available only on iOS.

One of the Commission's concerns in this case was whether data portability creates a substantial obstacle for consumers when switching between consumer communications apps. It concluded that data portability probably will not prevent switching, for the following reasons. First, these entities do not control any essential parts of the network or any mobile operating system, meaning, users of consumer communications apps are not locked-in to any particular physical network, hardware solution or anything else that needs to be replaced in order to use competing products. Additionally, the messaging history remains accessible on a user's smartphone even if the user starts using a different consumer communications app, until the moment the user delete the history or decides to uninstall the app, and the contact list of a WhatsApp user can be easily ported if user

---

361 Commitment in Case COMP/C-3/39.740 - *Foundem and others*, April 3, 2013 paras. 27–31, http://ec.europa.eu/competition/antitrust/cases/dec_docs/39740/39740_8608_5.pdf

362 Case No COMP/M.7217 - FACEBOOK/ WHATSAPP, Regulation (EC) No 139/2004 Merger Procedure, Date: 03/10/2014

363 The Google antitrust case: what is at stake? Speech of Joaquín Almunia - Former Vice President of the European Commission responsible for Competition Policy. October 2013, http://europa.eu/rapid/press-release_SPEECH-13-768_en.htm

gives consent to the competing app to access the contact list. Second, communication via the app tends to consist of a significant extent of short, spontaneous chats, which do not necessarily carry long-term value for consumers.[364] Both of these cases point out that the right to portability can be addressed by the competition law, but in specific cases and solely if the restriction on data portability qualifies as abuse of dominant position.

To clarify, the GDPR gives mHealth apps users the right to data portability, whereas, competition law has power to impose a duty on dominant services. The scope of the application of the two regimes is different. The right to data portability applies only to personal data; data that is not qualified as personal data is out of its scope. Whereas, competition law has a wider scope and applies to all data, irrespective if it is personal data or not. Although in the mHealth apps sector, it is disputable whether a particular app could establish a dominant position. Still, having in mind the existence of HealthKit (OS) and Google Fit (Android), this might be not far away from reality in the near future. Nevertheless, this relationship between the right to data portability and competition law is not within the scope of this thesis.[365]

After clarifying the purposes of the right to data portability, and what that mean for mHealth app users, the next step is to understand its position in the data protection law.

---

[364] Case No COMP/M.7217 - FACEBOOK/ WHATSAPP, Regulation (EC) No 139/2004 Merger Procedure, Date: 03/10/2014, see 113-115 and 134

[365] See, e.g. Graef, Inge and Verschakelen, Jeroen and Valcke, Peggy, Putting the Right to Data Portability into a Competition Law Perspective (2013). Law: The Journal of the Higher School of Economics, Annual Review, 2013, pp. 53-63. Available at SSRN: https://ssrn.com/abstract=2416537; Graef, Inge, Mandating Portability and Interoperability in Online Social Networks: Regulatory and Competition Law Issues in the European Union (July 22, 2013). Telecommunications Policy 2015, Vol. 39, No. 6, p. 502-514. Available at SSRN: https://ssrn.com/abstract=2296906 or http://dx.doi.org/10.2139/ssrn.2296906; Drexl, Josef and Hilty, Reto and Globocnik, Jure and Greiner, Franziska and Kim, Daria and Richter, Heiko and Slowinski, Peter R. and Surblyte, Gintare and Walz, Axel and Wiedemann, Klaus, Position Statement of the Max Planck Institute for Innovation and Competition of 26 April 2017 on the European Commission's 'Public consultation on Building the European Data Economy' (April 26, 2017). Max Planck Institute for Innovation & Competition Research Paper No. 17-08. Available at SSRN: https://ssrn.com/abstract=2959924 or http://dx.doi.org/10.2139/ssrn.2959924.

3. The right to data portability and mHealth apps

In order to understand the position of the RDP in the data protection law and how that reflects on the mHealth apps, we will first do a legal-historical overview of their evolution, from origin to final adoption. The right to data portability, in the original Commission proposal was first introduced in Article 18,[366] which stated:

> *1. The data subject shall have the right, where personal data are processed by electronic means and in a structured and commonly used format, to obtain from the controller a copy of data undergoing processing in an electronic and structured format which is commonly used and allows for further use by the data subject.*
>
> *2. Where the data subject has provided the personal data and the processing is based on consent or on a contract, the data subject shall have the right to transmit those personal data and any other information provided by the data subject and retained by an automated processing system, into another one, in an electronic format which is commonly used, without hindrance from the controller from whom the personal data are withdrawn.*
>
> *3. The Commission may specify the electronic format referred to in paragraph 1 and the technical standards, modalities and procedures for the transmission of personal data pursuant to paragraph 2. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).*[367]

In the first comments by the Article 29 WP on the proposed right to data portability, the positive effects were emphasised:

> It would also let individuals 'share the wealth' created by big data and incentivise developers to offer additional features and applications to their users. In many situations, safeguards such as allowing customers to have direct access to their data in a portable, user-

---

366 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), Brussels, 25.1.2012 COM(2012) 11 final

367 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), Brussels, 25.1.2012 COM(2012) 11 final.

> friendly and machine-readable format may help empower them, and redress the economic imbalance between large corporations on the one hand and users on the other.[368]

Indeed, this comment corresponds with the two already discussed purposes of the RDP.

It is worth noting that during the negotiation process the originally proposed text was amended. As a result of later amendments, the right to data portability was seen as a prolongation[369] of the right to access, Article 15(2a),[370] or as part of the right to access.[371] However, from the beginning the text (right) has been criticised as unprecedented and problematic,[372] one which would defeat its own purpose and might even reduce consumer welfare.[373]

---

[368] Article 29 WP, Opinion 03/2013 on purpose limitation, WP 203, p. 47.

[369] Council of the European Union, Interinstitutional File: 2012/0011 (COD), Working Group on Information Exchange and Data Protection (DAPIX), 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)- Data Portability (Revision of Article 18) Brussels, 6 June 2014, 10614/14, page 2, http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%2010614%202014%20INIT.

[370] European Parliament legislative resolution of 12 March 2014 on the 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) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)) (Ordinary legislative procedure: first reading), http://www.europarl.europa.eu/sides/getDoc.do?type=TA&language=EN&reference=P7-TA-2014-0212.

[371] Amendment 111, Right to access and to obtain data for the data subject '2a. Where the data subject has provided the personal data where the personal data are processed by electronic means, the data subject shall have the right to obtain from the controller a copy of the provided personal data in an electronic and interoperable format which is commonly used and allows for further use by the data subject without hindrance from the controller from whom the personal data are withdrawn. Where technically feasible and available, the data shall be transferred directly from controller to controller at the request of the data subject', REPORT on the 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) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)) Committee on Civil Liberties, Justice and Home Affairs Rapporteur: Jan Philipp Albrecht, A7-0402/2013, 21.11.2013, page 87, http://www.europarl.europa.eu/sides/getDoc.do?type=TA&language=EN&reference=P7-TA-2014-0212.

[372] 'Why the Right to Data Portability Likely Reduces Consumer Welfare: Antitrust and Privacy Critique', Peter Swire & Yianni Lagos , 72 Maryland Law Review 335 (2013), Ohio State Public Law Working Paper 204, p.337.

[373] *Id*., p. 349.

Some Member states expressed their concerns. For example, while the UK supported the concept of data portability, it considered it as not being within the scope of data protection but should be addressed as part of consumer or competition law. Therefore, the UK suggested that this article should be deleted. Several other countries[374] considered that this right should fall within the scope of the competition law or intellectual property law. Others[375] pointed out that it could present risk to the intellectual property and commercial confidentiality of the controllers. Some of the other remarks have been that it will imply significant administrative burdens, that it might endanger on-going research or the continuity of health services, as well as increase the risk of fraud. Regarding the last concern, some countries have fears that it may be used to fraudulently obtain the data of innocent data subjects. Other concern raised during the negotiation process has been difficulty or impossibility to exercise this right in 'multi-data subject' cases. For example, in a group photo, which contains data from several data subjects, some of them might not necessarily agree or even be known or be able to be contacted regarding exercising the right to data portability.[376]

Despite the comments and critics, the right to data portability survived the negotiation process and was considered as separate right (Article 20), which falls within the scope of the GDPR, since its main purpose is to increase the control of data subjects over their personal data and to ensure the free flow of personal data. In the final version, some criticisms have been accepted, and therefore in Article 20, paragraph 4, the following text has been added: ‘this right shall not adversely affect the rights and freedoms of others’. This has been added as an attempt to indirectly remedy the possible harmful effects on third parties, arising from intellectual property rights, trade secret, and copyright protecting the software. At the end, the core values of the right have not changed.

---

374 Denmark, Germany, France, Republic of Ireland, the Netherlands, Poland and Sweden.

375 Denmark, Germany and the UK.

376 Council of the European Union, Interinstitutional File: 2012/0011 (COD), Working Group on Information Exchange and Data Protection (DAPIX), 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)- Data Portability (Revision of Article 18) Brussels, 6 June 2014, 10614/14, page 3, http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%2010614%202014%20INIT.

One of the suggested amendments[377] by the Committee on Civil Liberties, Justice and Home Affairs, later adopted in the final version, is of particular interest for this thesis. It is the one that has advocated adding 'interoperable formats' in addition to 'structured and commonly used and machine-readable formats'. The initial thought about interoperable formats has been optimistic, starting from the idea that if the transfer of data about users is already possible through other interfaces, e.g. for third party application developers or for exchanges with affiliated companies, then the costs for implementation of the right to data portability will be minimal.[378] In contrast, some scholars have argued[379] that this will impose heavier duties on data processors, since they will have an obligation to make their data formats compatible and ensure that their system can process data from a different origin.

The opinion of the author is that adding 'interoperability formats' in addition to making the data structured, commonly used and machine-readable will not increase user control over personal data. First, as explained in the GDPR, data controllers are only encouraged to develop interoperable formats that enable data portability but are not obliged to do so.[380] Yet this is not the biggest issue. The second and the most worrying thing is that developing interoperable formats and transferring the data from one controller to other as some scholars argued: 'could mean the moment of identity fraud that can turn into a life-

---

[377] REPORT on the 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) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)) Committee on Civil Liberties, Justice and Home Affairs Rapporteur: Jan Philipp Albrecht, A7-0402/2013, 21.11.2013 page 24 http://www.europarl.europa.eu/sides/getDoc.do?pubRef=//EP//NONSGML+REPORT+A7-2013-0402+0+DOC+PDF+V0//EN

[378] Impact Assessment, Brussels, 25.1.2012 SEC(2012) 72 final p.106, https://www.cr-online.de/2012_0125_EU_Commission_Impact_Assessment_to_Proposal_Data_Protection_SEC_2012-72.pdf

[379] Graef, Inge and Verschakelen, Jeroen and Valcke, Peggy, Putting the Right to Data Portability into a Competition Law Perspective (2013). Law: The Journal of the Higher School of Economics, Annual Review, 2013, pp. 53-63. Available at SSRN: https://ssrn.com/abstract=2416537

[380] GDPR April 2016, Recital 68

time breach of personal data'.[381] The issue of interoperability and challenges arising from it between mHealth apps will be discussed in the next chapter.

Subsequently, despite the amendments, the main principles underlying the originally proposed text for the 'right to data portability' remained unchanged, merely a bit more complicated. The proposal for GDPR after four years of negotiation finally was adopted in April 2016, [382] and applied beginning on 25th of May 2018. Because the GDPR is a Regulation, it will directly apply in all EU countries, without the need to be passed into national law replacing the EU and national data protection legislation.[383]

In the GDPR, the right to data portability falls within Article 20, stating:

> 1. The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where:
>
> (a) the processing is based on consent pursuant to point (a) of Article 6(1) or point (a) of Article 9(2) or on a contract pursuant to point (b) of Article 6(1), and
>
> (b) the processing is carried out by automated means.
>
> 2. In exercising his or her right to data portability pursuant to paragraph 1, the data subject shall have the right to have the personal data transmitted directly from one controller to another, where technically feasible.

---

381 'Why the Right to Data Portability Likely Reduces Consumer Welfare: Antitrust and Privacy Critique', Peter Swire & Yianni Lagos , 72 Maryland Law Review 335 (2013), Ohio State Public Law Working Paper 204, p.339

382 On 8 April 2016 the Council adopted the Regulation and the Directive. And on 14 April 2016 the Regulation and the Directive were adopted by the European Parliament. On 4 May 2016, the official texts of the Regulation and the Directive have been published in the EU Official Journal in all the official languages. While the Regulation will enter into force on 24 May 2016, it shall apply from 25 May 2018. http://ec.europa.eu/justice/data-protection/reform/index_en.htm

383 See Article 288, TFEU, A regulation shall have general application. It shall be binding in its entirety and directly applicable in all Member States. It will directly apply in the legal order of the member states without being transposed in national law

> 3. The exercise of the right referred to in paragraph 1 of this Article shall be without prejudice to Article 17. That right shall not apply to processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.
>
> 4. The right referred to in paragraph 1 shall not adversely affect the rights and freedoms of others.

As a matter of fact, this is an absolutely new right in the data protection law, not just in Europe but also worldwide. Consequently, there are not many legal interpretations[384] or literature regarding the right to data portability of personal data. Therefore, for the purpose of this section our discussion will be based on the 'Guidelines on the right to data portability' published by the Article 29 Working Party.[385] The draft guidelines were published in December 2016 and they discussed the new right and clarified the conditions under which it is applicable.[386] After a public consultation in which stakeholders have been given the opportunity to comment on the draft guidelines, on 5 April 2017, the Article 29 WP issued the final version of the guidelines. According to the guidelines right to data portability consist of two rights.

The first one is '***to receive*** *the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format…'* The second one *is* ***the right to transmit*** *those data to another controller without hindrance from the controller to which the personal data have been provided*'.

We will discuss both, however, for the purpose of this thesis, attention will be particularly paid to the second one.

---

[384] Swire, Peter and Lagos, Yianni, Why the Right to Data Portability Likely Reduces Consumer Welfare: Antitrust and Privacy Critique (May 31, 2013). 72 Maryland Law Review 335 (2013); Ohio State Public Law Working Paper 204. Available at SSRN: https://ssrn.com/abstract=2159157, p.339.

[385] 'Guidelines on the right to data portability' by Article 29 Working Party, 5 April 2017, 16/EN WP 242 rev.01.http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp242_en_40852.pdf.

[386] Article 29 working party 'Guidelines on the right to data portability', 13 December 2016, 16/EN WP 242.

The first one allows the data subject to receive, in other words, to download the personal data that he has provided to a controller, and to store it on a private device, in order to reuse them. This would mean that it is not going to be transferred to another controller. This right to some extent complements the right to access.[387] Still, the scope of the 'right to access' is broader, and refers to processing of personal data concerning the data subject such as (a) the purposes of the processing; (b) the categories of personal data concerned; (c) the recipients to whom the personal data has been or will be disclosed; (d) the envisaged period for which the personal data will be stored; (e, f) the existence of other data subject's rights; (g) any available information as to the source of data; and (h) the existence of automated decision-making, including profiling, and meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject, and (i) to provide copy of the data in a commonly used electronic format. The main difference between the right to access and RDP is, that, based on the latter, the right to receive data is limited only to situations where personal data is 'provided by' the data subject in a 'structured, commonly used and machine-readable format'. This means that users of mHealth apps can download or receive only the personal data they provided to the app, such as steps, calorie intakes or other health parameters, and further reuse them by transferring them to another controller.

The second part of the RDP is right to transmit the personal data from one controller to other 'without hindrance'. This means it allows data subjects not just to receive the data and reuse them, but also to transfer them to another controller in order to prevent lock-ins. In this way, they can transfer their data from one controller to other, which may offer more affordable services, in terms of price and privacy, for example. Actually, it is obvious that the role of the data protection in the digital economy is presented as an element of the competition between controllers. That aim to encourage innovation and sharing of data between controllers.

---

[387] GDPR, Article 15 (3) 'The controller shall provide a copy of the personal data undergoing processing. For any further copies requested by the data subject, the controller may charge a reasonable fee based on administrative costs. Where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic form'.

4. Limitations on exercising the right to data portability

After outlining the two main elements of the RDP, 'receiving' and 'transferring' personal data, in the following section, we will analyse which limitations or conditions users of the mHealth app will confront in exercising this right. Limitations will be discussed from the legal and technical point of view.

Despite the best intentions of legislators, data portability most probably is and will be a distant concept to the average user of the mHealth apps, often because of the highly technical nature of the subject and solutions involved,[388] as well as lack of awareness for the existence of this right. Therefore, developers or owners of mHealth apps as data controllers have a crucial role. They have the obligation to inform users about the existence of this new right through data portability policy, explaining to them the conditions under which they can exercise their right. Basically, they should clearly explain the difference between the types of data that a mHealth app user can receive through the right to data portability in contrast to rights of access, as well as ensure that they distinguish the right to data portability from other rights. Other important fact is that data portability policy should be written in a concise, transparent, intelligible and easily accessible form, using plain and clearly understandable language. It is essential to do so in order to be understood by people with different educational background. Apart from this, the GDPR also had foreseen strict time limits for responding to a data request. The timeline from the data portability request till the execution, according to Article 12 (3) should be 'without undue delay' and in any case 'within one month of receipt of the request' or within a maximum of three months for complex cases. In general, the request should be complied with free of charge, unless, the requests are manifestly unfounded, excessive or repetitive. Interestingly, one of the ideas that appear in the Opinion is that the controller should also inform users about the right to data portability before they decide to close their accounts, the same as already envisioned in the Digital Content Directive.

---

[388] Realising the right to data portability for the domestic Internet of things, Lachlan Urquhart, Neelima Sailaja DOI 10.1007/s00779-017-1069-2, Published online 23 August 2017, page 9, https://link.springer.com/content/pdf/10.1007%2Fs00779-017-1069-2.pdf.

Indeed, apart from the existence of the right to data portability as such in the GDPR, the notion of 'strengthening user control over their data' can be additionally achieved with clear and easy understandable portability policies and strict timelines.

4.1. Legal limitations

No matter, if we are talking about the right 'to receive' or 'to transfer' the data, Article 20 is clear regarding conditions that need to be fulfilled in order for the data subject to request the right to data portability. These are listed in the subsections that follow.

4.1.1 Personal data provided by the data subject

The first condition is data to be provided by the data subject. However, this incorporates three sub-conditions.

4.1.1.1 Data concerning the user

The first one is the personal data must *concerning him* (i.e. the user). As we already noted above, the scope of the right to data portability covers only personal data concerning data subject. Put differently, this entails information relating to an identified or identifiable natural person. The following discussion will be based on Schwartz and Solove's three specific states of data: identified, identifiable, and non-identifiable.[389]

a) Non-identifiable or Anonymised data

If data concerning the mHealth app user is non-identifiable or anonymous data, then it falls out of the scope of GDPR, and the right to data portability cannot be exercised.[390] The GDPR does not provide definition of 'anonymisation'; only Recital 26 of the GDPR states that 'principles of data protection should not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or personal data rendered anonymous in such a manner that the data subject is not or no

[389] Solove, Daniel J. and Schwartz, Paul M., 'Reconciling Personal Information in the United States and European Union' (2013).GWLaw Faculty Publications & Other Works, Paper 956, http://scholarship.law.gwu.edu/faculty_publications/956.

