The issues of the protection of health, biometric and genetic data in regard to the General Data Protection Regulation (GDPR) and the new technologies concerning the health care sector.

Victoria Dipla

SCHOOL OF ECONOMICS, BUSINESS ADMINISTRATION & LEGAL STUDIES

A thesis submitted for the degree of

Master of Science (MSc) in Bioeconomy: Biotechnology and Law

November 2019

Thessaloniki – Greece

Student Name: Victoria Dipla

SID:
Supervisor: Dr. Panagiotis Vidalis

I hereby declare that the work submitted is mine and that where I have made use of another's work, I have attributed the source(s) according to the Regulations set in the Student's Handbook.

November 2019
Thessaloniki - Greece

Abstract

This dissertation was written as part of the MSc in Bioeconomy: Biotechnology and Law, at the International Hellenic University.
The work is divided into two large chapters, one concerning the protection of health, genetic and biometric data under the scope of the General Data Protection Regulation and the relevant national legal frameworks, from Europe and the United States, and the second relating to emerging new technologies applicable to the healthcare sector. The first part provides a definition of this set of data and the way it was handled and regulated from the prior legislation. In addition, a specific emphasis is given in the Greek legislation in comparison with other national legal documents from European countries, as well as the existing provisions for the protection of sensitive data in the United States.
Secondly, the dissertation aims to provide a comprehensive presentation of new technologies that are both amongst the most pioneering of the field but also amongst the most popular and incorporate in the life of a large number of the population, being either afflicted by a disease or not. Such cases constitute the direct-to-consumer genetic testing, mobile health applications, robotics, and AI. They are presented in a way that illustrates the legal provisions that regulate them, deriving from different parts of the world, like Europe and the US. There is also an examination of the ethical questions arising from the use of such technological innovations, and both the international and European point of view on the matter.

Keywords: GDPR, privacy, healthcare, technology, AI

Victoria Dipla
Date 29/11/2019

Preface

I would like to acknowledge the indispensable contribution to this dissertation of my supervisor Dr. Vidalis, with his never-ending interest to my efforts and to the enrichment of the final document, his aid was of incredible importance, without which it wouldn't have been possible to complete such a daunting task. In addition, I would also like to acknowledge the aid of Dr. Lilian Mitrou, especially relating to the first part of the dissertation, as her guidance on matters concerning the GDPR was of immeasurable value. Last but not least, the assistance coming from the National Hellenic Bioethics Commission deserves a special acknowledgment, as it was because of their support and effort to aid me that I had the chance to add valuable content to this document.

Contents

Introduction

Nowadays after the coming into force of the new General Data Protection Regulation[1], regulating a need which is the outcome of the advance of technology and the capability to store and process an immeasurable amount of data, a new domain of research has also immerged, in combination to the evolution in health, genetic and biometric data information and innovation technology .

Research on the essence and definition of the aforementioned category of data, known and described within the Regulation (henceforth GDPR), as sensitive personal information, sensitive data, is one of the main objectives of the present paper, amongst others. In addition, comparison and alignment of legislative means are to be further analyzed considering legal texts and rules produced prior to the GDPR and after within the EU borders, such as in Greece[2], UK, and Germany, but also outside EU regulation and jurisdiction, in the United States related provisions of the matter.

Furthermore, as it has been previously mentioned the emergence of new technologies capable of combining large amounts of data relating to health, genetic and biometric information about individuals, has brought forth the necessity of a high level of protection and safeguarding of the process. As a result, principles[3] and regulations, such as the GDPR, have been issued in an effort to update the law with technological innovations such as the Electronic Health Record (henceforth HER), Bio-banks and Direct to Consumer Genetic Testing, along with Mobile Health Applications, Artificial Intelligence technologies and Research & Development projects that involve themselves in the field of Robotics, especially in the health care sector and innovations in medicine.

Technology has allowed the modern society to advance its medical practices and treatment of its patients, through the use of the EHR system, the main method, and domain where health data are stored, thus the principal technological novelty to be examined in this paper, in relation to that form of data. Moreover, as far as it comes to genetic data storage, the principal institution(s) in the business of storing them on a large scale are bio-banks and most recently direct to consumer genetic testing technological companies, which will be the focal point of this analysis. Last but not least, biometric data storage and manipulation are frequently found amongst mobile health applications, posing a category of their own due to their accessibility by the public, alongside though artificial intelligence, algorithms and robotics alike, entail a whole new level of controversy on its own.

---

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation- GDPR).

[2]Νόμος 4624/2019, Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, μέτρα εφαρμογής του Κανονισμού (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και ενσωμάτωση στην εθνική νομοθεσία της Οδηγίας (ΕΕ) 2016/680 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 και άλλες διατάξεις.