[390] Recital 26, GDPR.

longer identifiable'. Put differently, data is considered to be anonymised if all identifying elements are eliminated from a set of personal data. Successfully anonymised data are no longer personal data, and cannot be considered as personal data under Article 4(1). As a matter of fact, this can be achieved only if anonymisation is engineered appropriately,[391] meaning no element is left in the information which may, by the exercise of reasonable effort, serve to re-identify the person. In any case, this requires data controllers, in particular, to separate anonymised data from other data, which have been manipulated using various techniques to mitigate risks of re-identification of the concerned individuals.[392]

The discussion regarding anonymised data is two-fold. On the one hand, some argue that this sets a high threshold for data to be considered anonymised, otherwise data protection law will continue to apply.[393] On the other hand, others argue that currently, anonymisation is increasingly difficult to achieve due to the advance of modern computers. technology and the ubiquitous availability of information,[394] for the reason that re-identification of individuals is an increasingly common and present threat. In order to examine the likelihood of re-identification of individuals from anonymised data, anonymisation techniques should take into account the current state of the art of technology. Consequently they should be able to prevent:

- Singling out – this occurs where it is possible to distinguish the data relating to one individual from all other information in a dataset.
- Data linking – this occurs when any linking of identifiers in a data set will make it more likely that an individual is identifiable. In other words, it is the ability to link, at least, two records concerning the same data subject or a group of data subjects either in the same database or in two different databases.

---

391 Opinion 05/2014 on Anonymisation Techniques, Article 29 WP Adopted on 10 April 2014, p. 3.

392 Article 29 WP, Opinion 06/2013 on open data and public sector information ('PSI') reuse, WP 207, Adopted on 5 June 2013, page 13.

393 Article 29 WP, Opinion 06/2013 on open data and public sector information ('PSI') reuse, WP 207, Adopted on 5 June 2013, page 13.

394 Ohm, Paul, Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization (August 13, 2009). UCLA Law Review, Vol. 57, p. 1701, 2010; U of Colorado Law Legal Studies Research Paper No. 9-12. Available at SSRN: https://ssrn.com/abstract=1450006

- Inference – this occurs when is possible to infer a link between two pieces of information in a set of data with a significant probability, even though the information is not expressly linked.

The discussion about anonymised data is relevant for the users of the mHealth app. If mHealth app developer successfully anonymised data by eliminating all identifying elements from a set of personal data then the data protection law does not apply, meaning mHealth users cannot exercise the right to data portability. Theoretically, this is true, but the reality is a bit different. As argued in the Opinion on Anonymisation, technically it is very difficult to ensure complete anonymisation of the data. For instance, even in big companies employer will be often able to single out individual employees with particular health indications. [395]

b) Identifiable or Pseudonymous data

On the other hand, pseudonymous data is personal data and therefore is considered to fall within the scope of the right to data portability under certain conditions.[396] But, what is 'pseudonymisation'? Simply it would mean that is achieved, for instance, by replacing identifiers such as name and surname with one pseudonym, such as numbers. However legal analysis of 'pseudonymisation' reveals that is more complex. In the GDPR,

> 'pseudonymisation' means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.[397] Personal data which have undergone pseudonymisation, which could be attributed to a natural person by the use of additional information, should be considered to be information on an identifiable natural person. To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or

---

[395] Opinion 2/2017 on data processing at work, WP249, Adopted on 8 June 2017, page 18

[396] 'Guidelines on the right to data portability' by Article 29 Working Party, Adopted on 13 December 2016, p.7

[397] Article 4, para. 5 GDPR.

> by another person to identify the natural person directly or indirectly. To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments.[398]

The Article and the recital provide a conceptual definition of pseudonymisation.[399] It does not clarify how such a process should or could be performed; instead, the focus is on the outcome, wherein personal data should no longer be attributed to a specific data subject without the use of additional information. According to the definition, to determine whether a natural person is identifiable (directly or indirectly), account should be taken of all the means reasonably likely to be used, as well as all objective factors for instance costs, the amount of time required for identification, and the available technology at the time of the processing and technological developments.

It should be emphasised that the wording in Article 4(5) and Recital 26 of the GDPR, in fact, does not provide a definition of pseudonymous data. Instead, the GDPR introduces a definition of 'pseudonymisation' as opposed to 'pseudonymised data' or 'pseudonymous data' to stress that pseudonymisation should be considered as an activity and not as a type of data. Therefore, it is considered solely as a way of processing data, while data that has undergone pseudonymisation is still personal data.[400]

Pseudonymisation as a way of processing personal data is based on the assumption that personal data must be collected and processed in compliance with the data protection legislation. In this context, pseudonymisation, is meant as the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, meaning, when pseudonymisation is achieved such personal data can be used for 'further processing'. More precisely, it pre-

---

[398] Recital 26, GDPR

[399] Article 29 WP, Opinion 05/2014 on Anonymisation Techniques, WP 216, Adopted on 10 April 2014, page 5.

[400] UK's Information Commissioner Office's (ICO) analysis on the GDPR during the negotiations. https://ico.org.uk/media/1432420/ico-analysis-of-the-council-of-the-european-union-text.pdf, page 2.

sents a ground for the lawfulness of processing. In principle, this means that controllers could use it for purposes beyond those for which it was originally obtained without data subject's consent or when is not based on a Union or Member State law. In such a case the controller shall, in order to ascertain whether processing for another purpose is compatible with the purpose for which the personal data are initially collected, among other facts should take into account the existence of appropriate safeguards, which may include encryption or pseudonymisation.[401] For example, when processing of sensitive data is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes,[402] then is allowed only if appropriate technical and organisational measures are used that respect the principle of data minimisation such as pseudonymisation.[403] In addition, pseudonymisation is discussed in the context of achieving data protection by design[404] and security of processing,[405] as a measure that will decrease the privacy risk. For example, if the pseudonymous profile is created for a mHealth app user, then in a case of a data breach, the privacy risk will be reduced, since there will be no immediate link between the profile and the real mHealth user.

However, one thing is imprecise in the definition, that is, whether pseudonymisation is intended to be an irreversible process or not. Arguably, yes, it should be an irreversible process. First, according to Article 29WP,[406] a pseudonym means that it is possible to backtrack to the individual so that the individual's identity can be discovered. Second, the answer to this question can be found by analysing Article 5(e), the principles relating to the processing of personal data, which read as follows:

> Personal data shall be 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.

---

401 Art. 6(4)(e).

402 Art. 9(2)(j), GDPR.

403 Art. 89(1), GDPR.

404 Art. 25, GDPR.

405 Art.32(1), GDPR.

406 Article 29 WP, Opinion 4/2007 on the concept of personal data, WP 136 Adopted on 20th June 2007.

Particularly, this article emphasises that personal data can be pseudonymous, but in a form that allows re-identification. Certainly, if the purposes for which personal data are processed do not longer require a data controller to keep or process additional information in order to identify the mHealth user. What does this mean for users of mHealth apps? Can they request the right to data portability, if data is pseudonymised?

The Article 29 WP in their opinion explained that in the case of pseudonymous data, the data controller can reject the data portability request. Solely if after the pseudonymisation, data cannot be clearly linked to a data subject.[407] According to the same opinion, the burden is on the data subject, to provide additional information enabling their identification.[408] It seems paradoxical that the data subject should provide more personal data to identify himself in order to receive the data back. At first sight this leads to excessively burdensome or perhaps even absurd consequences.[409] This interpretation is not in line with the initial thoughts of the right to data portability, introduced to strengthen user control over their personal data. In fact, this clarification presents an obstacle for the data subject to receive or transfer their data, if they cannot provide additional information to enable identification. It does not constitute a fair balance between, on one hand, the interest of the data subject in protecting his personal data, in particular right to data portability and, on the other hand, the obligation of the controller after pseudonymisation of personal data to clearly link them to a particular data subject. In order to provide more constructive interpretation in this context, we refer to the case law of the European Court of Justice, specifically, the case *College van burgemeester en wethouders van Rotterdam v M.E.E. Rijkeboer*.[410] The case is about the need to retain the data in an identifiable format to enable, data subjects to exercise their right to access. The Court ruled the following:

---

[407] Article 29 WP, Guidelines on the right to data portability, adopted on 13 December 2016, As last Revised and adopted on 5 April 2017, page 9.

[408] Article 11 (2), GDPR.

[409] Article 29 WP, Opinion 4/2007 on the concept of personal data, WP 136 Adopted on 20th June 2007, page 5.

[410] European Court of Justice, College van burgemeester en wethouders van Rotterdam v M.E.E. Rijkeboer, Case C-553/07, May 2009, provisions 65 and 66.

> requires the Member States to ensure a right of access to information on the recipients or categories of the recipient of personal data and on the content of the data disclosed not only in respect of the present but also in respect of the past. It is for the Member States to fix a time-limit for storage of that information and to provide for access to that information which constitutes a fair balance between, on the one hand, the interest of the data subject in protecting his privacy, in particular by way of his rights to object and to bring legal proceedings and, on the other, the burden which the obligation to store that information represents for the controller.

In fact, fair balance is particularly relevant based on Article 6(f) of the GDPR.[411] This means that the legitimate interest of data controllers that process pseudonymous data must be always balanced against the data subjects' rights and fundamental freedoms. In principle, if the controller has collected and subsequently pseudonymised personal data, it is required to retain the personal data in an identifiable format for a limited period of time, to enable the data subjects to exercise their rights.

Still, one can argue that this decision is based on the Directive 95/46/EC and is partly valid according to GDPR. To clarify, striking the balance between the interest of data subject and obligation of the controller is valid according to both the Directive and the GDPR. However, it might be arguable to what extent under the GDPR it is valid to ensure a right to data portability in respect of the past data, especially, based on the analysis of Article 11(1) and (2), regarding processing which does not require identification, and if the controller can demonstrate that is not possible to identify the user. Stating that if the purposes for which personal data are processed do no longer require the identification of a data subject, the controller is not obliged to process additional information in order to identify the data subject. Particularly, this is not required for the purpose of complying with the Regulation, meaning, the data controller is not obliged to process additional information in order to identify the data subject, who would like to revoke the right to data portability for past data.

To explain what is meant by 'is not required for the purpose' in the context of apps, first, it should be clarified what is the purpose of the app. For example, a running app or one

---

411 Article 29 WP, Opinion 05/2014 on Anonymisation Techniques, WP 216, Adopted on 10 April 2014, page 8.

that counts calories would place the retention period into the control of the user, while for a navigation app it is sufficient to store only the last 10 recently visited locations. Second, it should be taken into consideration how long app has been inactive. For instance, the inactivity might be due to switching to a new device or if the smart phone is lost. In such a case app developers should predefine a time period of inactivity, and inform the user of the running app, for example, that after this time the account will be treated as expired. Upon expiry of this time period, if user does not react, personal data relating to the user and usage of the app should be irreversibly anonymised or deleted. Additionally, the inactivity period depends on the purpose of the app and the location where the data are stored.[412]

This discussion is relevant for two reasons. First, as some of the data subject's rights, in particular, right to data portability, might be burdensome to comply with, Article 11 can encourage controllers or app developers, when it is possible, to strive more toward anonymous data or pseudonymisation. This certainly will result in reducing their obligations under the GDPR. Actually, this presents a decent way of refusing to act on a request for data portability and to protect their data sets, especially in situations when the data controller can demonstrate that is not in a position to identify data subject. Then, this is considered as justification to reject the request.[413] Second, it should be noted that the unique device number of the mobile devices and card identifiers such as IMEI number or IP address do not represent a pseudonym.[414]

c) Identified data

Despite the controller's obligation to demonstrate that is in a position to identify the mHealth app user, the user is also obliged to provide information that will enable his identification, for instance, usernames and passwords, or pin codes sent to the phone number provided during the registration or answer to previously chosen question. If the

---

[412] Article 29 WP, Opinion on apps on smart devices, WP202, Adopted on February 2013, page 25.

[413] Article 12, para. 2, GDPR.

[414] Orientierungshilfe zu den Datenschutzanforderungen an App-Entwickler und App-Anbieter,Bayerisches Landesamt für Datenschutzaufsicht, 16 June 2014, page 11.

controller has reasonable doubts about the identity of a mHealth apps user, it can request further information to confirm the data subject's identity.[415] In fact, this is very important for apps that process sensitive health data, in order to prevent data leakage to third parties. Nevertheless, verifying the correct identity should not lead to an additional, excessive collection of personal data about the data subject.[416]

d) Multi-data subjects

In general, data 'concerning him' should not be interpreted very restrictively, for the reason that it might include data from several other people. For example, let us take an running app. It measures the steps of the user but also it compares his running achievement with the successes of other users in the group. Therefore, it contains personal data concerning multiple people. In this case, based on data portability requests, the mHealth app user should be able to have these data concerning other people provided to him since it also includes his data. Exactly this kind of situation has raised red flags during the negotiation process, as it was characterised as difficult or impossible to exercise this right in 'multi-data subject' cases, Since some of these might not necessarily agree or even be known or contacted regarding the exercise of their right to data portability.

The Article 29 WP suggested that this be solved based on Article 13(2)(b)[417] 'the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability'.[418] This means at the time when personal data are obtained controller should inform the mHealth app user about the existence of data portability request, which involves his personal data. This legal obligation arises

---

[415] GDPR, Article 12(6).

[416] Article 29 WP, Opinion on apps on smart devices, WP202, Adopted on February 2013, page 25.

[417] Articles 13(2)(b) 'the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability.

[418] Article 29 WP, Guidelines on the right to data portability, Adopted on 13 December 2016, As last Revised and adopted on 5 April 2017, page 13.

from Article 14(2)(c)[419], and relates to data that have been not obtained from the data subject. In such a case the information should be provided: (a) within a reasonable time not exceeding one month after obtaining the data, (b) during a first communication with the data subject, or (c) when disclosure is made to third parties.[420] However, if, data concerning the mHealth app user obtained without prior user's information or from third parties qualifies as 'concerning him' and fall within the scope of the right to data portability is an open question.

4.1.1.2 Provided data

The other sub-condition is data provided to a data controller. The GDPR does not provide any clarification on the 'provided data', so most probably the Article 29 WP embraced a combined taxonomy of personal data from the World Economic Forum[421] and OECD privacy expert discussion.[422] The taxonomy of OECD categorised personal data into four groups (1) provided (2) observed (3) derived and (4) interfered data 'according to the manner in which they originate', while WEF categorised personal data only in three groups: (1) provided (2) observed and (3) interfered data. Unlike the OECD and WEF, the Article 29 WP distinguished only two types of data. The first one is observed data, which incorporates provided and observed data. The second type is interfered and derived data.

---

[419] Article 14(2)(c): 'the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject and to object to processing as well as the right to data portability'.

[420] Article 29 WP, Guidelines on the right to data portability, adopted on 13 December 2016, as last Revised and adopted on 5 April 2017, page 13.

[421] World Economic Forum 'Rethinking Personal Data: A New Lens for Strengthening Trust', May 2014, page 16.

[422] Working Party on Security and Privacy in the Digital Economy, OECD privacy expert roundtable, Protecting Privacy in a Data-driven Economy: Taking Stock of Current Thinking 21 March 2014, page 5 http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=dsti/iccp/reg(2014)3&doclanguage=en.

a) Observed data

To delimit, within the scope of RDP falls only data that has been provided actively and knowingly and observed data, during the use of the app. In other words, provided actively and knowingly, would mean that the app user is generally aware of the process and data is voluntary provided 'by him'.[423] To clarify, such data could be, for example, email address, username, age or weight, or caloric intake. Sometimes, some apps require a user to write down the calories of the food. On the other hand, observed data is 'about him',[424] or raw data provided during the use of the app, for example, activity measures (steps, running), health measures or location data.

The issue of 'observed data' has been one of the most controversial aspects of the guidelines. The European Commission has expressed its concern that the Article 29 WP has interpreted too broadly the scope of the data portability by adding 'observed data' next to actively and knowingly,[425]since the article clearly states only 'provided data'. The response to this comment by the Article 29 WP is that 'provided by' should be interpreted more broadly, including the observed data in order to meet the policy objectives and to give a full value of the right to data portability.[426] As explained in the footnotes of their Opinion on portability, 'By being able to retrieve the data resulting from observation of his or her activity, the data subject will also be able to get a better view of the implementation choices made by data controller as to the scope of observed data and will be in a better situation to choose what data he or she is willing to provide to get a similar service, and be aware of the extent to which his or her right to privacy is respected'.[427] The

---

[423] World Economic Forum 'Rethinking Personal Data: A New Lens for Strengthening Trust', May 2014 page 16.

[424] World Economic Forum 'Rethinking Personal Data: A New Lens for Strengthening Trust', May 2014, page 16.

[425] European Commission, experts uneasy over WP29 data portability interpretation, The Privacy Advisor, Published April 2017, https://iapp.org/news/a/european-commission-experts-uneasy-over-wp29-data-portability-interpretation-1/.

[426] 'Guidelines on the right to data portability' by Article 29 Working Party, Adopted on 13 December 2016, As last Revised and adopted on 5 April 2017, p. 10.

European Data Protection Supervisor shared the same opinion 'in order to be effective, the right to data portability must have a wide scope of application, and not only be applied to the processing operations that use data provided by the data subject'.[428]

b) Inferred data

What is not considered as provided data, and therefore does not fall within the scope of the right to data portability is inferred data and derived data. These data refer to the results of the algorithm, but still, there is a slight difference between them. Interfered data is based on probability-based analytic processes, whereas derived data is based on simple reasoning and basic mathematics to identify patterns. Some scholars explained inferred data as 'descriptive data about the individual's past or present life, inferred by an app via data mining or combination of raw data'. This can include data regarding past illnesses, sexual activity, addictions, consumption habits, and family status. In addition, it entails information produced from other data and referent to an individual's future life, such as individual life expectancy or future illnesses.[429] What does this mean for the mHealth app user in the context of right to data portability? It means that the app user can transfer raw data about his activity or results from the observation of his individual behaviour, but not analysis of that behaviour, such as personalisation, recommendation for improving wellbeing or a healthier lifestyle, or profiling.[430]

In fact, inferred data is the most important for app users since it might reveal the quantity and quality of personal data that are combined in their personal profiling. Additionally, inferred data could present a risk for discrimination, for instance, if health apps share

---

[427] 'Guidelines on the right to data portability' by Article 29 Working Party, Adopted on 13 December 2016, As last Revised and adopted on 5 April 2017, Footnote p.10

[428] EDPS recommendations on the EU's options for data protection reform, (2015/C 301/01), footnote page 8.

[429] Malgieri, Gianclaudio and Comandé, Giovanni, Sensitive-By-Distance: Quasi-Health Data in the Algorithmic Era (May 2, 2017). Information, Communication and Technology Law, Issue n. 3, 2017 (Forthcoming), page 3, available at SSRN: https://ssrn.com/abstract=3020628.

[430] 'Guidelines on the right to data portability' by the Article 29 Working Party, Adopted on 13 December 2016, As last Revised and adopted on 5 April 2017, p. 9.

their inferred data with other businesses (banks, insurance companies, etc.) or if they use such data directly by selling profiles or targets.[431]

This blurred concept of 'provided data' might be a significant obstacle for app users in exercising their RDP, due to the difficulty for an average app user to delimit the diverse levels of provided data. Yet, in this case, the data subject can exercise the right to access[432] or the right to automated individual decision making[433] to find out the significance and the consequences of such processing, as well as the logic involved behind the profiling. In reality, most probably, this will also be limited, partially due to app company/developer intellectual property rights and trade secret protection or a lack of algorithmic transparency.[434] The reasoning behind limiting the scope of the right to data portability only to provided and observed data, lay in the fact that the legislators needed to balance the interest between users and controllers or app companies.

4.1.2 Legal grounds for processing data

In order for processing of personal data by the data controller to be considered lawful, Article 6 of the GDPR states that it must be grounded at least on one of the following bases: (a) consent, (b) contract, (c) legal obligation, (d) to protect a vital interest, (e) for the public interest, or (f) for legitimate interests. Apart from processing based on consent, all other legal grounds allow processing of data only when it is necessary for a specific context.[435] To put it differently, consent as legal ground focuses on the self-determination of

---

[431] Malgieri, Gianclaudio and Comandé, Giovanni, Sensitive-By-Distance: Quasi-Health Data in the Algorithmic Era (May 2, 2017). Information, Communication and Technology Law, Issue n. 3, 2017 (Forthcoming), page 3, available at SSRN: https://ssrn.com/abstract=3020628.

[432] GDPR, Article 15.

[433] GDPR, Article 22: 'The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her'.

[434] Malgieri, Gianclaudio and Comandé, Giovanni, Sensitive-By-Distance: Quasi-Health Data in the Algorithmic Era (May 2, 2017). Information, Communication and Technology Law, Issue n. 3, 2017 (Forthcoming), page 4, available at SSRN: https://ssrn.com/abstract=3020628.

[435] Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, WP 217, Adopted on 9 April 2014, page 13.

the data subject, whereas all other legal grounds are subject to safeguards and measures in situations where it is appropriate and necessary to process the data within a certain context in pursuit of a specific legitimate interest.[436]

It is worth noting that mHealth app user can exercise the right to data portability only if data has been provided based on consent or contract as legal ground. Meaning, if processing is based on one of the other grounds than the right to data portability does not apply. Interestingly, these limitations exclude from the scope of data portability, data processing necessary for the performance of a task carried out in public interest or in the exercise of official authority vested in the controller and legitimate interests (Article 6 (1f) of GDPR). Recital 68 of the GDPR explicitly excludes processing carried out in public interest, while legitimate interests are not mentioned. Our further discussion will be focused only on 'consent' and 'performance of the contract' as the legal basis for processing of personal data and exercising right to data portability.

a) Processing based on Consent

Consent as an idea is not solely a legal notion, but also has ethical, social and instinctual elements.[437] It makes people's daily activities unproblematic. In the GDPR, the notion of consent, as clarified in the Opinion of Article 29 WP, 'is traditionally linked with the idea that the data subject should be in control of the use that is being made of his data.' [438] In fact, the fundamental role of consent is underlined by Articles 7 and 8 of the Charter of Fundamental Rights of the European Union. Therefore, from a fundamental rights perspective, control exercised through consent that empowers data subjects is an important concept.

---

[436] *Id.*

[437] Eugenio Mantovani, Paul Quinn, mHealth and data protection – the letter and the spirit of consent legal requirements, Article in International Review of Law Computers & Technology March 2013, DOI: 10.1080/13600869.2013.801581
https://www.researchgate.net/publication/255825921_mHealth_and_data_protection_-_the_letter_and_the_spirit_of_consent_legal_requirements

[438] Article 29 WP Opinion 15/2011 on the definition of consent, adopted 13 July 2011, page 8.

It is seen as a tool that gives data subjects control over whether or not, to whom and when, their personal data will be processed. In other words, it presents a choice to accept or decline the offered terms. Most importantly, if the choice is to decline the offered terms then it should be without detriment. Otherwise, control based on consent becomes illusory[439] and will be an invalid and unlawful basis for processing.

In the light of the latest technological developments, the legal basis of consent is quite a problematic issue. It is perceived as an inappropriate and falsely claimed applicable ground.[440] First the consent as control might be a weak legal basis and lose its value when processing of data is extended to purposes not initially envisioned, especially having in mind, that the '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'.[441] Second, 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'.[442] Basically, in such a circumstance the elements that constitute valid consent are most likely not present, which practically weakens the position of the user.

Despite the comments and criticisms, in the context of the mHealth apps consent is the necessary legal ground to permit the mHealth app developer to lawfully collect information from the app user and consequently process personal data.[443] Subsequently, pro-

---

[439] Article 29 Working Party, Guidelines on consent under Regulation 2016/679, WP 259 rev.01, Adopted on 28 November 2017, as last Revised and Adopted on 10 April 2018, page 3.

[440] 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 adopted, 20.03.2016, p. 17.

[441] 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 adopted, 20.03.2016, p. 17.

[442] Article 29 WP, Opinion 15/2011 on the definition of consent, WP187, adopted 13 July 2011, page 10.

[443] However, during the usage of the app, the app developer may invoke other legal grounds for other types of data processing as long as this does not involve processing of sensitive personal data.

cessing of data should be based either on the users consent to the processing of his personal data for one or more specific purposes[444] or when it comes to special categories of personal data, the mHealth app user has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provides that the prohibition may not be lifted by the data subject.[445]

In any case for the purpose of this thesis, it is important first, to clarify the EU legal definition of consent and second, what constitutes valid consent.

So what actually is consent? In the GDPR, Art. 4(11) defines that the data subject's consent shall mean 'any *freely given*, *specific*, *informed* and *unambiguous* indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her'.

The wording of the definition emphasises that consent does not require a certain form, it just needs to be an indication of 'any' kind. Yet, Recital 32[446] provides examples of indication 'such as' a written statement, including by electronic means or an oral statement. In line with this reasoning, one can argue that it opens the possibility of a wide interpretation of the scope of such an indication. Actually, it could be any kind of act, such as a signal, gesture, indicating a data subject's wishes, which the controller needs to ensure it has obtained to be able to demonstrate that the data subject has given consent. This might be needed in a case of a withdrawal,[447] in the context of a dispute with a data subject, or as evidence in enforcement action.

Essentially, these are the four main elements for the consent to be valid. Further we will analyse them in the context of mHealth apps.

---

[444] GDPR, Article 6(1)(a).

[445] GDPR Article 9(2)(a)

[446] GDPR, Recital 32

[447] Article 29 WP Guidelines on consent under Regulation 2016/679, Adopted on 28 November 2017, as last revised and adopted on 10 April 2018, WP 259, page 20.

The first element is 'freely given'. Pursuant to Recital 42, consent should not be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment.[448] In other words, freely given means, consent will 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 does not consent.[449] Analysis of the paragraph 'freely given'[450] reveals the intention of the regulator to take a non-exhaustive approach by using the word 'inter alia'.[451] That means to be wider enough to respond to other situation that are currently not included in the wording, but in future might have element of inappropriate influence of the user consent. In line with this reasoning, Article 29 WP in their revised opinion on consent,[452] further clarify the most common reason when consent is not considered as freely given.

The first reason is an imbalance of power, for example between the public authorities and data subject. It is questionable if and when public authorities can rely on consent since there is an obvious imbalance of power. For instance, when people are applying for passport, they need to consent a photo and fingerprints to be taken. In fact, a passport is necessary for traveling in other non-EU countries, but that does not mean the consent is freely given, for taking photo or fingerprints. Indeed, the ECJ in the case *Schwartz v. Stadt Bochum*,[453] emphasised when people are applying for passport they cannot be

---

[448] GDPR Recital 42.

[449] Article 29 WP Opinion 15/2011 on the definition of consent, adopted 13 July 2011, page 12.

[450] GDPR, Article 7 (4) 'When assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract'.

[451] Article 29 WP Guidelines on consent under Regulation 2016/679, Adopted on 28 November 2017, as last revised and adopted on 10 April 2018, WP 259, page 5.

[452] Article 29 WP Guidelines on consent under Regulation 2016/679, Adopted on 28 November 2017, as last revised and adopted on 10 April 2018, WP 259, page 6.

[453] Judgment of the Court (Fourth Chamber), Case C-291/12, Michael Schwarz v Stadt Bochum, 17 October 2013, para. 32.

deemed to have freely consented to have their fingerprints taken, because people need a passport.

The same can be concluded in an employment context. It cannot be expected that consent will be freely given due to the fears of the employees for their financial stability. Nevertheless, this does not totally exclude consent as a legal basis for processing of data in the context of public authorities or employment context.[454]

Does this mean that consent is freely given, for example, when wearable devices are given to the employees in order to track and monitor their health and activity during and out of the working hours? In the last years, the trend in some companies is to oblige their employees to use lifestyle and well-being apps, in order to deliver data-driven insights into their lives and to create a more productive workforce.[455] As some argue, healthy workers perform better.[456] It is worth noting that consent as a legal base for use of mHealth apps and wearables in the employment context is unlawful. First, because this involves processing of health data which is prohibited based on Article 9, except if one of the exceptions apply. Second, even though one of the exceptions apply, 'explicit consent', it is highly unlikely that will be legally valid since it cannot be considered as 'freely given', mostly due to the unequal position between the employer on one hand and the employees on the other hand. In theory, employees are able to refuse to consent but due to their financially dependence,[457] they might have financial losses.

The second reason is conditionality. It entails situations when the consent of the mHealth app user is 'bundled' with acceptance of the terms and conditions, or is 'tying' the provision of a contract or a service to ask for consent to process data not necessary for the per-

---

[454] Article 29 WP Opinion 2/2017 on data processing a work, Adopted 2017, WP 249, page 6.

[455] 'These companies are tracking the fitness of their employees', Guardian Monday 17 March 2014 https://www.theguardian.com/technology/2014/mar/17/why-companies-are-tracking-the-fitness-of-their-employees.

[456] de Korte EM, Wiezer N, Janssen JH, Vink P, Kraaij WEvaluating an mHealth App for Health and Well-Being at Work: Mixed-Method Qualitative Study JMIR Mhealth Uhealth 2018;6(3):e72.

[457] Articcle 29 WP Opinion 2/2017 on data processing at work, WP249, Adopted on 8 June 2017, page 18.

formance of the contract or a service.[458] For instance, a running app may ask the user to consent to allow a third-party online shop to use his data for marketing purposes. Processing of personal data for marketing purposes, in fact is not necessary for the performance of the contract, since the app only counts steps and running trajectory. In such a case if the user is denied continued use of the app, solely for the reason that he did not consent, then the consent cannot be freely given. The intention of the legislators to emphasise 'conditionality' as one of the reasons that undermine the meaning of freely given consent, and that its occurrence must be carefully examined. Essentially, this requires first delimiting a clear line between the consent and the contract as legal bases for processing data, since they cannot be blurred or merged. Second, it requires determining the scope of the contract, and strictly interpreting the meaning of data 'necessary for the performance of the contract. Otherwise, existence of the conditionality is perceived as an obstacle that limits mHealth app user choices.

The third reason that might restrict freely given consent is lack of 'granularity'.[459] For instance, granularity exists when the service involves multiple processing operations for more than one purpose, which according to Recital 43 would require user to consent to each separate purpose. If this is not the case and the user can not choose which purpose he accepts, then the consent is not freely given.

The fourth reason that might restrict freely given consent is if the refusal or withdrawal of the consent is followed by disadvantages or 'detriment' such as deception, intimidation, or coercion.[460] For example, the performance of the mHealth app is downgraded or limited solely for the reason that user after some time of usage of the app, withdraws their consent for processing of data not necessary for the app to work but is useful for the app developer to learn more about the user. Withdrawal, in this context, is seen as a way

---

[458] Article 29 WP Guidelines on consent under Regulation 2016/679, Adopted on 28 November 2017, as last revised and adopted on 10 April 2018, WP 259, page 8.

[459] Article 29 WP Guidelines on consent under Regulation 2016/679, Adopted on 28 November 2017, as last revised and adopted on 10 April 2018, WP 259, page 10.

[460] *Id*.

of exercising control.[461] It is not retroactive, but it should prevent any further processing of the individual's data by the controller.

The second condition is 'specific', and its aim is to guarantee a degree of users control and transparency. The consent will be considered specific if it refers clearly and precisely to the scope and the consequences of the data processing. What does it mean? For instance, it should be given in relation to one of more specific purposes. It cannot apply to an open-ended set of processing activities.[462] In such a way 'purpose specification' is understood as a safeguard against function creep. Basically, it is a tool to prevent gradual widening or blurring of initial purposes for which the data is processed, after a data subject has consented. Put differently, if the app developer needs to process the data for a different purpose then he needs to ask the mHealth app user for additional consent. Based on the 'granularity consent requests', this would mean asking the user to consent for various different purposes in a separate opt-in for each purpose, understandably by providing specific information for each separate consent request, and the impact of the different choices they have.

In the context of mHealth apps, according to the European Commission, the recommended method for gaining consent for health apps is granular consent:

> This advice also applies to all other apps that require access to personal data: Consent should be obtained using the most effective means to communicate with users. Granular consent, in which consent is sought during various stages of the use of the application, with additional consents being sought when a user uses the app in a new manner, can be considered a good practice if this permits the user to exercise better or more effective control over his or her personal data. Thus, consents can be obtained when installing it or at various times during use, as long as consent is obtained before processing begins.[463]

The third element of valid consent is 'informed'. It means mHealth app user prior to consenting should be provided with information, such as the identity of the controller and

---

[461] Article 29 WP Opinion 15/2011 on the definition of consent, Adopted 13 July 2011, page.9

[462] *Id.*, page 17.

[463] 'Draft code of conduct on privacy for mobile health applications', European Commission, 2016 page 6

the purposes of the processing for which the personal data are intended, what type of data will be collected and used, the existence of the right to withdraw consent, information about the use of the data for automated decision-making and data transfers. All this information is necessary for the user to make an informed decision. Otherwise, it is considered that violates the Data Protection Rules, as has been the case with the Nike running app.[464]

The text of the consent should be provided in any form easily accessible, using clear and plain language and it should not contain unfair terms.[465] It should be separate from other matters, for example contract, or terms and conditions. In any case, silence, pre-ticked boxes or inactivity does not constitute consent. If the processing has multiple purposes, consent should be given to all of them.

In other words, in the context of apps, as explained by Article 29 Working Party in its opinion on apps on smart devices,[466] 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. It means the information must be provided before the processing; otherwise, it is not deemed sufficient and is legally invalid.

Yet, in practice, this information is presented during the installation of the app, or in some cases, there are clauses that claim that by installing, using or accessing the mHealth app the user accepts the terms. Actually, this is not acceptable and is considered unlawful. The mHealth app user must be informed which data are being processed and why in a clear and plain language before downloading the app. This is highly relevant for the mHealth app users, especially, considering the range of sensors and data the apps have access to. Additionaly it should contain information whether the data may be reused by other parties, and if so, for what purposes.

---

[464] Nike ends privacy violations in running app after investigation by Dutch DPA, Dutch Data Protection Authorities, November 2016, https://autoriteitpersoonsgegevens.nl/en/news/nike-ends-privacy-violations-running-app-after-investigation-dutch-dpa.

[465] GDPR Recital (42).

[466] Article 29 WP, Opinion on apps on smart devices, page 22.

Other requests that fall under 'informed' is that mHealth app user also needs to know who is legally responsible for the processing of their personal data and how the controller can be contacted. For example, to have a contact person if they would need to exercise their rights, such as the right to access, right to erasure or right to data portability. Having in mind the fragmented nature of the app ecosystem, which includes app developers and other parties involved in the processing of personal data through the app, having a single point of contact is essential for the users.

The fourth element of valid consent is 'unambiguous'. For consent to be unambiguous, the procedure to seek and to give consent must leave no doubt to the user's intention. In other words, 'the indication by which the mHealth user signifies his agreement must leave no room for ambiguity regarding his intent'.[467] As Article 4(11) states, valid consent requires an unambiguous indication by means of statement or by a clear affirmative action. The need to act requires that the mHealth app user must 'signify' his consent. It implies that silence or simply inaction is insufficient and some sort of action is required to constitute consent. However, any action in terms of merely proceeding with service is not considered as active indication of choice. This action can be a written statement, or in the context of online activities and apps, would mean ticking a box when visiting a website or downloading a mHealth app. In any case should be visible and available to the data subject but not unnecessary disruptive.[468] Other acceptable acts that signifies consent is an oral statement or other statement or conduct which clearly indicates that users consent to the proposed processing data.

Yet, it is worth noting that the notion of 'indication' in the context of mHealth apps should be interpreted in another way, especially, when consent is needed for processing of special categories of data. Principally, the consent needs to be explicit, meaning that just 'any…indication' is not enough in order to legitimise the processing of data, for the reason that consent is seen as a possibility to legitimise the processing of sensitive data, which would otherwise be prohibited. Basically, this imposes a higher standard for

---

[467] Article 29 WP Opinion 15/2011 on the definition of consent, adopted 13 July 2011, page 21.

[468] Article 29 WP Guidelines on consent under Regulation 2016/679, adopted on 28 November 2017, as last revised and adopted on 10 April 2018, WP 259, page 16.

obtaining the consent, as this consent must be 'explicit' and go beyond the general standard of consent. In legal terms, 'explicit consent' is understood as having the same meaning as express consent. Put simply, explicit or express consent means positive active response, written or oral. 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. It is usually given in writing with a hand-written signature.[469] However, in the online context, explicit consent might be obtained by filing in an electronic form, by sending an email, by uploading a scanned document carrying out the signature of the data subject or by using an electronic signature.[470]

Having in mind the four elements of valid consent, one might say that users are having a hard time. Why? Daily, they are faced with multiple consent requests that need consenting through clicks and swipes. This causes a certain degree of click fatigue, which means after some point of time they are not even reading the consent requirement. Apart from this, some terms are very difficult to read as they are very long, ambiguous or written in overly technical, complex or vague language. Consequently, to give an informed consent is not possible for most of the users. Even though the idea of 'informed and unambiguous consent' is to provide the app users with control of their data, in reality, they only give the user a false feeling of control.

Indeed, interesting research on the topic of 'apps and valid informed consent' has been conducted by the Norwegian Consumer Council.[471] They found out that in average the user needs to read 250,000 words before consenting. This means 'the current state of terms and conditions for digital services is bordering on the absurd. Their scope, length

---

[469] Article 29 WP Opinion 15/2011 on the definition of consent, adopted 13 July 2011, page 25.

[470] Article 29 WP Guidelines on consent under Regulation 2016/679, Adopted on 28 November 2017, as last revised and adopted on 10 April 2018, WP 259, page 18.

[471] Norwegian Consumer Council, Research '250,000 words of app terms and conditions' - Published 24. May 2016 https://www.forbrukerradet.no/side/250000-words-of-app-terms-and-conditions/.

and complexity mean it is virtually impossible to make good and informed decisions.'[472] Moreover, many apps have generally unclear and complicated terms dominated by hypothetical languages, such as 'may' and 'can', making it difficult for the user to understand what the app will do.[473]

Discussion relating to consent and mHealth apps, inevitably, tackles the ePrivacy Directive.[474] Especially Article 5(3), which prescribes that:

> storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned has given his or her consent, having been provided with clear and comprehensive information, in accordance with Directive 95/46/EC, inter alia about the purposes of the processing. (…)'

In fact, this article as well as the ePrivacy Directive has a wider scope and relates to any entity that stores or access data from the smart phones, irrespective of whether it is personal data or not. However, considering the discussion in Chapter 3, various types of data stored on or generated by a smart device on which mHealth apps are installed are considered as personal data, meaning they are part of the private sphere of the users requiring protection under the European Convention for the Protection of Human Rights and Fundamental Freedoms.[475]

As we have said, in the context of mHealth apps consent is a principal applicable legal ground. Yet, it is worth noting that there is a difference between, on one hand, the con-

---

[472] Said Digital Policy Director Finn Myrstad at the Norwegian Consumer Council.Norwegian Consumer Council, '250,000 words of app terms and conditions' - Published 24 May 2016 https://www.forbrukerradet.no/side/250000-words-of-app-terms-and-conditions/.

[473] APPFALL 'Threats to Consumers in Mobile Apps' Report of the Norwegian Consumer Council March, 2016 page 4 https://fil.forbrukerradet.no/wp-content/uploads/2016/03/Appfail-Report-2016.pdf.

[474] The ePrivacy directive (2002/58/EC, as revised by 2009/136/EC). In January 2017 is adopted Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) Brussels, 10.1.2017 COM(2017) 10 final 2017/0003 (COD).

[475] Recital 24 ,ePrivacy Directive (2002/58/EC, as revised by 2009/136/EC).

sent required to store or gain data from the device (ePrivacy), and, on the other hand, the consent necessary to have a legal ground for the processing of different types of personal data (GDPR). As elaborated, both consent requirements are simultaneously applicable, but each are based on a different legal basis.[476] For instance, consent based on the ePrivacy Directive will be necessary if the mHealth app needs access to the data already stored on the smart phone, such as contacts, photos etc. On the other hand, consent based on Article 6(1) of the GDPR, will be needed for the running app to process data such as steps or running trajectory.