[3] Centre for Data Ethics and Innovation, (12/09/2019), Snapshot Paper - AI and Personal Insurance, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/831181/Snapshot_Paper_-_AI_and_Personal_Insurance.pdf

The following examination shall be highlighting both the legal and ethical questions raised by the newly formed situation in data gathering starting with the legislation, providing a comparative work followed by major ethical[4] issues, regarding the aforementioned technological breakthroughs. Legal texts and their analysis will be provided commencing with the most influential one, leading to a European change in handling sensitive personal information, the General Data Protection Regulation, followed by related national provisions and in contradiction to international ones. (Federal[5] and non-federal[6] acts and statutes legislating relative parts concerning health data protection and cybersecurity).

GDPR constitutes a legal document seeking to unify and harmonize Member- States legislation with the objective to mitigate a concerning issue of the current time, data privacy, reforming an already obsolete directive[7] (Directive 95/46 EC), proposed by the European Commission.

[4] Anna Jobin, Marcello Ienca & Effy Vayena, (02/09/ 2019), The global landscape of AI ethics guidelines, Nature Machine Intelligence ,volume 1, pages389–399 (2019), https://www.nature.com/articles/s42256-019-0088-2

[5] Health Insurance Portability and Accountability Act (HIPAA)

[6] California Consumer Privacy Act of 2018 (CCPA), effective into force on January 1, 2020, Assembly Bill No. 375 ,CHAPTER 55An act to add Title 1.81.5 (commencing with Section 1798.100) to Part 4 of Division 3 of the Civil Code, relating to privacy.

[7] EUROPEAN DATA PROTECTION SUPERVISOR, *The History of the General Data Protection Regulation* : "It replaces the1995 Data Protection Directive which was adopted at a time when the internet was in its infancy".(https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en accessed online 11/10/2019).

CHAPTER A- General Data Protection Regulation (EU) 2016/679

The European Commission on January 25, 2012,[8] proposed the reforming of the legal framework within the EU borders, but also with extended territorial applicability, updating the rules applying to data privacy, a topic covered previously by the now outdated Directive 95/46/EC.

The outcome of years in preparation[9] was the General Data Protection Regulation (Regulation (EU) 2016/679 of the European Parliament and the Council), which came into full force on May 25th, 2018. The regulation[10] litigates a number of prerequisites and obligations for organizations working within the EU or having any kind of activity inside EU borders, aiming to protect individuals and particularly employees, safeguarding their fundamental freedoms and rights, amongst them the right to privacy.[11]

Part of the aforementioned legal reform constitutes the definition and specified protection for the processing of sensitive personal data[12], health, genetic and biometric data.

1. HEALTH DATA

Health data according to the GDPR, Article 4 §15, refer to the personal information regarding an individual's mental or physical health including data and information provided by the health care system or services, in relation to the health status of the subject of these data.[13]

According to the European Court of justice the "data related to health" is regarded and interpreted in a broader scope, with the objective of the Court being that of including in its definition any possible personal information, both on the psychology and mentality and of the physiology of a person. Thus, even data regarding a previous injury of an individual can be perceived as sensitive personal information/data[14].

---

[8] EUROPEAN DATA PROTECTION SUPERVISOR *The History of the General Data Protection Regulation* : "EC proposal to strengthen online privacy rights and digital economyThe European Commission proposes a comprehensive reform of the EU's 1995 data protection rules to strengthen online privacy rights and boost Europe's digital economy." (https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en accessed online 11/10/2019).

[9] EUROPEAN DATA PROTECTION SUPERVISOR, *The History of the General Data Protection Regulation* : "In 2016, the EU adopted the General Data Protection Regulation (GDPR) … The timeline below contains key dates and events in the data protection reform process from 1995 to 2018". (https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en accessed online 11/10/2019).

[10] Stefanos Tsimikalis, 05/03/2019, *GDPR & Employee Personal Data, by Tsimikalis Kalonarou Law Firm, http://www.greeklawdigest.gr/topics/data-protection/item/314-gpdr-and-employee-personal-data accessed online 11/10/19).*

[11] The Greek Constitution Article 9, Article 9A (right to privacy) & (right to protection of personal information, Article 2§1 (right to dignity) and Article 5 §1 (right to developing freely ones personality).

[12] Article 9 of the General Data Protection Regulation (EU) 2016/679.

[13] Article 4 §15 of the GDPR :data concerning health' means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status;

[14] Case C101-01, Bodil Lindqvist, 6 November 2003.

Pursuant to Recital 35 of the GDPR,[15] there are a number of examples and cases where data concerning health can be perceived as such. For instance personal information entailed in this category, relating to the mental and physical health status of a person throughout their lifetime, constitute the following:

- Collected information upon registering for receiving treatment or general health care services at an institution acting as a provider of such services (i.e. a hospital).[16]
- Any identification number or symbolism or particular that is assigned to a natural person/ individual that can be used to identify them in a unique way in the context of health care.
- Information that is extracted after performing tests and examinations upon a part of the human body or its substances, adding to it also genetic and biometric data.
- Information of any kind relating to an illness, a disorder/ disability, disease risk, medical history, clinical treatment or the anatomical and biomedical status of an individual-subject of the personal data, regardless of the source from which they derive from, for instance, the health care system, a physician or a health/ medicine service provider and expert, even an in vitro diagnostic test.

2. GENETIC DATA

According to Article 4 (13) of the GDPR the definition given to the term " Genetic data" is that of personal information regarding hereditary and acquired attributes of a natural person providing knowledge of a unique kind on one's physiology and health status, the product of an examination and analysis of a biological substance or particle of the data subjects body[17].

The genetic information of the aforementioned nature can lead to the precise identification and differentiation of one individual from another. The DNA analysis is of the highest importance, as it could lead to the revelation of predisposition to diseases, from the data subject's part, alongside the existence of inherited characteristics[18]. Thus, processing personal data of this nature should be met with the highest precautions, while performed with respect to the need for confidentiality and security[19].

---

[15] Recital 35 of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation- GDPR).

[16] Directive 2011/24/EU of the European Parliament and of the Council of 9 March 2011 on the application of patients' rights in cross-border healthcare (OJ L 88, 4.4.2011, p. 45).

[17] Recital 34 of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation- GDPR).

[18] Chara D. Zerva (Nicolas Kanellopoulos-Chara Zerva and Associates Law Firm Health),(2019), Biometric and Genetic Data Under GDPR, Greek Law Digest the official guide to Greek Law, http://www.greeklawdigest.gr/topics/data-protection/item/304-health-biometric-and-genetic-data-under-gdpr [Accessed Online on 20/10/2019].

[19] Recital 39 of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation- GDPR).

3. BIOMETRIC DATA

Article 4 (14) of the GDPR states that "Biometric data" are: "personal data resulting from specific technical processing relating to the physical, physiological or behavioral characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopy data". The Regulation broadens the scope of biometric data's definition with this provision in order to render it applicable to both existent and possible techniques of processing biometric information in the foreseeable future.[20]

Biometric information when processed can result in the identification and/or the authentication/verification of the data subject, through the use of biometric technological applications, such as biometric systems. This kind of systematic processing is based upon traits of three particular kinds:[21]

1. *Universal traits,* all individuals possess such biometric characteristics
2. *Unique traits* can be in relation to one particular individual only.
3. *Permanent traits,* biometric elements that remain stable and unchanged in one individual through time.

Biometric techniques can be further devised into – now three[22]- categories in relation to the kind of characteristics they are based on:

1. Physiological characteristics such as fingerprint analysis and identification/ verification, iris & face recognition, retina analysis, voice recognition, DNA analysis, etc.
2. Behavioral-based analysis, opting in the measuring and collection of signs of the behavior of a certain individual such as signature in handwriting pattern, gait analysis, particular walking movement, subconscious mentality in patterns, like lying, etc.
3. Psychological attributes that an evolving biometric technique is relying upon in order to measure a person's particular reactions to certain events and tests so as to draw psychological profiles from.

3.1 Processing sensitive data

Pursuant to Article 5 (1) and Article 9 of the GDPR, health, genetic and biometric data constitute a set of sensitive data, as per the prior legislative framework, but also a special category of personal data, demanding a higher level of transparency, fairness,

[20] Chara D. Zerva (Nicolas Kanellopoulos-Chara Zerva and Associates Law Firm Health),(2019), Biometric and Genetic Data Under GDPR, Greek Law Digest the official guide to Greek Law, http://www.greeklawdigest.gr/topics/data-protection/item/304-health-biometric-and-genetic-data-under-gdpr [Accessed Online on 20/10/2019].

[21] ARTICLE 29 - Data Protection Working Party, Working document on biometrics
, Adopted on 1 August 2003, 12168/02/EN
WP 80.

[22] ARTICLE 29 DATA PROTECTION WORKING PARTY, Opinion 3/2012 on developments in biometric technologies, 00720/12/EN
WP193.

and protection, as far as it comes to their processing.[23] One of the basic principles laid out on Article 5 (1b) relates to the purpose limitation principle[24], meaning that data shall be collected and processed pursuant to the original objective for which they were stored and the procedure of their analysis will not deviate from the purpose that it was initiated for. Broader flexibility and freedom have been appointed to the achievement of purposes regarding the public interest, science, history or research in general, but in accordance to Article 89, introducing allowance to processing only when safeguarding of the rights and freedoms of the data subjects is secured and offered (Article 9 §.2).