Fundamentally, in both cases, the consent should fulfil the same elements necessary to be considered valid, such as 'freely given', 'specific', 'informed 'and 'unambiguous' as prescribed in Article 4 (11) of the GDPR. Thus, it creates an opportunity for the two types of consent to be combined in practice.

Consent as a legal ground has an important role, but this does not exclude the possibility, depending on the context, of other legal grounds to be more appropriate either from the controller's or from the data subject's perspective.

b) Processing based on Contract

Despite the consent as a legal ground to ask for data portability, another legal ground for the processing of data is based on a contract, meaning the processing of data is 'necessary for the performance of a contract to which the data subject is a party or in order to take steps at the request of the data subject prior to entering into a contract'.[477] Drawing from Article 6(1b), one may conclude that this legal basis consists of two different situations. First when processing is 'necessary for the performance', and second 'prior to entering into a contract'. The focus of our discussion will be concentrated only on the first situation.

---

[476] Article 29 WP, Opinion 02/2013 on apps on smart devices, WP202 , Adopted on 27 February 2013, page 14

[477] GDPR, Article 6 (1b).

An example for the first situation is if a user consents to the installation of a running app. In order to fulfil a request to count how many steps and to locate the trajectory, the app does not have to ask for the separate consent of the user to count his steps and to disclose his location. This disclosure is strictly necessary in order to perform the contract with this specific user, and therefore the app has a legal ground in Article 6 (1b) of the GDPR. The same reasoning applies for example regarding communication apps. The app user needs to provide essential information such as an account name, e-mail address or phone number to another individual if he wishes to communicate with. Therefore, the disclosure is obviously necessary to perform the contract.

The Article 29 WP is of the opinion that 'necessary' needs to be interpreted very strictly, further clarifying that this does not cover situations when processing is not genuinely necessary but is rather imposed by the data controller on the data subject. In other words, this will be a situation when the app is collecting additional data that is not necessary for the performance of the contract. In the context of a running app, it will be the case if the app, beside steps and location data, is collecting data about contacts from the address book. This data is obviously not 'necessary' for the performance of the contract.

Striking the line between being considered, and not considered as 'necessary' for the performance of a contract in the mHealth app context will be difficult and sometimes certain situations will be on the borderline. Therefore 'necessary' should comply with the 'purpose limitation' as one of the main principals relating to the processing of personal data. The right to data portability also applies in the context of employee data only if the processing is based on a contract to which the data subject is a party.[478]

4.1.3 Rights and freedom of other users

As can be concluded from the discussion, right to data portability is not isolated right, but mostly is complemented or contradicted by other rights arising from the GDPR or other Directives. Thus, the intent of this paragraph is to avoid the situation where other

[478] Article 29 WP, Guidelines on the right to data portability, adopted on 13 December 2016, As last Revised and adopted on 5 April 2017, page 9.

users might be prevented from exercising their rights as data subjects under the GDPR, such as but not limited to the right to access or right to be forgotten.[479]

Basically, exercising the right to data portability, in other words, receiving and transferring of personal data, should not affect the freedom and rights of other data subjects.[480] Let us clarify what this means. For example, in the first case, if the user of the mHealth running app would like *to receive* or download his personal data, it is possible that this data set contains data about other users. By other users, we mean those with whom he is competing to achieve better health or activity goals. Receiving other users personal data as part of the data portability request, is allowed only to the extent that the data are kept under the sole control of the requesting mHealth app user. Put differently, received or downloaded data should be used solely in terms of purely personal or household needs.[481]

The second case is if the user of the mHealth running app would like *to transfer* his personal data from one app to other, this data set might contain data about other users. In such a case the new app controller is not allowed to process the transferred data for any other purposes, for example for marketing purposes, or to enrich the profile of the third-party data subject and rebuild his social environment, without their knowledge and consent. Otherwise, this will be considered as unlawful and unfair, especially if the users concerned are not informed and cannot exercise their rights as data subjects.

What happens after receiving or transferring the data based on RDP? Can the mHealth app user continue using the app or will he have the right to be forgotten? Actually, yes, it should be clear that the portability of data does not automatically mean that data will be reassured after it is transferred. On contrary, the user can still continue using the mHealth app, despite the request to receive or transfer the data. Even, later on, if the data subject would like to exercise his right to be forgotten then right to data portability should not be

---

[479] Article 29 WP, Guidelines on the right to data portability, Adopted on 13 December 2016, As last Revised and adopted on 5 April 2017, page.11

[480] *Id.*

[481] *Id*., page 12.

seen as an obstacle. On the other hand, it does not impose obligations on the controllers to retain the data for a longer period than is necessary, beyond any specific retention period or to delay and refuse erasure.[482] Moreover, the mHealth app user can also exercise the right to access (Article 15) if he finds out that personal data requested under the right to data portability does not fully address his request.

In line with the rights and freedoms of other, the right to data portability does not apply to 'processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller'.[483] Although it does not seem logical for the right to data portability to be exempted, especially, having in mind the initiative in the EU for re-use of data as a pre-request to strengthen the EU data economy.[484] Yet a closer look at the proposal for a revision of the re-use of public sector information Directive,[485] also known as the 'PSI Directive' put emphasis on the economic aspects of the re-use of data rather than on access to data by citizens. In addition, it mentions protection of personal data as one of the reasons for when the Directive does not apply.[486]

Consequently, analysis of the legal limitation of the right to data portability reveals how complex this right is. First, in order to understand what is entailed by 'provided by' and what 'necessary for the performance of the contract' means, apart from the legal knowledge requires substantial technical knowledge. Second, it is questionable as to what extent will really strengthen user control, considering the limited interpretation of 'provided data' and the burden of the data subject to prove his identity if the date has been pseudonymised. Third, the wording as some argue is too restrictive, because it does

---

[482] 'Guidelines on the right to data portability' by Article 29 Working Party, adopted on 13 December 2016, p. 6.

[483] GDPR Article 20(3).

[484] Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the re-use of public sector information (recast), Brussels, 25.4.2018, COM(2018) 234 final, 2018/0111(COD).

[485] On 25 April 2018, the European Commission adopted a proposal for a revision of the PSI Directive.

[486] Article 1 para. (2) (cc) and Recital 21 of the DIRECTIVE 2003/98/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 17 November 2003 on the re-use of public sector information.

not cover situations where the controller has illegally processed the data.[487] For example, data that is processed without the data subject's knowledge, more precisely without valid consent, which might be the case with some mHealth apps. Generally speaking, applicability of the right to data portability in the mHealth apps context should be based on a case by case approach.

5.1 Technical limitations

5.1.1 Processing carried out by automated means

Taking into account that the debate surrounding the right to data portability arose in the context of online activities, it seems logical that only data carried out by automated means falls within the scope.[488] This means it does not cover paper files. Having in mind Chapter 2, where we explained the technical functioning of the apps, it can be concluded that processing of personal health data by the app is considered as processing carried out by automated means.

Based on the legal analysis from the previous section the right to data portability consists of two rights, 'to receive' and 'to transfer' the data. In both cases from the technical point of view data controllers are responsible to provide the data to the data subjects or to other data controllers by:

– a direct transmission of the overall dataset of portable data, or

– an automated tool that allows the extraction of relevant data.[489]

Basically, the moment of transfer of data, is considered as moment of transferring the accountability. To illustrate that in fact the controller that is answering the request for data portability and is transferring the data to others, it is not responsible for the handling of

---

[487] Data Portability - A Tale of Two Concepts, Prof. Dr. Ruth Janal, JIPITEC – Journal of Intellectual Property, Information Technology and E-Commerce Law 8 (2017) JIPITEC 59 para 1. https://www.jipitec.eu/issues/jipitec-8-1-2017/4532.

[488] The right to Data portability in the context of the EU data protection reform, Gabriela Zanfir, International Data Privacy Law Advance Access, published May 11, 2012.

[489] Article 29 WP, Guidelines on the right to data portability, 5 April 2017, 16/EN WP 242 rev.01, page 16.

data by the other controller or by the data subject.[490] Moreover the receiving data company is the new data controller, which is responsible regarding the new data processing, meaning before the transfer of the data takes place, it is its obligation to clearly state the purpose of the new processing.

If portability includes a data set that is broader than the purpose, they must limit the processing on data necessary for the purpose and delete the unnecessary data.[491] The other safeguard is that the data subject initiating the transfer of the data needs to give consent or sign a contract with the new data controller.[492] The new data controller should perform the data processing under its responsibility. According to Article 5(1)(f) of the GDPR, it should guarantee the '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'. Besides, it should apply the principles laid down in Article 5, such as lawfulness, fairness and transparency, purpose limitation, data minimisation, accuracy, integrity and confidentiality, storage limitation and accountability.

5.1.2 Structured, commonly used, machine-readable and interoperable

The discussion in the previous section has been mostly about what is the right to data portability, what it entails and the conditions for exercising the right. It can be concluded that obstacles for exercising this right can be legal, financial or technical in nature.[493] In the author's opinion, the most substantial condition for successfully exercising the right to data portability, after its current legal interpretation, is actually interoperable data formats. In other words, data subject can fulfil all necessary legal requirement to exercise the right to data portability, but if the data format is not adequate which means the

---

[490] 'Guidelines on the right to data portability' by Article 29 Working Party, 5 April 2017, 16/EN WP 242 rev.01., p. 5.

[491] 'Guidelines on the right to data portability' by Article 29 Working Party, adopted on 13 December 2016, p. 6.

[492] *Id.*, p.9

[493] *Id.*, page 15.

receiving system is not technically capable to receive the incoming data, it presents a major obstacle for transferring the data to another controller. In fact, according to GDPR data must be provided without hindrance in a structured, commonly used and machine-readable[494] format. The text of the Regulation does not set out specific standards for the reason that it would not serve the need for technological neutrality as it would be difficult to reconcile it with future technological developments.[495] Meaning it is up to each sector or industry to apply the format commonly used.

In line with this paragraph, Article 29 WP in the Guidelines for data portability clarifies that 'structured', 'commonly used' and 'machine-readable'[496] are a set of minimal requirements that should facilitate the interoperability of the data format provided by the data controller[497].

In fact, some clarification on the format has been provided in the Directive 2013/37/EU on the re-use of public sector information, whereas Recital 21 defines machine-readable format as:

> a file format structured so that software applications can easily identify, recognise and extract specific data, including individual statements of fact, and their internal structure. Data encoded in files that are structured in a machine-readable format are machine-readable data. Machine-readable formats can be open or proprietary; they can be formal standards or not. Documents encoded in a file format that limits automatic processing, because the data cannot, or cannot easily, be extracted from them, should not be

---

494 GDPR, Article 20(1), April 2016.

495 Council of the European Union, Interinstitutional File: 2012/0011 (COD), Working Group on Information Exchange and Data Protection (DAPIX), 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)- Data Portability (Revision of Article 18) Brussels, 6 June 2014, 10614/14, page 2, http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%2010614%202014%20INIT.

496 Data in a data format that can be automatically read and processed by a computer, such as CSV, JSON, XML, etc. Machine-readable data must be structured data. Compare human-readable. http://eur-lex.europa.eu/eli-register/glossary.html.

497 'Guidelines on the right to data portability' by Article 29 Working Party, Adopted on 13 December 2016, p. 13.

> considered to be in a machine-readable format. Member States should where appropriate encourage the use of open, machine-readable formats'.

However, if no specific format is in common use within the industry or sector, as UK ICO[498] suggests, the personal data should be provided using open formats such as .CSV, .XML and JSON. As explained, these formats are the easiest to use when answering data portability requests.

CSV stands for 'Comma Separated Values'. It is defined by the Open Data Handbook as 'a standard format for spreadsheet data. Data is represented in a plain text file, with each data row on a new line and commas separating the values on each row. As a very simple open format, it is easy to consume and is widely used for publishing open data.' CSV is used to exchange data and is widely supported by software applications. Although CSV is not standardised, it is nevertheless structured, commonly used and machine-readable and is, therefore, an appropriate format for responding to a data portability request.[499]

XML stands for 'Extensible Markup Language'. It is defined by the Open Data Handbook as: 'a simple and powerful standard for representing structured data.' It is a file format that is intended to be both human-readable and machine-readable. Unlike CSV, XML is defined by a set of open standards maintained by the World Wide Web Consortium ('W3C'). It is widely used for documents but can also be used to represent data structures such as those used in web services. This means XML can be processed by APIs, facilitating data exchange. For example, the company may develop or implement an API to exchange personal data in XML format with another organisation. In the context of data portability, this can allow transmitting personal data to an individual's personal data store, or to another organisation if the individual has asked.

JSON stands for 'JavaScript Objection Notation'. The Open Data Handbook defines JSON as: 'a simple but powerful format for data. It can describe complex data structures, is highly machine-readable as well as reasonably human-readable, and is independent of

---

498 UK ICO, The Guide to the General data protection regulation , Right to data portability, https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/?template=pdf&patch=42#link25.

499 *Id*.

platform and programming language, and is, therefore, a popular format for data interchange between programs and systems.' It is a file format based on the JavaScript language that many websites use and is used as a data interchange format. As with XML, it can be read by humans or machines. It is also a standardised open format maintained by the W3C.[500]

The RDF or 'Resource Description Framework' format is also a structured, commonly-used, machine-readable format. It is an open standard published by the W3C and is intended to provide interoperability between applications exchanging information.

Recital 68 of the GDPR further explains that this format should be interoperable only if technically feasible,[501] specifying that controllers do not have obligations to adopt or maintain processing systems that are technically compatible. It is evident that the GDPR does not impose specific recommendations on the format. Most probably, because the most appropriate format will differ across sectors where adequate formats may already exist. In this case, the controller may fulfil the portability requirement by providing the data in the format presently used.[502] Therefore, data controllers are only encouraged to develop interoperable formats that enable data portability. What this means for mHealth app user, interoperability and the complexity of this term will be discussed in the next Chapter.

4 Conclusion

This chapter discussed the right to data portability. It is one of the newly introduced rights in the GDPR, whose aim is to give users control over their personal data. The control means two possibilities for the users '**to receive'** their personal data which he or she

---

[500] UK ICO, The Guide to the General data protection Regulation, Right to data portability, https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/?template=pdf&patch=42#link25

[501] Article 20, para. 2.

[502] Data Portability - A Tale of Two Concepts, Prof. Dr. Ruth Janal, JIPITEC – Journal of Intellectual Property, Information Technology and E-Commerce Law 8 (2017) JIPITEC 59 para 1. https://www.jipitec.eu/issues/jipitec-8-1-2017/4532.

has provided to a controller or the right **'to transmit'** those data to another controller without hindrance from the controller to which the personal data have been provided. The first one 'to receive' means that users of lifestyle and wellbeing apps can download or receive all the personal data they provided to the app, such as steps, calorie intakes or other health parameters, and further reuse them. The second, 'to transmit' means the possibility to transfer personal data from one controller to another controller 'without hindrance', for instance to another controller that offers better, cheaper and more privacy-friendly service.

In both cases three conditions should be fulfilled in order to be able to exercise the right to data portability. The first condition is data to be provided by the data subject. In fact, the first condition includes three sub-conditions. 1) Only personal data concerning the subject, provided to the controller. 2) It includes data that has been provided actively and knowingly or observed data, meaning during the use of the service or device, for instance email, username, age or weight, or calorie intake. However, it does not include data that refer to the results of an algorithm. 3) Exercising the right to data portability should not affect the freedom and rights of other data subjects, in order to avoid a situation where third parties might be prevented from exercising their rights as data subjects under the GDPR, such as the right to information access.

The second condition is that processing should be based on consent or contract, as the legal basis for processing personal data. And the third condition is that processing should be carried out by automated means.

In any case, data controllers have the obligation to inform users about the existence of this new right through data portability policy, explaining to them the conditions under which they can exercise their right. The data portability policy should be written in a concise, transparent, intelligible and easily accessible form, using plain and clearly understandable language in order to be understood by people with the different educational backgrounds. It should explain the difference between the types of data that a data subject can receive based on the right to data portability and other rights. Answering the request for transferring the data should be 'without undue delay' and in any case 'within one month of receipt of the request' or within a maximum of three months for complex cases. The controller should process the request free of charge, since, it prohibits the data

controller from charging a fee for the provision of the personal data unless he can demonstrate that the requests are manifestly unfounded or excessive.

However, request for exercising the right to data portability might be rejected when the controller demonstrates that it is not in a position to identify the data subject. In such situations, the data subject should provide more information to enable his or her identification.

Yet, the most substantial condition for successfully exercising the right to data portability is actually data format, since as defined, data must be provided without hindrance in a structured, commonly used and machine-readable format. Why is the format the most important condition? Well, the data subject can fulfil the necessary legal requirement to exercise the right to data portability, but if the data format is not adequate, which means the receiving system is not technically capable to receive the incoming data, it is a major obstacle for transferring the data to another controller, and data would be useless for the user. On the issue of data format, the Article 29 WP in the Guidelines for data portability clarifies that 'structured', 'commonly used' and 'machine-readable' are a set of minimal requirements that should facilitate the interoperability of the data format provided by the data controller.[503] However, data controllers are not obliged to develop interoperability formats. In fact, this is a major obstacle that might jeopardise the idea of the right to data portability as a tool which should give users control over their personal data. In the next chapter, we will discuss the challenges arising from data interoperability between Health apps.

---

503 'Guidelines on the right to data portability' by Article 29 Working Party, adopted on 13 December 2016, p.13

CHAPTER 5: INTEROPERABILITY OF mHEALTH APPS IN DATA-DRIVEN ECONOMY

1. Introduction

This chapter will be devoted to the issue of data interoperability between mHealth apps in the data-driven economy. As concluded in the previous chapter, interoperability is one of the crucial conditions for exercising the right to data portability (RDP), which should strengthen mHealth apps users control over their data in the digital economy. To clarify, when we talk about right to data portability, we should have in mind two perspectives. First, from the user perspective, the RDP should empower users and give them more control over their personal data, by means of receiving and transmitting their data to another controller. Second, from a business perspective, its aim is to enforce competition in the digital economy by making data protection an element of this competition, by challenging the traditional system of competition law, intellectual property rights, copyright, trade secret and a 'problematic opportunity' in terms of interoperability of systems.[504] The last one, 'interoperability' is of particular interest for this thesis and will be addressed in this chapter, for the reason that, as we will argue, it presents an obstacle for exercising the RDP. Lack of interoperability can lead to the impossibility of transferring data from one controller to other. As a matter of fact, in the EU the lack of interoperability has been identified as one of the significant obstacles to the flourishing of the digital economy.[505]

What is the problem with interoperability and the GDPR? According to Recital 68 of the GDPR, interoperability formats are not a legal requirement, therefore data controllers are only encouraged to develop them if technically feasible. Thus, as argued this can prevent

---

[504] The right to data portability in the GDPR: Towards user-centric interoperability of digital services, PaulDe Hert, Vagelis Papakonstantinoua, Gianclaudio Malgieria, Laurent Beslay, Ignacio Sanchez, Computer Law & Security Review Volume 34, Issue 2, April 2018, page 193.

[505] COMMISSION STAFF WORKING DOCUMENT, A Digital Single Market Strategy for Europe - Analysis and Evidence Accompanying the document Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions-Digital Single Market Strategy for Europe Brussels May 2015{COM(2015) 192 final} page 61.

users to exercise RDP, if 'data controllers prove that in a given situation the level of technological development of their organisation makes technically unfeasible a direct transmission of data to another controller, e.g., because interoperable formats (encouraged, but not imposed) have not yet been developed'.[506]

But what is interoperability, and why it is an obstacle? Solving these questions will provide us answer to the research question: challenges arising from interoperability between mHealth apps in the data-driven economy. Therefore, first, we will explain the position of mHealth apps in the data-driven economy. Second, we will provide a framework for understanding interoperability as a concept and its four layers of the complex system. Third, we will dive into explaining what is interoperability and its challenges in the mHealth apps ecosystem and fourth, we will provide conclusions.