Processing, according to Article 4 (2) of the GDPR: "processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction";

Sensitive data/ Special category of data: information that can reveal the racial or ethnic origin of a person, political, religious or philosophical mindset or beliefs, trade union membership and the newly added, in Article 9 (1) of the GDPR, the genetic and biometric data that can lead to the identification of a person, data concerning their health, gender, sex life or sexual orientation. All the above-mentioned categories of data cannot be processed unless specific legal conditions are met set by the same article.[25]

Namely they include, but are not limited to: a) explicit consent by the data subject, unless the Member state's or the Union's relating existent provisions do not allow for the lifting of the aforementioned prohibition, even by the subject's consensual agreement, b) it is vital for the fulfillment of obligations or exercising of rights both of the controller and of the data subject in the employment and social security sector and social protection law, under the authorization of Union or Member State law or relative agreement provided again that the necessary safeguards for the fundamental rights and interests of the data subject are being offered, c) for the protection of the data subject's interests or of another person's when the subject is physically unable or legally incapable of giving their consent, d) they have been manifestly made public by the data subject, e) there needs to be a processing of sensitive data for the purposes of preventive and occupational medicine, for assessing the working potency of an employee, for purposes of medical diagnosis, the providing of health or social care or treatment, the managing of health or social care systems or services based on Union or Member State law, in accordance with a contract with a health professional but also subjected to the following conditions.[26]

In Paragraph 3 of Article 9 of the GDPR, the regulation stresses that the lifting of the processing prohibition can only be valid while the said processing is performed

---

[23] Recital 51 of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation- GDPR).

[24] Article 5 (1b) of the GDPR: collected for specified, explicit and legitimate purposes… not be considered to be incompatible with the initial purposes ('purpose limitation');

[25] Article 9 par. 2 of the GDPR.

[26] Recital 53 of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation- GDPR).

by a health care professional subject to the obligation of professional secrecy, pursuant to Union or Member State law or provisions set into force by competent bodies or another individual also subject to the above mentioned legal framework.

Last but not least, a novelty introduced by the GDPR, with the aim to further facilitate and not impede research, is the concept of broad consent. Even though not explicitly stated with in the Regulation, broad consent as an option when processing personal data for research purposes is apparent from the combination of Article 7[27] and Recital 33[28] of the GDPR. According to these, the regulation acknowledges the fact that the exact purposes of a research might not be possible to be fully explained from its beginning, thus they provide with the solution for the data subject to provide consent to the general area of the research. More specifically, the data subject can give its consent to certain parts of the research, only to certain parts of the research or to parts of a particular research project.[29] However, even in this case in order to provide with the necessary protection, the researcher should acquire this form of consent after sufficiently informing the data subject about the research and after they have also acquired a clear and unambiguous indication of the data subject's desire to have their data processed during the research project. An issue, although could occur, in relation to a certain contradiction between the recital and the actual articles (7 and 9). The Regulation, actually, stresses the need for "recognized ethical standards for scientific research" to be upheld, in order for broad consent to be lawful, when on the same time the derogations for research purposes permitted by the legal text might not be compatible with these ethical standards.[30]

3.2 Derogations

In accordance with Article 9 (4)[31] of the General Data Protection Regulation Member States can introduce deviations, entertaining stricter measures, from the above conditions for processing special category personal data, including health, genetic and biometric data. However, on Recital 53 -relating to the processing of Sensitive data on Health and Social sector, it is highlighted that such limitations should not impede the liberal exchange and flow of data within the Union and amongst the

---

[27] Article 7 of the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation- GDPR).

[28] Recital 33 of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation- GDPR), "It is often not possible to fully identify the purpose of personal data processing for scientific research purposes at the time of data collection. 2Therefore, data subjects should be allowed to give their consent to certain areas of scientific research when in keeping with recognised ethical standards for scientific research. 3Data subjects should have the opportunity to give their consent only to certain areas of research or parts of research projects to the extent allowed by the intended purpose."

[29] Health Research Board, GDPR Guidance for Researchers, Broad Consent, https://www.hrb.ie/funding/gdpr-guidance-for-researchers/gdpr-and-health-research/consent/broad-consent/ (online) accessed 06 Dec 19.

[30] Staunton, C., Slokenberga, S. & Mascalzoni, D. (2019), The GDPR and the research exemption: considerations on the necessary safeguards for research biobanks. Eur J Hum Genet 27, 1159–1167 doi:10.1038/s41431-019-0386-5

[31] Article 9 (4), GDPR: "Member States may maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or data concerning health."

Member States when they could be applicable to cross-border processing of such kind of data. In this context, Member States could deviate from the initial restrictions on processing sensitive data, while at the same time they need to be providing with the relative safeguards and protections of the fundamental right and interests of the data subjects.

Making use of this provision, the German Data Protection Law[32] allows for the processing of sensitive personal data in certain cases, without the consent of the data subject, when such processing is vital for the procurement of preventive medicine, when it is crucial for the determination of the working capacity of an employee, along with the securing of the superiority of the quality of the health care industry and medicinal products and services. Moreover, the UK Data Protection Act 2018[33] introduces clauses with limitations on the implementation of the GDPR's provisions – pursuant to Article 23 (1) of the GDPR and the ability to restrict rights and obligations that it includes- that is in relation to health care, such as the processing of data by health care professionals in order to provide medical services.

4. Prior Legislation

The previous legal framework for the protection of personal data and of special categories of data, within the Union, constitute the Directive 95/46/ EC[34] (hereinafter the Directive) of the European Parliament and of the Council, an effort to ensure lawful protection of an individual's privacy in relation to new technologies. Although, as innovation in the technological sector begun to escalate beyond the existent scope of the Directive, the European Commission on 2009 launched the endeavour of the reformation of the Directive, trying to update the existent provisions, rendering them more contemporary and appropriate to the emerging needs of the modern reality, but also providing with a higher level of harmonization, through the establishment of a Regulation – the GDPR – instead of a Directive that had to be further implemented by 27 Member States, a legal document of direct force to every Member State.[35]

The Directive presented with several differences upon comparison with the Regulation. Even if there was a reference to personal data and their definition along with a definition for sensitive personal data as a separate category of the data subject's information, there was no direct reference in the Articles of biometric and genetic data, even though health data were included in the scope of the Directive and demanded for special conditions for processing, pursuant to Article 8[36]. However, in the GDPR there is an explicit reference of the term "genetic", for providing with a

[32] Art. 22 of the German Federal Data Protection Act (BDSG).

[33] Schedule 3 of the UK Data Protection Act (2018).

[34] 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, Official Journal L 281 , 23/11/1995 P. 0031 – 0050.

[35] Mahsa Shabani & Pascal Borry, (2017), Rules for processing genetic data for research purposes in view of the new EU General Data Protection Regulation, European Journal of Human Geneticsvolume 26, pages149–156 (2018), https://www.nature.com/articles/s41431-017-0045-7 [Accessed Online on 20/05/2019].

[36] Article 8 of Directive 95/47/ EC : The processing of special categories of data " Member States shall prohibit the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life."

definition of personal data- is Article 4(1), but also in Article 9[37] it explicitly includes in the category of sensitive personal information biometric and genetic data (while on the same time providing with definitions of such kind of data, as seen above).

All things aside, the new Regulation follows the general principles laid by its predecessor, the Directive, adding though some novel provisions and revisions, but not in all subjects. Regarding the issue of the distinction between the anonymous and the anonymized data[38], the Regulation, as the Directive before it, fails to provide a clarification relating to these deferent kinds of data, while it explains the scope of personal data on Recital 26[39]. Anonymization, according to Article 29 Working party could be considered further processing of the already collected in an identifiable way set of data[40]. On the contrary, the Regulation included in its provisions a definition for pseudonymization, a provision lacking from the Directives framework. Pursuant to Article 4(5) pseudonymized data are those data that cannot be credited to a data subject without the use of supplementary information, kept within the relevant safeguards for ensuring the inability to be related to an identifying of an identifiable natural person. According to Recital 26 of the Regulation, this kind of data can be regarded as personal data if by "all means reasonably likely to be used" they can be lead to the identification of the data subject, the original source of the pseudonymized data. In the same context and pursuant to the proportionality principle, depending on the likelihood of such an event to occur the conditions and limitations of the Regulation shall apply with an accordingly equal and proportionate flexibility to this kind of data.[41]

5. National Legislations

The GDPR, despite its legal scope and nature as a regulation (of immediate application to the Member States' legal system), entails several clauses that allow to the national legislator to deviate from the legislation's scope, including the chapter

[37] Article 9 of the GDPR: Processing of special categories of personal data "Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the 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 shall be prohibited."

[38] Beyleveld D, Townend D. When is personal data rendered anonymous? Interpreting recital 26 of Directive 95/46/EC. Med Law Int. 2004;6:73–86.

[39] Recital 26 of Directive 95/46/ EC: "Whereas the principles of protection must apply to any information concerning an identified or identifiable person; whereas, to determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify
the said person; whereas the principles of protection shall not apply to data rendered
anonymous in such a way that the data subject is no longer identifiable; whereas codes of conduct within the meaning of Article 27 may be a useful instrument for providing guidance as to the ways in which data may be rendered anonymous and retained in a form in which identification of the data subject is no longer possible;".

[40] Article 29 WP: "Anonymization constitutes a further processing of personal data; as such, it must satisfy the requirement of compatibility by having regard to the legal grounds and circumstances of the further processing".

[41] Article 29 Working Party. Opinion 4/2007 on the concept of PersonalData, 2007.

relating to processing sensitive data, such the aforementioned ones.[42] The Greek Law in implementation of the Regulation is Law 4624/2019.

Pursuant to the above right of legislating according to national standards and particular circumstances Article 30 introduces exceptions to the general prohibition of Article 9 of the GDPR regarding the possibility of processing for statistical or public interest or for scientific and historical research purposes. However, the exceptions are only permitted if they are in accordance with Article 89, which states, along with Article 9§2, that specific measures need to be taken in order to safeguard the rights of the data subject in interest. The Greek Law makes no such remarks, apart from those already existing within the framework and text of the Regulation (e.g. pseudonymization[43]).