2. The Digital Economy

2.1 The Data-driven economy

The use of mHealth apps, fitness bands and other Internet of things equipped with sensors generate a huge amount of real-time data. Some studies show that the increase in the volume of data is exponential and it is expected that by 2020 more than 16 zettabytes of useful data will exist, which implies an equivalent growth of 236% per year.[507] Today, data is what once upon a time what oil was. Only, as a substitute for oil refineries, there are data centres, where collected data is stored, processed, analysed, shared and monetised in different ways.[508] In fact, today data is the main resource for growth and chang-

---

[506] The right to data portability in the GDPR: Towards user-centric interoperability of digital services, PaulDe Hert, Vagelis Papakonstantinoua, Gianclaudio Malgieria, Laurent Beslay, Ignacio Sanchez, Computer Law & Security Review Volume 34, Issue 2, April 2018, Pages 200

[507] COMMISSION STAFF WORKING DOCUMENT, A Digital Single Market Strategy for Europe - Analysis and Evidence Accompanying the document Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions-Digital Single Market Strategy for Europe Brussels May. 2015{COM(2015) 192 final} page 59.

[508] Moro Visconti, Roberto and Larocca, Alberto and Marconi, Michele, Big Data-Driven Value Chains and Digital Platforms: From Value Co-Creation to Monetization (January 18, 2017). Available at SSRN: https://ssrn.com/abstract=2903799 or http://dx.doi.org/10.2139/ssrn.2903799.

es, an asset and in some transactions a new currency of the current and future economy, called the data-driven or digital economy.

The term digital economy emerged as a result of the penetration of internet in all spheres of society and has received increased attention after the publication of the book by Don Tapscott. [509] Since 2007 it gained further popularity with introduction and diffusion of smart phones. Actually, this issue is also addressed by OECD, which is publishing a broad variety of reports, referring to different aspects of the digital economy.[510]

Data-driven economy in the EU is based on the Digital Single Market (hereafter DSM) framework, which presents free movement of goods, persons, services and capital, allowing natural persons and companies within the EU to easily access online activities while respecting personal data and consumer protection and fair competition.[511] It is based on digital technologies, which know no borders, and has the potential to create jobs and innovation, leading to growing markets and more choices for a better price. For instance, mHealth apps are a typical example of these advantages. Functioning of mHealth apps and digital technology is founded on reliable, high-speed and affordable networks[512] and data flow. It is worth noting that data flows are capable of improving almost everything from health, food, energy, intelligent transport systems to smart cit-

---

[509] 'In the new economy, information in all its forms becomes digital-reduced to bits stored in the computers and racing at the speed of light across networks' Digital economy - Promise and peril in the age of networked intelligence, Don Tapscott June 1997 (ISBN-10: 0070633428, ISBN-13: 978-0070633421), page 6.

[510] The OECD Digital Economy Papers series covers a broad range of ICT-related issues and makes selected studies available to a wider readership. OECD Digital Economy Papers, more on https://www.oecd-ilibrary.org/.

[511] COMMISSION STAFF WORKING DOCUMENT, A Digital Single Market Strategy for Europe - Analysis and Evidence Accompanying the document Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions-Digital Single Market Strategy for Europe Brussels May. 2015{COM(2015) 192 final} page 3.

[512] COMMISSION STAFF WORKING DOCUMENT, A Digital Single Market Strategy for Europe - Analysis and Evidence Accompanying the document Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions-Digital Single Market Strategy for Europe Brussels May. 2015{COM(2015) 192 final} page 34.

ies.[513] Yet, this can be only achieved by collecting, storing, and processing data, which, if further analysed, can provide answers to economic questions giving more precise insights about value, use, risk, utility, characteristics, markets, customer behaviour analytics, performances and policy decisions.[514]

Talking about the advantages of the data-driven economy, one must also look at the disadvantages. On one hand, in the data-driven economy, companies will be those that will benefit most, contrary to the millions of users that create a considerable part of the data. Even though one can argue that users are also benefiting, because by willingly sharing more personal data they are able to connect with friends and family (social and emotional value, as well as inexpensive communication), the possibility to network for professional purposes, access to services that enable them to save time and money (e.g. car sharing), information exchange (to make more informed decisions on product purchases) to monitor their health and wellbeing (constantly, cheaper and from a distance).[515] On the other hand, it seems like in the digital economy users are losing the control over their data. However, the EU Commission has envisaged this and consequently has proposed legal instruments to solve this issue, meaning, it proposed tools that will enable the user to gain control over their data by receiving or transferring the data that they provided to other company. One legal instrument is the proposal of a Directive for the supply of digital content.[516] Within the scope of this directive is data in general, not only personal data, and thus it will be not discussed in this thesis. Another instrument is as previously discussed, the GDPR and the right to data portability.

---

[513] COMMISSION STAFF WORKING DOCUMENT, A Digital Single Market Strategy for Europe - Analysis and Evidence Accompanying the document Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions-Digital Single Market Strategy for Europe Brussels May. 2015{COM(2015) 192 final} page 4.

[514] Moro Visconti, Roberto and Larocca, Alberto and Marconi, Michele, Big Data-Driven Value Chains and Digital Platforms: From Value Co-Creation to Monetization (January 18, 2017). Available at SSRN: https://ssrn.com/abstract=2903799 or http://dx.doi.org/10.2139/ssrn.2903799.

[515] *Id.*, page 17

[516] Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on certain aspects concerning contracts for the supply of digital content, COM/2015/0634 final - 2015/0287 (COD) http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52015PC0634.

Regardless of the intention of the EU Commission, on one hand, to boost the EU data-driven economy and make it a market leader, while, on the other hand, attempt to return users control over their data, it faces some obstacles. European Commission in the Digital Agenda has identified absence of interoperability or portability, in other word problems in changing provider or with access to data[517] as one out of a few of the most significant obstacles; a few relevant for this thesis, especially for this chapter, are economic interests vs. data protection rights and ownership of data.[518]

2.2 Personal data and economic interests

In the data-driven economy, the core business models of many companies is centred on processing of data, which often involves processing of personal data, such as a person's age, address, gender, preferences, flight reservation but also their visited websites, posted comments, photos uploaded to social media, and other. These data for the companies has an immense economic value because it reveals individual behaviours and interests, that are increasingly regarded as business assets that can be used to target users, in order to provide them relevant advertising, or to be traded with other parties.[519]

Subsequently, this processing of personal data requires companies or apps to comply with data protection rules, although some companies consider that specific data protection rules, practically create an excessively heavy obligation that could affect their eco-

---

[517] COMMISSION STAFF WORKING DOCUMENT, A Digital Single Market Strategy for Europe - Analysis and Evidence Accompanying the document Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions-Digital Single Market Strategy for Europe Brussels May. 2015{COM(2015) 192 final} page 61.

[518] This includes issues such as ownership of data, treatment of personal and industrial data, availability, access and re-use, contractual terms and conditions, data security, quality of data (e.g. timely updates), authentication of users, cybercrime, acceptance of electronic documents, liability for incorrect information, standardisation of languages and formats. See COMMISSION STAFF WORKING DOCUMENT, A Digital Single Market Strategy for Europe - Analysis and Evidence Accompanying the document Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions-Digital Single Market Strategy for Europe Brussels May. 2015{COM(2015) 192 final} page 61.

[519] Acquisti, Alessandro and Taylor, Curtis R. and Wagman, Liad, The Economics of Privacy (March 8, 2016). Journal of Economic Literature, Vol. 52, No. 2, 2016; Sloan Foundation Economics Research Paper No. 2580411. Available at SSRN: https://ssrn.com/abstract=2580411 or http://dx.doi.org/10.2139/ssrn.2580411, page 4

nomic interests. Therefore, a question arises, if the economic interests of companies or apps in the data-driven economy, could limit the right to data protection. One of the cases that among others matters tackle this issue is the CJEU *Google Spain* Case.[520] Briefly, the case is regarding Mr. Mario Costeja González's request, asking Google to remove the links to the search results that each time appear when someone types his name in the Google search engine. Actually, the search results were connected with announcements in printed editions, that later become available online, concerning debts that forced him to sell his property. The Court in this case considered how this would affect the fundamental rights to privacy and to the protection of personal data. It has pointed out that the use of search engines and the structured overview of the search results can establish a detailed profile of an individual, results that may concern a different aspects of an individual's private life, which otherwise could not have been easily found or interconnected without a search engine.[521] It thus constituted a potentially serious interference with the data subjects' fundamental rights to privacy and protection of personal data.

In respect of the economic interest of the search engines, which offer advertising space to make their service economically profitable,[522] the CJEU stated that 'it is clear that [the interference] cannot be justified by merely the economic interest which the operator of such an engine has in that processing', and that 'as a rule' the fundamental rights under Articles 7 and 8 of the Charter override such economic interest and the interest of the general public in finding that information upon a search relating to the data subject's name.[523] This judgment has probably been the subject of more academic commentary in a few months than other CJEU data protection cases have been in the 16 years since the

---

[520] CJEU, C-131/12, Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González [GC], 13 May 2014

[521] CJEU, C-131/12, Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González [GC], 13 May 2014, para.80

[522] CJEU, C-131/12, Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González [GC], 13 May 2014, para.55-56

[523] CJEU, C-131/12, Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González [GC], 13 May 2014, para.81

Directive came into force.[524] It has received a wide range of reactions, from criticism to approval.

Apart from other matters addressed in this case, such as whether an Internet search engine should be considered to be a data controller or a data processor; the territorial application of EU data protection law; and the extension of data protection rights to the Internet, for this thesis is relevant that it requests fair balancing of rights, between right to data protection and privacy of individual, the interest of others to have access to such information, and, on the other hand, the economic interest of the search engine.[525] This means that the rights of the individual should prevail, as a rule, not only over the economic interest of the search engine but also the interest of the public in general in finding that information, although the individual's rights should not take precedence if other factors would justify an interference with them, such as the data subject's role in public life.

2.3 Data ownership issue

As stated, in the digital economy, information about individuals is often and increasingly seen by companies as having a value comparable to money. For instance, digital products or services are frequently offered not in exchange for a money but by giving access to personal data or other data. In fact, those explicit business models apply in different forms in a substantial part of the market.[526] Thus, it is obvious the decision of some companies is to opt for closed platform and to limit the interoperability of their products

---

[524] Kuner, Christopher, The Court of Justice of the EU Judgment on Data Protection and Internet Search Engines (September 15, 2014). Final version published as 'The Court of Justice of the EU Judgment on Data Protection and Internet Search Engines: Current Issues and Future Challenges', in: Burkhard Hess and Cristina M. Mariottini (eds.), Protecting Privacy in Private International and Procedural Law and by Data Protection 19-55 ; LSE Legal Studies Working Paper No. 3/2015. Available at SSRN: https://ssrn.com/abstract=2496060 or http://dx.doi.org/10.2139/ssrn.2496060 page 4, See also See the website <http://www.cambridgecode.org/googlespain.html>, listing dozens of academic blog entries on the case in the few months since it was issued.

[525] CJEU, C-131/12, Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González [GC], 13 May 2014, para.97

[526] Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on certain aspects concerning contracts for the supply of digital contentCOM/2015/0634 final - 2015/0287 (COD) Recital (13) http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52015PC0634.

and services, basically trapping the users into the platform without possibility to transfer their data from one app to other.

Speaking from the business point of view, the company who actually has developed the product and the underlying business model is de facto in control of the technical process of 'producing' the data. It is their business idea and their investment in realising the product or service. However, the problem arises from the fact that, as some argue the specific data will not be produced without the use of the device and the kind of data produced depends on who uses the device and how it is used.[527] Despite the fact that data subject by using device or service in a particular way produced data, the service cannot claim ownership of the data. In the EU ownership of others' personal data it is not recognised, for the reason that protection of the personal data has the status of a fundamental human right.

In order to protect their data assets, companies are refusing to develop data in an interoperable format. This has a negative impact on the user's right to portability, because they cannot transfer their data from one app to other. To clarify, portability and interoperability are two connected, but very diverse, attributes of a component within a computing system.

Portability is 'the ability of software or data to be transferred from one machine or system to another', meaning the ability to physically move software or data from one system to another. In the context of mHealth apps, this would mean to transfer the data from one app to other, whereas interoperability is 'the ability of two or more systems or applications to exchange information and to mutually use the information that has been exchanged'. In other words, is the ability to interact between systems via a well-defined interface to obtain predictable results, while the software or data continues to reside on the

---

527 Josef Drexl, Reto M. Hilty, Jure Globocnik,Franziska Greiner, Daria Kim,Heiko Richter,Peter R. Slowinski, Gintarė Surblytė, Axel Walz, Klaus Wiedemann Position Statement of the Max Planck Institute for Innovation and Competition on the European Commission's 'Public consultation on Building the European Data Economy' 26 April 2017, page 10.

same physical machine after the interaction.[528] Each of these capabilities is important for the right to data portability.

3. Interoperability in data-driven economy

It is evident that interoperability is an important part of the EU rhetoric on the future of digital economy. Large segments are now interconnected as never before: government agencies, financial institutions, transportation infrastructures, healthcare and energy systems are linked by new, invisible information channels, which are essential components of today's global economy. In fact, this is also expected to grow dramatically thanks to the emergence of the Internet of Things, referring to anything that can be connected to the Internet. This internet interconnectedness does not mean only new forms of interactions with end users, but also new forms of interactions with other devices. For instance, a fitness bracelet is connected to the user's phone and informs the user about his fitness progress. This technology is built primarily on a single concept: interoperability. In order to send and receive important data, it needs to be able to seamlessly connect to other systems and networks in ways that are meaningful and secure. That necessary interconnection of systems is interoperability. As Gasser phrases it, 'interoperability as a concept is central, and yet often invisible, to many parts of a highly interconnected modern society'.[529]

In point of fact, there is no general agreement on the definition of interoperability, most probably because it depends on the context and perspective. For example, users of mHealth app might define interoperability as simple access to their fitness and well-being data, while app developers will define it as ability to technically interconnect with the APIs on the smart phone and integrate that data in order to optimise the functioning of the app. Subsequently it comprises many forms of interaction, which frequently occur simultaneously.

---

[528] European Committee for Interoperable Systems, Special Paper on Cloud Computing: Portability and Interoperability, June 27, 2016.

[529] Gasser, Urs. 2015. 'Interoperability in the Digital Ecosystem.'Berkman Klein Center for Internet and Society Research Publication No. 2015-13, page 7.

In the EU interoperability is defined as 'the ability of disparate and diverse organisations to interact towards mutually beneficial and agreed common goals, involving the sharing of information and knowledge between the organisations, through the business processes they support, by means of the exchange of data between their respective ICT systems'.[530] On the other hand, ISO/IEC 2382-01 defines interoperability as: 'The capability to communicate, execute programs, or transfer data among various functional units in a manner that requires the user to have little or no knowledge of the unique characteristics of those units.' Moreover, Directive 2009/24/EC on the legal protection of computer programs, in recital 10 defines interoperability as the ability to exchange information and mutually to use the information which has been exchanged. Interoperability is also mentioned in Article 18 and Recital 31[531] of the Directive 2002/21/EC on a common regulatory framework for electronic communications networks and services[532] (Framework Directive), as well as, in the Council Regulation on standards for security features and biometrics in passports and travel documents issued by Member States.[533]The Software

---

530 Article 2 of Decision No 922/2009/EC of the European Parliament and of the Council of 16 September 2009 on interoperability solutions for European public administrations (ISA) OJ L 260, 03.10.2009, p. 20.

531 Recital 31: *' Interoperability of digital interactive television services and enhanced digital television equipment, at the level of the consumer, should be encouraged in order to ensure the free flow of information, media pluralism and cultural diversity. It is desirable for consumers to have the capability of receiving, regardless of the transmission mode, all digital interactive television services, having regard to technological neutrality, future technological progress, the need to promote the take-up of digital television, and the state of competition in the markets for digital television services. Digital interactive television platform operators should strive to implement an open application program interface (API) which conforms to standards or specifications adopted by a European standards organisation. Migration from existing APIs to new open APIs should be encouraged and organised, for example by Memoranda of Understanding between all relevant market players. Open APIs facilitate interoperability, i.e. the portability of interactive content between delivery mechanisms, and full functionality of this content on enhanced digital television equipment. However, the need not to hinder the functioning of the receiving equipment and to protect it from malicious attacks, for example from viruses, should be taken into.'* Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive).

532 Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services.

533 Article 1(2): 'Member States shall also include fingerprints in interoperable formats.' Council Regulation (EC) No 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States.

Copyright Directive[534] and the EU Draft Directive on Digital Good and Services[535] entail a similar but more context specific definition.

Yet, despite the lack of a widely accepted definition, for the purpose of this thesis, we will adopt the definition of Palfrey and Gasser, two leading figures of the interoperability debate: 'interoperability is the ability to transfer and render useful data and other information across systems, applications, or components'.[536] To avoid further confusion, it is worth mentioning that in fact, interoperability is a subcategory of broader but also vague concept of compatibility.[537]

In line with the definition, Palfrey and Gasser further clarify that theoretically speaking, there are four levels of interoperability, (a) legal, (b) human, (c) technical, and (d) data interoperability. This clarification will enable us to concentrate our discussion only on two levels of interoperability, technical and data interoperability. Therefore, we will briefly explain all of them and then concentrate only on the technical and data interoperability between mHealth apps.

---

[534] Directive 2009/24/EC of the European Parliament and of the Council of 23 April 2009 on the legal protection of computer programs , Recital 10: 'The function of a computer program is to communicate and work together with other components of a computer system and with users and, for this purpose, a logical and, where appropriate, physical interconnection and interaction is required to permit all elements of software and hardware to work with other software and hardware and with users in all the ways in which they are intended to function. The parts of the program which provide for such interconnection and interaction between elements of software and hardware are generally known as "interfaces". This functional interconnection and interaction is generally known as "interoperability"; such interoperability can be defined as the ability to exchange information and mutually to use the information which has been exchanged.'

[535] Proposal for a Directive of the European Parliament and of the Council on certain aspects concerning contracts for the supply of digital content, Brussels, 9.12.2015 COM(2015) 634 final, 2015/0287(COD) Article 2(9)'interoperability' means the ability of digital content to perform all its functionalities in interaction with a concrete digital environment.

[536] Interoperability in the Digital Ecosystem - Urs Gasser 2015, The Berkman Center for Internet & Society at Harvard University, page 10.

[537] See the Standard Glossary of Software Engineering Terminology' (IEEE 610.12-1990) The ability of two or more systems or components to perform their required functions while sharing the same hardware or software environment (2) The ability of two or more systems or components to exchange information (interoperability) page 18. Interoperability is defined as 'The ability of two or more systems or components to exchange information and to use the information that has been exchanged'.

3.1 Levels of interoperability

Legal interoperability requires legal systems to work with one another towards establishing an international order that can accommodate the interconnected nature of the world in which we live.[538] It is essential in order to facilitate global communication, to reduce costs in cross-border business, to drive innovation, economic growth and for protection of the human rights and freedoms. This can be achieved by applying a top-down model[539] or bottom-up process,[540] for instance, a top-down model would be by harmonisation, standardisation, mutual recognition and other approaches.[541] One example of legal interoperability is the harmonised legal rules necessary for implementation of Domain Name Systems (DNS). On contrary, example for lack of legal interoperability is the issue of privacy arising from the trans-border data flows, and different levels of protection on personal data, as confirmed by the ECJ in the case *Schrems v Data Protection Commissioner*.[542] There is a different approach and level of protection between EU and US law, as well as other regions of the world regarding privacy and data protection issues. Leading to different regulations that needs to be taken into account when mHealth app is offered to the EU users or US users.

The position of mHealth apps is a complex issue regarding legal interoperability. It involves developers, systems and technology from all around the world, meaning they should comply with the EU legislation. From a legal perspective, mHealth apps is a hori-

---

538 Interoperability Case Study-The European Union as an Institutional Design for Legal Interoperability, The Berkman Centre for Internet & Society at Harvard University, Félix Tréguer 2012

539 This model would require establishing a global agency or institution, such as UN or International Telecommunication Union.