Contrary to the recent legal provision, the previous legislation[44], which incorporated the Directive 95/46/EC in the national legal system, followed its example regarding the general prohibition of processing sensitive data (Art.8 95/46/EC). At the same time, though, it allowed processing by associating its legality not only with the existence of specific and substantial reasons for it but also by the acquiring of a permit from the National Data Protection Authority (Art. 7 Law 2472/1997).

In additional contradiction to the vagueness of the newly established legal scope in Greece, the German legislation with the Federal Data Protection Act[45], provides with a detailed list of measures to be applied so as to ensure the protection of fundamental rights of the data subject, such as but not limited to: a) "measures to ensure that it is subsequently possible to verify and establish whether and by whom personal data were input, altered or removed b) measures to increase awareness of staff involved in processing operations and c) measures to ensure the ability, confidentiality, integrity, availability and resilience of processing systems and services related to the processing of personal data, including the ability to rapidly restore availability and access in the event of a physical or technical incident" (Federal Data Protection Act of 30 June 2017 (Federal Law Gazette I p. 2097). Last but not least, in the same more specific nature, the Austrian law, implementing GDPR principles, provides a detailed course of action in order to enact the clause that lifts the exception in processing, which is correlated with the procurement of a permit from the Data Protection Authority. In fact, in the legal text, it is even explained thoroughly the process and the criteria on which the decision of the Authority will be based upon.[46]

Moreover, in the United Kingdom the Data Protection Act,2018 (henceforth DPA), also makes use of the potential exemption from the prohibition of processing sensitive personal data, on several grounds and upon meeting the lawful conditions. Amongst them there is also the condition reserved for archive, historic and research purposes, which does not appear to be introduced with any changes, in the national legislation (or with any specified provisions, apart from pseudonymization)[47]. A novelty constitutes, the provision relating to processing for employment, social security and

---

[42] L.Mitrou, The General Data Protection Regulation, Athens 2017, pp.25 etc.

[43] Art. 89 §1 , GDPR

[44] Law 2472/1997.

[45] Federal Data Protection Act of 30 June 2017 (Federal Law Gazette I p. 2097, (BDSG) , Sub-chapter 1, Section 22§2 and Sub-chapter 2, Section 27.

[46] Federal Act concerning the Protection of Personal Data (DSG), Part 2 §2 & §3.

[47] Schedule 1, Part 1, paragraph 4 DPA.

social protection purposes, which is allowed provided that there is an appropriate data policy document drafted, stating the data controller's procedure for ensuring the compliance with principles in Article 5 of the GDPR.[48] Another novelty introduced is the change in the age limit of consent in the case of minors. According to the GDPR, the age limit is 16 years but pursuant to the DPA is now 13 years.[49]

6. US Legislation

The US has to display not a concrete base of one federal law ruling over the issue of data privacy, in relation to health, biometric and genetic data, but a combination of both federal laws and state laws, which protect Americans to different extents.

First and foremost, chronologically and in a federal scope, there is the Health Insurance Portability and Accountability Act (HIPAA)[50], which provides a specified set of described entities and collections of data that are regulated in its framework (Protected Health Information (PHI). Notwithstanding the efficacy and adequacy of the level of HIPPA's protection there is an issue with the extent of that same protection as only "covered entities" and " associated business" fall under its scope. Thus, the majority of well-known data minors, such as Google and Amazon which deal with huge amounts of data and some of them health-related, are usually excluded from this legal framework.[51] In addition, HIPPA protects information that can lead to the identification of a person (part 160 & 164), leaving any information rendered unidentifiable outside the law's protective provisions. Such kinds of de-identified data can occur in two ways according to HIPPA: a) by striking out designated in the law identifying information and b) by acquiring estimation from an expert in statistics confirming the significantly low risk of re-identification. However, both ways have been found to be rather inadequate[52] in practice, particularly in the case of genetic data and information, usually de-identified, but only to a minimum extent, so as avoid applicability of HIPPA, when actually information that could lead to the re-identification of the data subject are frequently kept and up for exchange by the so-called data minors (e.g. doctor's names, case number's, dates)[53]

Moreover, another federal legislation aiming at enriching the level of protection, this time relating to genetic information, is The Genetic Information Non-discrimination Act, Public Law 110-223 (GINA). GINA constitutes a means for prohibiting discrimination in the Insurance (I)[54]and the Employment (II)[55] sector.

---

[48] Schedule 1, Part 1, paragraph 1 DPA, Schedule 1, Part 4, paragraph 39 DPA.

[49] Part 2, Chapter 2, Section 9 DPA.

[50] The Health Insurance Portability and Accountability Act of 1996 (HIPAA). P.L. No. 104-191, 110 Stat. 1938 (1996).

[51] A. Tanner, Strengthening Protection of Patient Medical Data The Century Foundation (2017), https://tcf.org/content/report/strengthening-protection-patient-medical-data , accessed 26/11/19)

[52] K. Benitez and B. Malin, Evaluating Re-identification Risks With Respect to the HIPAA Privacy Rule, 17 J. am. med. inform. assoc. 169, 177 (2010).

[53] J. Kulynych and Henry T. Greely, Clinical Genomics, Big Data, and Electronic Medical Records: Reconciling Patient Rights With Research When Privacy and Science Collide, 4 J. law. biosci. 94, 132, 122 (2017).

[54] TITLE I—GENETIC NONDISCRIMINATION IN HEALTH INSURANCE, GINA 2008.

[55] TITLE II—PROHIBITING EMPLOYMENT DISCRIMINATION ON THE BASIS OF GENETIC INFORMATION, GINA 2008.

Americans are protected from having their genetic information used by the above parties to hamper their access to beneficial insurance contracts (e.g. regardless of their genetic condition) and to fair employment offers. This framework includes family medical history, not undergoing genetic testing upon request, the results and information relating to similar tests already taken, all applicable to both the private and the public sector.[56] More specifically, GINA incorporates provisions that affect the participants of clinical research with an emphasis on informed consent and how and what grounds it should be acquired upon.[57] What GINA does not regulate are companies that fall under its exception by having less than 15 employees, long-term care insurance, life insurance or disability insurance. Furthermore, GINA provides a definition of genetic testing, as the analysis of DNA, RNA chromosomes, proteins or metabolites aiming at the detection of genotypes, mutations, or chromosomal changes. Any other kind of testing (e.g. enzyme tests) is not considered as genetic tests under the protection scope of GINA. Genetic tests of proteins and metabolites that are associated with the manifestation of diseases and disorders are not considered genetic testing under GINA as well.[58]

On a state level several efforts have been set in place from states such as the State of California (California Consumer Privacy Act, CCPA), the state of Illinois (2008 Illinois Biometric Information Privacy Act (BIPA) and the ruling of January 2019 on the Rosenbach v. Six Flags case) and the San Francisco's Board of Supervisors anti-surveillance ordinance (May 2019).

California Consumer Privacy Act (CCPA)[59] passed on the 25th of January 2019 and will be effective from January 2020. It provides the protection of rights to privacy of the citizens of California, focusing on consumer protection, but in relation to the collection of biometric data. Its definition of the latter set of data appears broader than the one given in the GDPR: "an individual's physiological, biological or behavioral characteristics, including an individual's DNA that can be used, singly or in combination with each other or with other identifying data, to establish individual identity."[60]

According to the ruling of the Supreme Court of Illinois in the case of Rosenbach v. Six Flags case[61], the Illinois Biometric Information Privacy Act (BIPA)[62] provides with the right to take action brought before the court without the need of claiming additional harm, just the absence of an opt-in consent for the collection of biometric data, such as fingerprint and face recognition data.

---

[56] 'Genetic Information Non-discrimination Act, PUBLIC LAW 110–233—MAY 21, 2008,

[57] A description of any reasonably foreseeable risks or discomforts to the subjects (45 CFR 46.116(a)(2)); and A statement describing the extent, if any, to which confidentiality of records identifying the subject will be maintained (45 CFR 46.116(a)(5), GINA, 2008.

[58] Human Research Protection, Genetic Information Nondiscrimination Act Guidance (2009), March 24, 2009.

[59] Assembly Bill No. 375, California Consumer Privacy Act, Date Published:06/29/2018.

[60] LAURA JEHL AND ALAN FRIEL, BAKERHOSTETLER LLP, A Chart comparing some of the key requirements of the California Consumer Privacy Act (CCPA) and the EU General Data Protection Regulation (GDPR), https://www.bakerlaw.com/webfiles/Privacy/2018/Articles/CCPA-GDPR-Chart.pdf , (Online), accessed on: 26 Nov. 19.

[61] Rosenbach v. Six Flags Entertainment Corp., 2019 IL 123186, Supreme Court, 25th of January.

[62] 740 ILCS 14/ Biometric Information Privacy Act.

San Francisco's Board of Supervisors'[63] anti-surveillance ordinance (May 2019) ruled against the use of facial recognition technology from major representatives of the public sector and law enforcement (e.g. police, governmental bodies).

CHAPTER B- NEW TECHNOLOGIES

New technologies have brought groundbreaking changes in the lives of billions worldwide since the beginning of the century. Now more than ever, computational and informational technology alongside cutting-edge research on the field of data analysis the potential to bring upon revolutionary possibilities in the health care sector.

From direct to consumer genetic testing, overcoming the legal impediments and procuring the public with a ready to use time capsule and by its evolution as service a lot more than that, to the mobile health applications (hence fort apps), with their portable nature providing access to biometric data, health status analysis and indispensable aid to those in need (e.g. mental health care apps).