540 It must be based on a step-by-step model that encompasses the major concerned entities and persons of the substantive topic.

541 Legal Interoperability as a Tool for Combatting Fragmentation, Global Commission on Internet Governance Paper Series: No.4-December 2014 Rolf H. Weber, page 7.

542 Judgment of the Court (Grand Chamber) Maximillian Schrems v Data Protection Commissioner, Case C-362/14, 6 October 2015.

zontal matter which touches upon several fields[543] including but not limited to data protection, medical devices directive, e-commerce, free movement of services within the EU, cross-border healthcare and ISO standards, soft law and Binding Corporate Rules.

Human interoperability, on the other hand, means the ability of humans to understand and act on the data exchanged. As Gasser stated, it can involve the use of a common language as a form of communication, or a willingness to work together and to succeed.[544]

For the reason, that technology and data are inseparable concepts, the two levels, technical and data interoperability, will be explained together. Technological interoperability is defined as the ability of hardware and codes to connect, and data interoperability as the ability of interconnected systems to understand each other. Talking about mHeatlh apps, this would mean that functioning of apps depends on a permanent and smooth data flow between apps (software) and the operating system (OS)[545] of the smart device (hardware). This data flow is possible through an interface called an Application Programming Interface (API) installed by the operating system (OS) and device manufacturers. In other words, it is built into devices and enables apps to access data collected by or stored in the device. Thus, the app developer will be able to access data that the OS and device manufacturers make available through the API. In fact, technical and data interoperability of mHealth apps is possible only if APIs[546] are open.

---

543 Book eHealth: Legal, Ethical and Governance Challenges, Carlisle George – Diane Whitehouse-Penny Duquenoy.

544 Interoperability in the Digital Ecosystem - Urs Gasser 2015, The Berkman Center for Internet & Society at Harvard University, page 11.

545 App developers can develop apps for different operating systems (Android, iOS, Windows etc). In any case they will need to sign license agreement. For example Android License agreement state '*You agree to use the Preview and write applications only for purposes that are permitted by (a) the License Agreement, and (b) any applicable law, regulation or generally accepted practices or guidelines in the relevant jurisdictions (including any laws regarding the export of data or software to and from the United States or other relevant countries)'.* See point 4.2 https://developer.android.com/preview/license.html.

546 Interoperability in the Digital Ecosystem - Urs Gasser 2015, The Berkman Center for Internet & Society at Harvard University.

Talking about technical and data interoperability, it is particularly important to distinguish between horizontal and vertical interoperability. Horizontal interoperability means interoperability of competing products, services or platforms, while vertical interoperability refers to the interoperability of a product, service or platform with complementary products and services, in other words, the degree to which complementary product can be shared across different platforms. In general, companies have entrepreneurial freedom to decide the extent of interoperability of their products and services. They can decide for an open platform which allows sharing products and services with other platforms. In this way, they can increase the value for customers and therefore increase profits.

On the other side of the spectrum are companies that decide on closed systems. The reasoning behind this is that they want to develop more innovative products and services with explicit components and services, which can only be achieved if they are capable of controlling the entire value network according to their own specific requirements. Interoperability and openness to complementary products may endanger their business model. For instance, the business model of Apple is a closed system that bundles its products with the iOS operating system. With the App Store, it established a closed system, which allows for far-reaching control of all apps that run on the iOS operating system. [547]

Apart from being free to decide the extent of interoperability of their products and services, in some areas the EU has gone far beyond this voluntarism by creating a legal basis for mandating interoperability. While in other cases, it can be imposed by competition law.

The best example is the telecommunication sector, where interoperability is mandated on all providers on EU level. Traditionally known as public monopolies, this sector in the EU, in 1998 saw full liberalisation. Afterwards, in 2002 the Telecoms Regulatory Framework for electronic communications was adopted and updated in 2009. In the meantime it has been supplemented by a number of additional legislative instruments. The current framework is made of a package of 5 Directives and 2 Regulations. Essen-

---

[547] Wolfgang Kerber, Heike Schweitzer, Interoperability in the Digital Economy, 8 (2017) JIPITEC 39 para 1.

tially, the Directive of access to electronic communications networks[548] harmonises the way in which EU countries regulate access to, and interconnection of, electronic communications networks and associated facilities. It establishes a regulatory framework for the relationships between suppliers of networks and services that will result in sustainable competition and interoperability of electronic communications services. Basically, it establishes a fundamental rule whereby operators of public communications networks have a right and an obligation to negotiate interconnection with each other in order to ensure service interoperability throughout the European Union.[549] While at the level of the EU member states, National Regulatory Authorities are responsible to determine if one or more operators have a significant power on the market. If that is the case, among other obligations, they can impose obligation to the operator 'to grant open access to technical interfaces, protocols or other key technologies that are indispensable for the interoperability of services'.[550]

The second case is when interoperability is imposed by competition law. In particular, if the refusal for disclosing interoperability information comes from a dominant company, it is considered as abusing the dominant position on the market. An example is the *Microsoft* case.[551] The Court found that Microsoft abused its dominant position on the market for client PC operating systems by its refusal to supply its competitors with 'interoperability information' and to authorise the use of that information for the purpose of

---

548 The directive applies to all forms of public communication networks carrying publicly available electronic communications services. These include fixed and mobile telecommunications networks, networks used for terrestrial broadcasting, cable TV networks, and satellite and Internet networks used for voice, fax, data and image transmission.

549 Directive 2002/19/EC of the European Parliament and of the Council of 7 March 2002 on access to, and interconnection of, electronic communications networks and associated facilities (Access Directive), Article 4(1).

550 Directive 2002/19/EC of the European Parliament and of the Council of 7 March 2002 on access to, and interconnection of, electronic communications networks and associated facilities (Access Directive), Article 12(e).

551 Judgement of the court of first instance (Grand Chamber), Microsoft Corp. v Commission of the European Communities, Case T-201/04, 17 September 2007

developing and distributing products competing with Microsoft's own products on the work group server operating systems market.[552]

In the context of mHealth apps, this would mean that if there is a lack of interoperability between two apps, and users are not able to transfer their data from one app to other, in order competition law to step in it is necessary to be proved that app has a dominant position on the market. Currently users of the mHealth apps has option only to download their health data in a chosen format, but they do not have an option to directly transfer their data from one app to other.

Therefore, in order to respond to the current lack of regulation in the online world, some companies on their own self-initiative started working on a solution. Considering the fact that portability and interoperability are central to innovation, Facebook, Google, Microsoft and Twitter in 2017 formed the Data Transfer Project (DTP). It is an open-source, service-to-service data portability platform which would allow users in the online world to easily move their data between online service providers whenever they want. Its aim is to allow individuals to choose among services, which facilitates competition, empowers individuals to try new services and enables them to choose the offer that best suits their needs.[553] Theoretically, the DTP would mean giving control of users to choose any app that best competes for protecting their data and privacy. Practically, the DTP tool is still not completed but based on the published paper, one might get idea how it will work. Yet at this point of time it is not clear if and to what extent this project will really give users control over their data. Or, whether this is one more project that will allow them to better position their monopoly tech companies in the online world.

---

[552] Judgement of the court of first instance (Grand Chamber), Microsoft Corp. v Commission of the European Communities, Case T-201/04, 17 September 2007, para.30-37

[553] See more on Data Transfer, Project https://datatransferproject.dev/ last visited on 22.07.2018

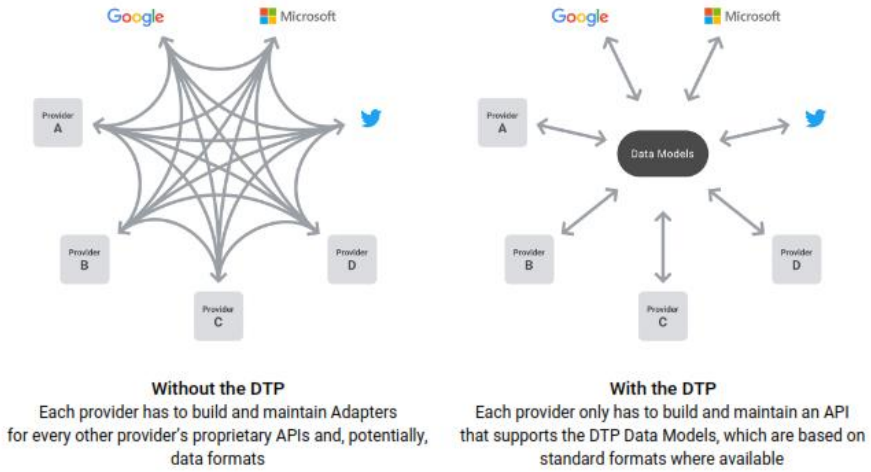

Figure 5. The Data Transfer Project. Source: White paper, Data Transfer Project, Overview and Fundamentals published July 20, 2018

The left image in Figure 5 illustrates the current situation. It shows the paths of the data due to the lack of interoperability and portability between online services or apps. The right hand image is the proposed solution to the current challenge of the interoperability issue.

3.3 Privacy issues

Despite these advantages, interoperability comes with some weaknesses. Actually, interoperability is mostly associated with decreasing privacy. The reasoning behind this is that increased levels of interoperability may increase the number of actors who could have access to personal information exchanged via an interoperable system.[554] For the reason, that interoperability encourages more complex ecosystems, with more participants, and thus creates more risk vectors.

---

554 Gasser, Urs. 2015. 'Interoperability in the Digital Ecosystem.'Berkman Klein Center for Internet and Society Research Publication No. 2015-13 page 13
https://dash.harvard.edu/bitstream/handle/1/28552584/SSRN-id2639210.pdf?sequence=1

4. Interoperability of mHealth app operating systems

In order to understand the interoperability challenges arising between mHealth apps, we need to analyse the current situation on the market. Presently on the market, there are three large dominant mobile operating systems that are installed on nearly 90% of mobile devices available. (Table 1).

Table 1: Worldwide market share of smartphone operating systems[555]

Period	Android	iOS	Windows Phone	Others
2016 Q1	83.4%	15.4%	0.8%	0.4%
2016 Q2	87.6%	11.7%	0.4%	0.3%
2016 Q3	86.8%	12.5%	0.3%	0.4%
2016 Q4	81.4%	18.2%	0.2%	0.2%
2017 Q1	85.0%	14.7%	0.1%	0.1%

These are Android OS, iOS and Windows. Each of these operating systems has different specifics and levels of interoperability. Android OS, as can be concluded from the table, is the most used mobile operating system in the world, and as an open source operating system it is distributed by many companies on the mobile devices they produce. Android OS is an operating system based on the Linux Kernel and it was developed by Google.

The second most used operating system on mobile devices is iOS. It is an operating system developed by Apple. It is the only company which distributes iOS on the mobile devices they produce. Windows Phone OS is the third most used mobile operating system in the world. It is an operating system developed by Microsoft exclusively for

[555] Smartphone operating systems market share 2017 https://www.idc.com/promo/smartphone-market-share/os.

smartphones and is based on Windows Kernel. Though it is not an open source mobile operating system, Windows Phone unlike iOS is distributed by many smartphone manufacturers on their devices.

Thus, it can be concluded that each mobile device had its own operating system (OS) installed, depending on the companies that produce them. This way they are opening the path to the development of OS based applications. There are different software developer kits (SDK) for developing apps that are running on iOS or Android. This as some researchers argue lead to an operational incompatibility between the applications running on the dominant operating systems on the market.[556] Stemming from this fact, development of applications for each operating system is hindered by the lack of communication, interoperability, and synchronisation.[557]

Yet, one study has developed conceptual framework that provides the ability to interoperate data between applications running on different mobile operating systems installed on smartphones. As they have concluded

> the data transfer protocol will be composed not only of operating system information but will also be taken in consideration communication environment used, the format of the data to be transferred, and technical limits that the devices involved in the data transfer have. As manipulation of data could reach a high level of complexity depending on the processes involved, the framework will use an automation module that will take care of data packages switched between processes so that the user's intervention is reduced to only apply or select from options made available by the framework.[558]

5. Conclusion

Data-driven economy in the EU is based on the Digital Single Market framework which presents free movement of goods, persons, services and capital allowing natural persons

---

[556] Interoperability framework for communication between processes running on different mobile operating systems, A Gal et al, 2016 IOP Conf. Ser.: Mater. Sci. Eng.106/012007, page 3, http://iopscience.iop.org/article/10.1088/1757-899X/106/1/012007/meta.

[557] *Id*.

[558] *Id*, page 7.

and companies within the EU to easily access online activities, while respecting the personal data, consumer protection and fair competition. In the data-driven economy, the core business models of the companies is centred on processing of data, which often involves processing of personal data. For instance, mHealth apps and fitness bands and the like are equipped with sensors and are generating a huge amount of real-time data. Today, data is what once upon a time the oil was. In fact, today data is the main resource for growth and changes, an asset and in some transactions a new currency of the current and future economy.

These data for the companies has an immense economic value, because they reveal individual behaviours and interests that are increasingly regarded as business assets that can be used to target users, in order to provide them relevant advertising, or to be traded with other parties. However, this processing of personal data requires companies or apps to comply with the data protection rules. Although some companies consider that specific data protection rules practically create an excessively heavy obligation that could affect their economic interests. Therefore, a challenge arises whether the economic interests of companies or apps in the data-driven economy could limit the right to data protection.

Despite its advantages, one must look at the disadvantaged of the data-driven economy. Actually, the companies will be those that will benefit most, contrary to the millions of users that create a considerable part of the data. Furthermore, it seems like in the digital economy users are losing the control over their data. Regardless of the intention of the EU Commission, on one hand, to boost the EU data-driven economy and make it a market leader, while, on the other hand, attempts to return users control over their data, it faces some obstacles. European Commission in the Digital Agenda has identified absence of interoperability or portability, in other word problems in changing providers, as one out of few ‘most significant obstacles’.

As Gasser phrases it ‘interoperability as a concept is central, and yet often invisible, to many parts of a highly interconnected modern society’. There is no widely accepted definition of interoperability. When talking about technical and data interoperability, it is particularly important to distinguish between horizontal and vertical interoperability. Horizontal interoperability means interoperability of competing products, services or platforms, while vertical interoperability refers to the interoperability of a product, ser-

vice or platform with complementary products and services, in other words, the degree to which complementary product can be shared across different platforms. In general, companies have entrepreneurial freedom to decide the extent of interoperability of their products and services. Apart from being free to decide the extent of interoperability of their products and services, in some areas the EU has gone far beyond this voluntarism by creating legal basis for mandating interoperability. While in other cases, it can be imposed by the competition law.

The issue of interoperability is closely related with data ownership, it is obvious some companies have opted for closed platform and to limit the interoperability of their products and services, basically, trapping the users into the platform without possibility to transfer their data from one app to other. Speaking from the business point of view, the company who actually has developed the product and the underlying business model is de facto in control of the technical process of 'producing' the data. It is their business idea and their investment in realising the product or service. However, the problem arises from the fact that, as some argue the specific data will not be produced without the use of the device and the kind of data produced depends on who uses the device and how it is used. The EU has not recognised ownership of personal data, for the reason that protection of the personal data has the status of a fundamental human right.

Interoperability between mHealth apps, in terms of directly transferring data from one operating system to other does not exist, for example from iOS to Android, while there is a possibility to import data installed on the iPhone to the Apple Health. Surely it is possible to download the data in a pre-suggested format.

CHAPTER 6: CONCLUSION

1. Introduction

The main research question of this thesis is whether the new right to data portability (RDP) will strengthen or undermine control over personal data of mHealth apps users, as it encounters challenges arising from interoperability between mHealth apps. The central question entails two sub-questions. The first one is what the RDP is. The second one is if and to what extent the right to data portability is possible from technical point of view (interoperability) between mHealth apps. In this thesis, the RDP has been discussed as instrument that should give users greater control over their personal data to protect two fundamental human rights: the right to data protection and privacy.

The findings of this study lead to the conclusion that right to data portability in practise might to some extent strengthen the users of mHealth apps control over their personal data but in most cases, this will be first challenged by the legal interpretation of the RDP, and second by lack of interoperability. The purpose of this chapter is to explain how we came to this conclusion. In order to achieve this purpose, we will summarise the findings and conclusions from the previous chapters. In fact, each chapter is built upon the finding of the previous one, leading to the answer of the main research question.

2. Problems and Answers

The functioning of lifestyle and well-being apps is based on the collection, storing and analysis of data for prolonged periods so that users can monitor their progress toward fitness, health and well-being goals and ultimately to make more informed decisions about their health and lifestyles. Consequently, for users it is important to have control over this data for prolonged periods and to be able to transfer their data from one app to other.

This control over the data, or the possibility to transfer the data from one app to other, derives from the new right to data portability introduced in the General Data Protection Regulation in the EU.

For the reason that data collected and processed by the mHealth apps falls within the scope of the four main building blocks, which constitute the definition of personal data:

‘any information’, ‘relating to’, ‘an identified or identifiable’, and ‘natural person’. To illustrate, they are installed on smart devices, which in most cases are associated with a user of the phone. Meaning it ‘relates to’ a ‘natural person’. Second, they typically have direct access to many different sensors, data provided by the user or uniquely generated data by the device or OS. Meaning there is a possibility a user to be directly or indirectly ‘identified’ or is ‘identifiable’. By its nature information collected from the mHealth apps, in most cases falls within the special category of data, or health data. Having in mind the way the app is functioning, it is possible based on the raw sensor data used by itself or in combination with other data to draw a conclusion about the actual health status or health risks of a user. On the other hand, if seemingly innocuous raw data is tracked over a longer period of time, it might also reveal the health status of the user.

Anyway, it is challenging to capture the notion of health data, partly due to the highly technical and complex technology used in the apps, which is continuously developing and improving. Considering the fact that there is no simple definition of health data, some argue that it should be decided case by case. In view of this, controllers or app developers should be held accountable as to how they legally define the data from the mHealth apps, merely as a personal data or as health data. The main reasoning behind is that, in most cases, they possess the crucial technical knowledge necessary to qualify such information as health data or not.

The analysis of the legal limitation of the right to data portability reveals how complex this right is. First, in order to understand what entails ‘provided by’ and what ‘necessary for the performance of the contract’ means apart from the legal knowledge, it requires substantial technical knowledge. Second, it is questionable as to what extent it will really strengthen user control, considering the limited interpretation of ‘provided data’ and the burden of the data subject to prove his identity if the data has been pseudonymised. Third, the wording, as some argue, is too restrictive because it does not cover situations where the controller has illegally processed the data,[559] for example, data that is pro-

[559] Data Portability - A Tale of Two Concepts, Prof. Dr. Ruth Janal, JIPITEC – Journal of Intellectual Property, Information Technology and E-Commerce Law 8 (2017) JIPITEC 59 para 1, https://www.jipitec.eu/issues/jipitec-8-1-2017/4532.

cessed without data subject knowledge, more precisely without valid consent, which might be the case with some mHealth apps.

What does this mean for the users of mHealth apps? Can they request the right to data portability, if data is pseudonymised?

The Article 29 WP in their opinion explained that in the case of pseudonymous data, the data controller can reject the data portability request, solely if after the pseudonymisation, data cannot be clearly linked to a data subject.[560] According to the same opinion, the burden is on the data subject to provide additional information's enabling their identification.[561] It seems paradoxical that the data subject should provide more personal data to identify himself in order to receive the data back. At first sight this leads to excessively burdensome or perhaps even absurd consequences.[562] This interpretation is not in line with the initial thoughts of the right to data portability, introduced to strengthen user control over their personal data. In fact, this clarification presents an obstacle for the data subject to receive or transfer their data, if they cannot provide additional information to enable identification. It does not constitute a fair balance between, on one hand, the interest of the data subject in protecting his personal data, in particular right to data portability and, on the other hand, the obligation of the controller after pseudonymisation of personal data to clearly link them to a particular data subject.

The right to data portability, from the moment of its introduction, has been accepted sceptically, because portability creates a more complex set of issues. While all would agree that 'lock in' is undesirable and that open standards facilitating the portability of information across competitive services are preferred, it is very difficult to require that information from one application or service be useful in another application or service, mostly due to the fact that applications often have considerably different functions, uses and formats of information limiting potential utility of portability. In many cases, the

---

560 Article 29 WP, Guidelines on the right to data portability, adopted on 13 December 2016, as last Revised and adopted on 5 April 2017, page 9.

561 Article 11 (2), GDPR.

562 Article 29 WP, Opinion 4/2007 on the concept of personal data, WP 136 Adopted on 20th June 2007, page 5

reason behind this is motivated by differentiation of the products and modifying them to emerging or more specific market needs. The uncertainties stem from the implications that RDP might have on innovation if is excessively prescriptive and specifies detailed formats or functionality implementations. The general agreement is that RDP can be accomplished through open standards, but it cannot be a mandated solution.[563] It should be also taken into consideration, that app companies have an interest in the personal data, resulting from the data-driven economy. This supports them to better position on the market.

Additionally, RDP does not sit in isolation but within a wider, complex framework of the GDPR, which mandates a vast range of compliance obligations. Thus, the range of compliance varies from not transferring data outside of the EU to countries with inadequate protection, collecting only minimal data and storing for a limited time, ensuring secure and transparent processing, privacy by design and default and many more. Hence, responding to the right to data portability as some authors argue goes beyond the technical requirements of making systems interoperable or creating APIs so data can be ported. [564]

Based on the previous findings, recommendations for the app developers, but also to developers of other technology and manufactures which products and services process personal data in a wide range of areas[565] will be to:

- Encourage them to design their products and services in a manner that right to data portability is taken into consideration from the beginning.
- Allow user to have control over their "provided" personal data, in terms of transferring their data directly to other apps, products and services.

---

[563] International Chamber of Commerce (ICC) Comments on EU Directive: 95/46/EC COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS 'A comprehensive approach on personal data protection in the European Union' January 2011, page 5, http://ec.europa.eu/justice/news/consulting_public/0006/contributions/not_registered/icc_en.pdf.

[564] Realising the right to data portability for the domestic Internet of things, Lachlan Urquhart, Neelima Sailaja DOI 10.1007/s00779-017-1069-2, Published online 23 August 2017, page 4, https://link.springer.com/content/pdf/10.1007%2Fs00779-017-1069-2.pdf.

[565] Tech companies, banks, social networks and other.

- Collaborate and agree on commonly acceptable interoperable data formats
- Provide the personal data in formats that have a high level of portability from any internal or proprietary format.
- Encourage them to identify in advance personal data which fall within the scope of portability in their own systems.[566] Consequently, only the data that fall within the RDP can be extracted from the platform.
- Use data portability as competitive advantage to position themself on the market
- Share the responsibilities between the sender and receiver of the ported personal data
- Delete ported personal data which is not relevant for the particular transfer

[566] Article 29 WP, Guidelines on the right to data portability, adopted on 13 December 2016, as last Revised and adopted on 5 April 2017, page 17.

BIBLIOGRAPHY

1. A cross-cultural comparison of health status values, D L Patrick, Y Sittampalam, S M Somerville, W B Carter, and M Bergner , Am J Public Health. 1985 December; 75(12): 1402–1407

2. A new support system using a mobile device (smartphone) for diagnostic image display and treatment of stroke. Takao H, Murayama Y, Ishibashi T, Karagiozov KL, Abe T. 2012. Stroke. 43(1), 236-39 10.1161/STRO

3. A Taxonomy of mHealth Apps – Security and Privacy Concerns, 2015 48th Hawaii International Conference on System Sciences. Miloslava Plachkinova, Steven Andrés and Samir Chatterjee, Claremont Graduate University

4. A Typology of Privacy (March 24, 2016) Koops, Bert-Jaap and Newell, Bryce Clayton and Timan, Tjerk and Škorvánek, Ivan and Chokrevski, Tom and Galič, Maša,. University of Pennsylvania Journal of International Law, Forthcoming; Tilburg Law School Research Paper No. 09/2016.

5. Acquisti, Alessandro and Taylor, Curtis R. and Wagman, Liad, The Economics of Privacy (March 8, 2016). Journal of Economic Literature, Vol. 52, No. 2, 2016; Sloan Foundation Economics Research Paper No. 2580411. Available at SSRN: https://ssrn.com/abstract=2580411

6. Ageing Report 2012: Economic and budgetary projections for the 27 EU Member States (2010-2060), chapter 3 https://ec.europa.eu/digital-agenda/en/news/ehealth-action-plan-2012-2020-innovative-healthcare-21st-century

7. Anita L. Allen, Uneasy Access: Privacy for Women in a Free Society (1988)

8. APPFALL 'Threats to Consumers in Mobile Apps' Report of the Norwegian Consumer Council March, 2016

9. Apple announces effortless solution bringing health records to iPhone, 24th January 2018, https://www.apple.com/newsroom/2018/01/apple-announces-effortless-solution-bringing-health-records-to-iPhone/ last visited 29.01.2018

10. Apple: ResearchKit is a pipeline for future diagnostic medical apps, October 15, 2015 http://mobihealthnews.com/47611/apple-researchkit-is-a-pipeline-for-future-diagnostic-medical-apps/

11. Apps as Artifacts: Towards a Critical Perspective on Mobile Health and Medical Apps - Deborah Lupton , Societies 2014, 4(4), 606-622; doi:10.3390/soc4040606, http://www.mdpi.com/2075-4698/4/4/606/htm

12. Article 29 Working Party ,Guidelines on the right to data portability', WP242 Adopted on 13 December 2016

13. Article 29 Working Party ,Guidelines on the right to data portability', WP242 Adopted on 13 December 2016, As last Revised and adopted on 5 April 2017

14. Article 29 Working Party Advice Paper on Special Categories of Data (sensitive data). http://ec.europa.eu/justice/dataprotection/article29/documentation/otherdocument/files/2011/2011_04_20_letter_artwp_mme_le_bail_directive_9546ec_annex1_en.pdf

15. Article 29 Working Party document No WP 105: ‘Working document on data protection issues related to RFID technology’, adopted on 19.1.2005, p. 8

16. Article 29 Working Party, Guidelines on consent under Regulation 2016/679, WP 259 rev.01, Adopted on 28 November 2017 As last Revised and Adopted on 10 April 2018

17. Article 29 Working Party, Opinion 05/2014 on Anonymisation Technique, adopted on 10 April 2014, WP216

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

19. Article 29 Working Party, Opinion 8/2014 on the on Recent Developments on the Internet of Things, adopted September 2014, WP 223

20. 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 adopted, 20.03.2016

21. Article 29 Working party, WP 168, 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, Adopted on 1st December 2009

22. Article 29 WP ANNEX-health data in apps and devices’, 2015

23. Article 29 WP Guidelines on consent under Regulation 2016/679, Adopted on 28 November 2017, as last revised and adopted on 10 April 2018, WP 259

24. Article 29 WP Opinion 02/2013 on apps on smart devices, WP 202, Adopted on 27 February 2013

25. Article 29 WP Opinion 15/2011 on the definition of consent , WP187, Adopted 13 July 2011

26. Article 29 WP Opinion 2/2017 on data processing at work, WP249, Adopted on 8 June 2017

27. Article 29 WP, Advice paper on special categories of data (‘sensitive data’), 20/04/2011

28. Article 29 WP, Opinion 03/2013 on purpose limitation, WP 203

29. Article 29 WP, Opinion 06/2013 on open data and public sector information ('PSI') reuse, WP 207, Adopted on 5 June 2013

30. Article 29 WP, Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, WP 217, Adopted on 9 April 2014

31. Article 29 WP, Opinion 13/2011 on Geolocation services on smart mobile devices, WP 185, 16 May 2011

32. Article 29 WP, Opinion 9/2014 on the application of Directive 2002/58/EC to device fingerprinting WP 224, Adopted on 25 November 2014

33. Beyond the OECD Guidelines: Privacy Protection for the 21st Century, Roger Clarke, 2000, http://www.rogerclarke.com/DV/PP21C.html

34. Book eHealth: Legal, Ethical and Governance Challenges, Carlisle George – Diane Whitehouse-Penny Duquenoy

35. Book eHealth: Legal, Ethical and Governance Challenges, Carlisle George – Diane Whitehouse-Penny Duquenoy

36. Cabello, F., Franco, M. G. & Haché, A. (2013). The social web beyond 'walled gardens': interoperability, federation and the case of Lorea/N-1. PsychNology Journal, 11(1), 43–65, from www.psychnology.org

37. Case C-212/13, Mr Ryneš vs Office for Personal Data Protection, judgment of the CJEU of 11.12.2014

38. Case No COMP/M.7217 - FACEBOOK/ WHATSAPP, Regulation (EC) No 139/2004 Merger Procedure, Date: 03/10/2014

39. Chances and Risks of Mobile Health Apps (CHARISMHA) – Albrecht, Urs-Vito, Hannover Medical School, 2016.

40. Charles Fried, 'Privacy [a moral analysis],' in Philosophical Dimensions of Privacy: An Anthology. New York: Cambridge University Press, 1968, pp. 333-345.

41. CJEU Patrick Breyer v Federal Republic of Germany, Case C-582/14, 19 October 2016,

42. CJEU, C-101/01, Criminal proceedings against Bodil Lindqvist, 6 November 2003, para. 47

43. CJEU, C-131/12, Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González [GC], 13 May 2014

44. CJEU, C-70/10, Scarlet v Sabam, 24 November 2011, par. 51, The case is concerning Scarlet's refusal to install a system for filtering electronic communications which use file-sharing software ('peer-to-peer'), with a view to preventing file sharing which infringes copyright.

45. CJEU, Joined cases C-92/09 and C-93/02, Volker und Markus Schecke GbR v. Land Hessen, Opinion of Advocate General Sharpston, 17 June 2010

46. Code and Privacy or How Technology is Slowly Eroding Privacy - R.Leenes &Bert-Jaap Koops

47. COM (90) 314 final, 13.9.1990

48. 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 realise, Brussels, 25 January 2012, http://europa.eu/rapid/press-release_IP-12-46_en.htm?locale=en

49. COMMISSION STAFF WORKING DOCUMENT A Digital Single Market Strategy for Europe - Analysis and Evidence Accompanying the document Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions A Digital Single Market Strategy for Europe, {COM(2015) 192 final}, Brussels, 6.5.2015

50. Commission staff working document on the applicability of the existing EU legal framework to telemedicine services Communication from the commission to the European parliament, the council, the European economic and social committee and the committee of the eHealth Action Plan 2012-2020 – innovative healthcare for the 21st century, Brussels, 6.12.2012

51. Commission staff working paper- Impact Assessment Accompanying the document 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 Regula-

tion) and Directive of the European Parliament and of the Council on the prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data SEC (2012) 72 final

52. Commission staff working paper- Impact Assessment Accompanying the document 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) and Directive of the European Parliament and of the Council on the prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data SEC (2012) 72 final

53. Commitment in Case COMP/C-3/39.740 - *Foundem and others*, April 3, 2013

54. Comparative Study on Different Approaches to new Privacy Challenge's in Particular in the light of the technological developments - January, 2010 European Commission, DG Justice, Freedom and Security.
http://ec.europa.eu/justice/policies/privacy/docs/studies/new_privacy_challenges/final_report_en.pdf

55. Consolidated version of the Treaty on the Functioning of the European Union';

56. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Jan. 28, 1981 [Convention 108], available at:
http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm.

57. Cortez, Nathan, The Mobile Health Revolution? (June 24, 2013). UC Davis Law Review, Vol. 47, 2104; SMU Dedman School of Law Legal Studies Research Paper No. 128. Available at SSRN: http://ssrn.com/abstract=2284448 or http://dx.doi.org/10.2139/ssrn.2284448

58. COUNCIL DIRECTIVE 93/42/EEC of 14 June 1993 concerning medical devices

59. Council of the European Union, Interinstitutional File: 2012/0011 (COD), Working Group on Information Exchange and Data Protection (DAPIX), 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)- Data Portability (Revision of Article 18) Brussels, 6 June 2014, 10614/14

60. Council Regulation (EC) No 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States

61. Council Regulation 1/2003 of 16 December 2002 on the implementation of the rules on competition laid down in Articles 81 and 82 of the Treaty [2002], OJ L1/1. See more on: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32003R0001

62. Court of Justice of the EU (Grand Chamber), judgment of 9.11.2010, Joined cases C-92/09 and C-93/09. Volker und Markus Schecke GbR (C-92/09) and Hartmut Eifert (C-93/09) v Land Hessen,Judgment, [2010] ECR I-0000

63. Data Portability - A Tale of Two Concepts, Prof. Dr. Ruth Janal, JIPITEC – Journal of Intellectual Property, Information Technology and E-Commerce Law 8 (2017) JIPITEC 59 para 1.
https://www.jipitec.eu/issues/jipitec-8-1-2017/4532

64. Data Protection Report, Special Eurobarometer 431, Fieldwork: March 2015, Publication: June 2015. This survey has been requested by the European Commission, Directorate-General for Justice and Consumers and coordinated by the Directorate-General for Communication.

65. Data Transfer, Project https://datatransferproject.dev/ last visited on 22.07.2018

66. de Korte EM, Wiezer N, Janssen JH, Vink P, Kraaij WEvaluating an mHealth App for Health and Well-Being at Work: Mixed-Method Qualitative Study JMIR Mhealth Uhealth 2018;6(3):e72

67. Decision No 922/2009/EC of the European Parliament and of the Council of 16 September 2009 on interoperability solutions for European public administrations (ISA) OJ L 260, 03.10.2009

68. Delphine Christin, Andreas Reinhardt, Salil S. Kanhere, Matthias Hollick: A Survey on Privacy in Mobile Participatory Sensing Applications. In: Elsevier Journal of Systems and Software, vol. 84, no. 11, p. 1928--1946, November 2011. Page. 8

69. Diet and Physical Activity Apps: Perceived Effectiveness by App Users, Wang Q, Egelandsdal B, Amdam GV, Almli VL, Oostindjer M JMIR mHealth uHealth 2016;4(2):e33, DOI: 10.2196/mhealth.5114, http://mhealth.jmir.org/2016/2/e33/

70. Digital economy - Promise and peril in the age of networked intelligence, Don Tapscott June 1997 (ISBN-10: 0070633428, ISBN-13: 978-0070633421)

71. Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC (Text with EEA relevance)

72. Directive 2002/19/EC of the European Parliament and of the Council of 7 March 2002 on access to, and interconnection of, electronic communications networks and associated facilities (Access Directive), Article 4 (1)

73. Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive)

74. Directive 2002/22/EC of the European Parliament and of the Council of 7 March 2002 on universal service and users' rights relating to electronic communications networks and services (Universal Service Directive).

75. DIRECTIVE 2003/98/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 17 November 2003 on the re-use of public sector information

76. Directive 2009/24/EC of the European Parliament and of the Council of 23 April 2009 on the legal protection of computer programs

77. Directive 2011/24/EU on the application of patients' rights in cross-border healthcare
78. Directive 93/42/EEC concerning medical devices

79. 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 , http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML

80. Draft Code of Conduct on privacy for mobile health applications, 2015

81. Draft code of conduct on privacy for mobile health applications', European Commission, 2016

82. DRAFT REPORT with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL)). European Parlament, Comittee on Legal affairs, 31.05.2016

83. Drexl, Josef and Hilty, Reto and Globocnik, Jure and Greiner, Franziska and Kim, Daria and Richter, Heiko and Slowinski, Peter R. and Surblyte, Gintare and Walz, Axel and Wiedemann, Klaus, Position Statement of the Max Planck Institute for Innovation and Competition of 26 April 2017 on the European Commission's 'Public consultation on Building the European Data Economy' (April 26, 2017). Max Planck Institute for Innovation & Competition Research Paper No. 17-08.

84. Driving Innovation in Health Systems through an Apps-Based Information Economy - Mandel et al., Published online 2015 June 11. doi: 10.1016/j.cels.2015.05.001. http://europepmc.org/articles/PMC4556429#R2

85. ECHR, CASE OF NIEMIETZ v. GERMANY, Application no. 13710/88,16 December 1992

86. ECHR, CASE OF TYRER v. THE UNITED KINGDOM, Application no. 5856/72,25 April 1978

87. ECJ Joined Cases C-465/00, C-138/01 and C-139/01 2003, Rechnungshof v Österreichischer Rundfunk and Others and Christa Neukomm and Joseph Lauermann v Österreichischer Rundfunk, paragraph 70; Case C-101/01 2003, Criminal proceedings against Bodil Lindqvist, Paragraph 99; Case C-73/07 Tietosuojavaltuutettu v Satakunnan Markkinapörssi Oy and Satamedia Oy 2008

88. ECtHR, Bernh Larsen Holding AS and Others v. Norway, No. 24117/08, 14 March 2013.

89. EDPS Opinion 1/2015 Mobile Health, 21 May 2015.

90. EDPS recommendations on the EU's options for data protection reform, (2015/C 301/01)

91. eHealth and Privacy in U.S. Employer Wellness Programs, Anna Slomovic May 2015, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2613452

92. eHealth: Legal, Ethical and Governance Challenges, Carlisle George – Diane Whitehouse-Penny Duquenoy

93. Engaging Privacy and Information Technology in a Digital Age, James Waldo,Herbert S. Lin, and Lynette I. Millett, editors, 2007.

94. Enhancing data protection globally: Council of Europe updates its landmark convention - Council of Europe, Elsinore (Danemark) 18 May 2018.

95. ePrivacy Directive (2002/58/EC, as revised by 2009/136/EC)

96. Eugenio Mantovani, Paul Quinn, mHealth and data protection – the letter and the spirit of consent legal requirements, Article in International Review of Law Computers & Technology March 2013, DOI: 10.1080/13600869.2013.801581

97. Eugenio Mantovani, Paul Quinn, mHealth and data protection – the letter and the spirit of consent legal requirements, Article in International Review of Law Computers & Technology March 2013, DOI: 10.1080/13600869.2013.801581

98. European Charter of Human Rights

99. European Commission, experts uneasy over WP29 data portability interpretation, The Privacy Advisor, Published April 2017,

100. European Committee for Interoperable Systems, Special Paper on Cloud Computing: Portability and Interoperability, June 27, 2016

101. European Court of Human Rights, I. v. Finland - 20511/03, Judgment 17.7.2008,

102. European Court of Justice, College van burgemeester en wethouders van Rotterdam v M.E.E. Rijkeboer, Case C-553/07, May 2009

103. European Data protection Supervisour, Guidelines on the protection of personal data processed by mobile applications provided by European Union institutions, November 2016

104. European Data Protection Supervisour, Opinion 1/2015 Mobile Health Reconciling technological innovation with data protection, 21 May 2015

105. European mHealth Initiative, Draft Code of Conduct on privacy for mobile health applications, On 7 June 2016,

106. European Parliament legislative resolution of 12 March 2014 on the 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) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)) (Ordinary legislative procedure: first reading),

107. Explanatory Report of Modernised Convention 108

108. FDA Mobile Medical Applications - Guidelines for Industry and Food and Drug Administration Staff, September 2013

109. Fitbit and Google Announce Collaboration to Accelerate Innovation in Digital Health and Wearables - Fitbit to leverage Google Cloud to increase operational efficiency, agility and speed to market, Press release, 04/30/2018 https://investor.fitbit.com/press/press-releases/press-release-details/2018/Fitbit-and-Google-Announce-Collaboration-to-Accelerate-Innovation-in-Digital-Health-and-Wearables/default.aspx

110. France in October 2016 adopted legislative act on data retrial and data portability, which entered into force in May 2018. Art.L-224-42-1-L.224-42-4. It oblige online public communication service to allow consumer a free recovery of online data posted by the consumer, according to Article 20 (right to data portability) in the GDPR

111. From patient centred to people powered: autonomy on the rise, Dave de Bronkart *speaker, policy adviser, and co-chair, BMJ* 2015;350:h148 doi: 10.1136/bmj.h148 (Published 10 February 2015

112. Gasser, Urs. 2015. 'Interoperability in the Digital Ecosystem.'Berkman Klein Center for Internet and Society Research Publication No. 2015

113. Gavison, Ruth E., Privacy and the Limits of Law (May 16, 2012). The Yale Law Journal, Vol. 89, No. 3 (Jan., 1980), pp. 423 Available at SSRN: http://ssrn.com/abstract=2060957

114. Google Cloud - New collaboration with Fitbit to drive positive health outcomes, Google blog, Published 30.04.2018 https://blog.google/topics/google-cloud/new-collaboration-fitbit-drive-positive-health-outcomes/

115. Google to Facebook: You can't import our user data without reciprocity, published Nov. 5 2010 https://techcrunch.com/2010/11/04/facebook-google-contacts/

116. Graef, Inge and Husovec, Martin and Purtova, Nadezhda, Data Portability and Data Control: Lessons for an Emerging Concept in EU Law (December 15, 2017). TILEC Discussion Paper No. 2017-041; Tilburg Law School Research Paper No. 2017/22. Available at SSRN: https://ssrn.com/abstract=3071875 or http://dx.doi.org/10.2139/ssrn.3071875

117. Graef, Inge and Verschakelen, Jeroen and Valcke, Peggy, Putting the Right to Data Portability into a Competition Law Perspective (2013). Law: The Journal of the Higher School of Economics, Annual Review, 2013, pp. 53-63. Available at SSRN: https://ssrn.com/abstract=2416537

118. Graef, Inge and Verschakelen, Jeroen and Valcke, Peggy, Putting the Right to Data Portability into a Competition Law Perspective (2013). Law: The Journal of the Higher School of Economics, Annual Review,

119. Graef, Inge and Verschakelen, Jeroen and Valcke, Peggy, Putting the Right to Data Portability into a Competition Law Perspective (2013). Law: The Journal of the Higher School of Economics, Annual Review, 2013, pp. 53-63. Available at SSRN: https://ssrn.com/abstract=2416537

120. Graef, Inge, Mandating Portability and Interoperability in Online Social Networks: Regulatory and Competition Law Issues in the European Union (July 22, 2013). Telecommunications Policy 2015, Vol. 39, No. 6,

121. Green Paper on the European Workforce for Health COM(2008) 725 final of 10.12.2008 http://ec.europa.eu/health/ph_systems/docs/workforce_gp_en.pdf

122. GSMA Intelligence, Definitive data and analysis of the mobile industry, Global Mobile Trends 2017

123. Handbook on European data protection law 2018 edition, CoE: ISBN 978-92-871-9849-5, April 2018

124. Health 4.0: How Virtualization and Big Data are Revolutionizing Healthcare, edited by Christoph Thuemmler, Chunxue Ba, Springer 2017 (DOI 10.1007/978-3-319-47617-9),

125. Helsinki Declaration 1964.

126. History of Mobile Applications, Theory and Practice of Mobile Applications Professor John F. Clark

127. History of Telemedicine Evolution, Context, and Transformation, Rashid L. Bashshur, Ann Arbor, Michigan, Gary W. Shannon 2009, Print ISBN: 1-934854-11-5

128. How smartphones are changing the face of mobile and participatory healthcare: an overview, with example from eCAALYX. Boulos MN, Wheeler S, Tavares C, Jones R. 2011.Biomed Online. 10,24. .10.1186/1475-925X-10-24 http://europepmc.org/articles/PMC3959919;jsessionid=8weYDTrgw1gGUrWyma29.0#r2

129. ICO Privacy in mobile apps. Guidelines for app developers December 2013 https://ico.org.uk/media/for-organisations/documents/1596/privacy-in-mobile-apps-dp-guidance.pdf

130. Impact Assessment, Brussels, 25.1.2012 SEC(2012) 72 final

131. Improving Privacy Protection in the area of Behavioural Targeting, Frederik Zuiderveen Borgesius, 2014, p.166

132. International Chamber of Commerce (ICC) Comments on EU Directive: 95/46/EC COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS 'A comprehensive approach on personal data protection in the European Union' January 2011

133. Interoperability Case Study-The European Union as an Institutional Design for Legal Interoperability, Félix Tréguer 2012 The Berkman Center for Internet & Society at Harvard University

134. Interoperability framework for communication between processes running on different mobile operating systems, A Gal et al, 2016 IOP Conf. Ser.: Mater. Sci. Eng.106/012007

135. Interoperability in the Digital Ecosystem - Urs Gasser 2015, The Berkman Center for Internet & Society at Harvard University

136. Is the GDPR and Its Right to Data Portability a Major Enabler of Citizen Science? Paul Quinn, Published June 2018 Global Jurist, DOI: 10.1515/gj-2018-0021, https://www.researchgate.net/publication/325635784_Is_the_GDPR_and_Its_Right_to_Data_Portability_a_Major_Enabler_of_Citizen_Science

137. iWander: An Android application for dementia patients. Sposaro F, Danielson J, Tyson G, Conf Proc IEEE Eng Med Biol Soc 2010, 2010:3875-3878 http://europepmc.org/abstract/MED/21097072

138. J.H.Moor,'Towards a theory of privacy in the information age,' ACM SIGCAS Computers and Society vol. 27, pp. 27-32, 1997.

139. Josef Drexl, Reto M. Hilty, Jure Globocnik,Franziska Greiner, Daria Kim,Heiko Richter,Peter R. Slowinski, Gintarė Surblytė, Axel Walz, Klaus Wiedemann Position Statement of the Max Planck Institute for Innovation and Competition on the European Commission's 'Public consultation on Building the European Data Economy' 26 April 2017, page 10

140. Judgement of the court of first instance (Grand Chamber), Microsoft Corp. v Commission of the European Communities, Case T-201/04, 17 September 2007

141. Judgement of the European Court of Justice, Lindqvist Case C-101/01, 6 November 2003

142. Judgment of the Court (Fourth Chamber), Case C-291/12, Michael Schwarz v Stadt Bochum, 17 October 2013, par.32

143. Judgment of the Court (Grand Chamber) Maximillian Schrems v Data Protection Commissioner, Case C-362/14, 6 October 2015

144. Kuner, Christopher, The Court of Justice of the EU Judgment on Data Protection and Internet Search Engines (September 15, 2014). Final version published as 'The Court of Justice of the EU Judgment on Data Protection and Internet Search Engines: Current Issues and Future Challenges', in: Burkhard Hess and Cristina M. Mariottini (eds.), Protecting Privacy in Private International and Procedural Law and by Data Protection 19-55 ; LSE Legal Studies Working Paper No. 3/2015

145. Legal Interoperability as a Tool for Combatting Fragmentation, Global Commission on Internet Governance Paper Series: No.4-December 2014 Rolf H. Weber

146. Lupton, Deborah. 2012. 'M-Health and Health Promotion: The Digital Cyborg and Surveillance Society.' Social Theory & Health, http://www.palgrave-journals.com/sth/journal/v10/n3/full/sth20126a.html

147. M. R. Koot, Measuring and Predicting Anonymity, Amsterdam: Informatics Institute cop., 2012, p 101 http://dare.uva.nl/document/2/107610

148. Malgieri, Gianclaudio and Comandé, Giovanni, Sensitive-By-Distance: Quasi-Health Data in the Algorithmic Era (May 2, 2017). Information, Communication and Technology Law, Issue n. 3, 2017 (Forthcoming

149. Mandating portability and interoperability in online social networks: Regulatory and competition law issues in the European Union, , Inge Graef, Telecommunications Policy Volume 39, Issue 6, July 2015

150. Mantovani, Eugenio, and Paul Quinn. 2014. 'mHealth and Data Protection–the Letter and the Spirit of Consent Legal Requirements.' International Review of Law, Computers & Technology

151. Manual on borderline and classification in the community regulatory framework for medical devices Version 1.16 (07-2014) http://ec.europa.eu/health/medicaldevices/files/wg_minutes_member_lists/borderline_manual_ol_en.pdf

152. Mapping mHealth Research: A Decade of Evolution, Maddalena Fiordelli, Nicola Diviani,Peter J Schulz -Institute of Communication and Health, Faculty of Communication Sciences, University of Lugano, Switzerland, Pub. online 2013 May 21. doi: 10.2196/jmir.2430 http://www.ncbi.nlm.nih.gov/pmc/articles/PMC3668610/

153. mHealth App Developer Economic 2014 – The State of the Art of mHealth App Publishing

154. mHealth App Economics 2017, Current Status and Future Trends in Mobile Health-How digital intruders are taking over the healthcare market, Research 2Guidance, Published November 2017, page 10

155. mHealth Digital Agenda for Europe – https://ec.europa.eu/digital-agenda/en/mhealth last visited 03.06.2015

156. Mobile Health - A technology Road Map, Sasan Adibi Editor-Faculty of Science Engineering & Built Environment School of Information Technology Burwood, Victoria Australia, Springer Series in Bio-/Neuroinformatics Volume 5-2015

157. Mobile medical and health apps: state of the art, concerns, regulatory control and certification, Maged N. Kamel Boulos, Ann C. Brewer, Chante Karimkhani, David B. Buller, and Robert P. Dellavalle, Online J Public Health Inform. 2014; 5(3): 229 http://www.ncbi.nlm.nih.gov/pmc/articles/PMC3959919/

158. Mobile Privacy Disclosures FTC Staff Report | February 2013 # Building Trust Through Transparency, page 15

159. Mobile technology supporting trainee doctors' workplace learning and patient care: an evaluation.Hardyman W, Bullock A, Brown A, Carter-Ingram S, Stacey M. 2013. BMC Med Educ. 13, 6 10.1186/1472-6920-13-6, http://europepmc.org/articles/PMC3552772/

160. Moore, Adam D., Privacy (2007). Library Hi Tech, Vol. 25, pp. 58-78, 2007

161. Moro Visconti, Roberto and Larocca, Alberto and Marconi, Michele, Big Data-Driven Value Chains and Digital Platforms: From Value Co-Creation to Monetization (January 18, 2017). Available at SSRN: https://ssrn.com/abstract=2903799 or http://dx.doi.org/10.2139/ssrn.2903799

162. Nike ends privacy violations in running app after investigation by Dutch DPA, Dutch Data Protection Authorities, November 2016

163. Norwegian Consumer Council, Research '250,000 words of app terms and conditions' - Published 24. may, 2016

164. OECD Guidelines on the Protection of Privacy and Trans border Flows of Personal Data -The Recommendation was adopted and became applicable on 23 September 1980, http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

165. Ohm, Paul, Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization (August 13, 2009). UCLA Law Review, Vol. 57, p. 1701, 2010; U of Colorado Law Legal Studies Research Paper No. 9-12. Available at SSRN: https://ssrn.com/abstract=1450006

166. Opinion 1/ 2015 Mobile Health, 21 May 2015, European Data Protection Supervisor

167. Optimized - Lifelogging and Quantified Self Improvement App https://itunes.apple.com/us/app/optimized-lifelogging-quantified/id785042895?mt=8

168. Orientierungshilfe zu den Datenschutzanforderungen an App-Entwickler und App-Anbieter, Bayerisches Landesamt für Datenschutzaufsicht, 16 Juni 2014

169. Oviedo Convention on Human Rights and Biomedicine No. 164, Oviedo, 4.4.1997

170. Privacy and Data Protection Issues of Biometric Applications - A Comparative Legal Analysis, Springer edition eBook ISBN 978-94-007-7522-0, Kindt, Els J. 2013

171. PRIVACY AND MHEALTH: HOW MOBILE HEALTH 'APPS' FIT INTO A PRIVACY FRAMEWORK NOT LIMITED TO HIPAA 2014, Anne Marie Helm, Daniel Georgatos, University of California-Hasting College of the Law

172. Privacy in mobile apps - Guidance for app developers; ICO (Information Commissioners Office), December 2013 https://ico.org.uk/media/for-organisations/documents/1596/privacy-in-mobile-apps-dp-guidance.pdf

173. Proposal for a Directive of the European Parliament and of the Council on certain aspects concerning contracts for the supply of digital content, Brussels, 9.12.2015 COM(2015) 634 final, 2015/0287(COD)

174. Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on certain aspects concerning contracts for the supply of digital content COM/2015/0634 final - 2015/0287 (COD)

175. Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the re-use of public sector information (recast), Brussels, 25.4.2018, COM(2018) 234 final, 2018/0111(COD)

176. Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the re-use of public sector information (recast), Brussels, 25.4.2018, COM(2018) 234 final, 2018/0111(COD)

177. Proposal for a Regulation of the European Parliament and of the Council on a framework for the free flow of non-personal data in the European Union (COM(2017)495), Brussels, 13.9.2017

178. Purtova, N., E. Kosta, and B.J. Koops. 2014. Chapter 3 'Laws and Reputation for Digital Health.' Page 47-74, Springer Edition "Requirements Engineering for Digital Health" - eBook ISBN, 978-3-319-09798-5

179. Realising the right to data portability for the domestic Internet of things, Lachlan Urquhart, Neelima Sailaja DOI 10.1007/s00779-017-1069-2, Published online 23 August 2017

180. REPORT on the 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) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)) Committee on Civil Liberties, Justice and Home Affairs Rapporteur: Jan Philipp Albrecht, A7-0402/2013, 21.11.2013 page 87

181. REPORT on the 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) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)) Committee on Civil Liberties, Justice and Home Affairs Rapporteur: Jan Philipp Albrecht, A7-0402/2013, 21.11.2013 page 24

182. Samuel D. Warren & Louis D. Brandeis, The Right to Privacy, Harvard Law Review, V. IV, No. 5, December 1890

183. Smartphones set to boost large-scale health studies, International weekly journal of science'Nature' http://www.nature.com/news/smartphones-set-to-boost-large-scale-health-studies-1.17083, last visited 20.03.2015

184. Solove, Daniel J. and Schwartz, Paul M., 'Reconciling Personal Information in the United States and European Union' (2013).GWLaw Faculty Publications & Other Works.Paper 956. http://scholarship.law.gwu.edu/faculty_publications/956

185. Solove, Daniel J., Conceptualizing Privacy. California Law Review, Vol. 90, p. 1145, 2002. Available at SSRN:

186. Solove, Daniel J., Conceptualizing Privacy. California Law Review, Vol. 90, p. 1090, 2002. Available at SSRN:

187. Standard Glossary of Software Engineering Terminology' (IEEE 610.12-1990)

188. Swire, Peter and Lagos, Yianni, Why the Right to Data Portability Likely Reduces Consumer Welfare: Antitrust and Privacy Critique (May 31, 2013). 72 Maryland Law Review 335 (2013); Ohio State Public Law Working Paper 204. Available at SSRN: https://ssrn.com/abstract=2159157 or http://dx.doi.org/10.2139/ssrn.2159157

189. Technical Analysis of the Data Practices and Privacy Risks of 43 Popular Mobile Health and Fitness Applications, Craig Michael Lie Njie, Released August 12, 2013

190. The development and feasibility of a web-based intervention with diaries and situational feedback via smartphone to support self-management in patients with diabetes type 2. Nes AA, van Dulmen S, Eide E, Finset A, Kristjansdottir OB, et al. 2012. Diabetes Res Clin Pract. 97(3), 385-93 10.1016/j.diabres.2012.04.019 http://europepmc.org/abstract/MED/22578890

191. The digitally engaged patient: Self-monitoring and self-care in the digital health era, Debora Lupton, Social Theory & Health (2013) 11, 256–270

192. The Emergence of Personal Data Protection as a Fundamental Right of the EU, ISSN 2352-1902 ISSN 2352-1910 (electronic), 2014 By Gloria González Fuster

193. The ePrivacy directive (2002/58/EC, as revised by 2009/136/EC). In January 2017 is adopted Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) Brussels, 10.1.2017 COM(2017) 10 final 2017/0003 (COD)

194. The Google antitrust case: what is at stake? Speech of Joaquín Almunia - Former Vice President of the European Commission responsible for Competition Policy. October 2013, http://europa.eu/rapid/press-release_SPEECH-13-768_en.htm

195. The lifestylisation of healthcare? 'Consumer genomics' and mobile health as technologies for healthy lifestyle - Applied &Translational Genomics, Volume 4, March 2015, pages 44-49, Federica Lucivero, , Barbara Prainsack http://dx.doi.org/10.1016/j.atg.2015.02.001

196. The OECD Digital Economy Papers series covers a broad range of ICT-related issues and makes selected studies available to a wider readership. OECD Digital Economy Papers

197. The place of Privacy in Data Protection law, Lee A.Bygrave, 2001

198. The Privacy, Data Protection and Cybersecurity Law Review - Germany, The Law Reviews Edition 4, Nikola Werry, Benjamin Kirschbaum, Jens-Marwin Koch, Published December 2017.

199. The right to Data portability in the context of the EU data protection reform, Gabriela Zanfir, International Data Privacy Law Advance Access published May 11, 2012

200. The right to data portability in the GDPR: Towards user-centric interoperability of digital services, Paul De Hert,Vagelis Papakonstantinou, Gianclaudio Malgieri, Laurent Beslay, Ignacio Sanchez, Computer Law & Security Review, Volume 34,

201. The Two Western Cultures of Privacy: Dignity versus Liberty, 2014 James Q. Whitman, Yale Law School

202. The Universal Declaration of Human Rights (UDHR).

203. These companies are tracking the fitness of their employees, Guardian Monday 17 March 2014 https://www.theguardian.com/technology/2014/mar/17/why-companies-are-tracking-the-fitness-of-their-employees

204. Trust but verify - five approaches to verify safety medical apps 2015 – September 2015-BMC Medicine 13(1):205, DOI: 10.1186/s12916-015-0451-z, LicenseCC BY 4.0 , Paul Wick and Emil Chiazzi

205. UK ICO, The Guide to the General data protection Regulation , Right to data portability, https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/?template=pdf&patch=42#link25

206. UK's Information Commissioner Office's (ICO) analysis on the GDPR during the negotiations.

207. Unique in the Crowd: The privacy bounds of human mobility, Yves-Alexandre de Montjoye, César A. Hidalgo, Michel Verleysen & Vincent D. Blondel, Published online: 25 March 2013 https://www.nature.com/articles/srep01376

208. Universal Declaration on Bioethics and Human Rights of the 2005

209. Updating the law of Information Privacy: The new framework of the European Union, Marc Rotenberg &David Jacobs

210. Vision on eHealth European Interoperability Framework - A study prepared for the European Commission DG Connect, 2013

211. What is e-health? Gunther Eysenbach, J Med Internet Res. 2001 Apr-Jun; 3(2): e20.

212. What is the Internet of medical things? The Journal of mHealth, A White paper by Intersog, October 2016

213. WHO - Global Observatory of eHealth services, mHealth: new Horisons for health through mobile technologies 2011,http://www.who.int/goe/publications/ehealth_series_vol3/en

214. Widespread Deployment of Telemedicine Services in Europe Report of the eHealth Stakeholder Group on implementing the Digital Agenda for Europe Key Action 13/2 'Telemedicine' Version 1.0 final (12 March 2014)

215. Wolfgang Kerber, Heike Schweitzer, Interoperability in the Digital Economy, 8 (2017) JIPITEC 39 para 1.

216. Working Party on Security and Privacy in the Digital Economy, OECD privacy expert roundtable, Protecting Privacy in a Data-driven Economy: Taking Stock of Current Thinking 21 March 2014, page 5

217. World Economic Forum ‘Rethinking Personal Data: A New Lens for Strengthening Trust’, May 2014

218. Zombie’s run https://zombiesrungame.com/