Last but not least, Artificial Intelligence (henceforth AI) technology and innovation has offered the opportunity to collect, combine and analyze a very large amount of data (big data analysis), while at the same time resulting in comprehensive conclusions able to promote the advancement of medical studies even further, to disease prevention, precision medicine, epidemiological analysis and the accelerating of medical procedures in general.

However, the progress made on a scientific level demonstrates not only the potential of mankind but also its obligation to synchronize the current legislation and ethical conversation with the demands of the modern era. Technology constitutes a tool that, like any other, can be misused without proper guidance.

1. DIRECT TO CONSUMER GENETIC TESTING/ GENETIC DATA

1.1 The US.

The technological revolution of genome sequencing has brought incredibly rapid changes in the ability to sequence a large amount of genetic data in a faster, cost-effective and accurate way. Next-generation sequencing with its potential to map the entire genome of a person with unprecedented quality and velocity opened up new possibilities to the scientific community, the pharmaceutical industry, the public sector, and various biotechnological companies, now enabled to draw information from the largest pool of big data ever available to researchers.

Direct- to- consumer genetic testing (DTC) is the product of such advancement, made possible by the increasing affordability of genome sequencing, accompanied

[63] Stop Secret Surveillance Ordinance (05/06/2019), Board of Supervisors.

though with its respective legal challenges, as health information is being more and more directed outside the public care sector and into the private commercial initiative. The U.s Food and Drug Administration has had a leading role in the regulatory effort related to this emerging genetic testing device, moving from the more traditional "Protective" Medical Device approach to adopting, after taking under consideration the Consumer-Based "Libertarian" Critique, a more hybrid and flexible position. This final aspect was highlighted by its licensing to the well-known company 23andMe to provide medical information relating to the potential of its clients to have disease risk factors in their DNA (Genetic Health Risk Test).[64]

The more traditional "Protective" Medical Device prototype derived from the FDA's jurisdiction to regulate any medical device under the scope of the Federal Food, Drug and Cosmetic Act (FDCA), with a general description as: "an instrument, apparatus, implement, machine, contrivance, implant, in vitro reagent, or other similar or related article ...which is ... intended for use in the diagnosis of a disease or other conditions or in the cure, mitigation, treatment, or prevention of disease."[65] In addition, medical devices are classified into 3 separated categories related to their high, moderate or low-risk factors, according to the 1976 Medical Device Amendments (MDA) to the FDCA.[66] In the context of this framework there is a description provided of in vitro diagnostics (IVDs), in contradiction to Laboratory Developed Tests (LDTs), IVDs constitute: "Those reagents, instruments, and systems intended for use in the diagnosis of disease or other conditions, including a determination of the state of health, in order to cure, mitigate, treat, or prevent disease or its sequelae. Such products are intended for use in the collection, preparation, and examination of specimens taken from the human body."[67] Those kinds of tests are available for distribution to hospitals, clinics and directly to patients, while on the contrary LDTs are meant for research purposes only. As a result, the FDA has made clear that the Direct-to-Consumer testing does not fall under the scope of the latter, but instead its manufacturers have to inform the FDA prior to market release, and do not partake in the regulatory exception of the LTD.[68]

A more liberal approach to the matter has been brought forward by stakeholders and the scientific community, relating to the lack of flexibility and acceptance from the FDA's and the traditional medical care professionals' part. Unwilling to embrace the innovative steps to bring health information in the hands of the patients, based upon them losing their traditional role as key facilitators of the process, they appear to be impeding the progress of informational technology, hampering the rights of the consumers. Consequently, FDA revised its course of action

---

[64] Sharkey, C. M. (2019). Direct-to-consumer genetic testing: The fda's dual role as safety and health information regulator. DePaul Law Review, 68(2), 343-384. https://heinonline.org/HOL/Page?collection=journals&handle=hein.journals/deplr68&id=372&men_tab=srchresults# (online) accessed: 20 Nov.2019).

[65] 21 U.S.C. § 321(h), (h)(2) (2012).

[66] 21 U.S.C. § 360c(a)(1)(C)(ii)(I)-(II) (2012).

[67] 21 C.F.R. § 809.3 (2018), Overview of IVD Regulation, U.S. FOOD & DRUG ADNMwN., https://www.fda.gov/MedicalDevices[DeviceRegulationandGuidance/IVDRegulatoryAssistance (online) accessed : 20 Nov.19.

[68] Nancy K. Stade et al., FDA Challenges Direct-to-Consumer Genetic Tests, LAw360 (Mar. 22, 2016, 11:47 AM), https://www.1aw360.com/articles/772679/fda-challenges-direct-to-consumer-genetic-tests. (Online) accessed: 20 Nov. 19.

by introducing 2012 Food and Drug Safety and Innovation Act and its fast-forward "de-novo" process of filling for the approval of the Administration[69], in combination with the authorization of Genetic Health Risk (GHR) tests in the market since 2017 (23andMe included)[70].

1.2 EU.

At the moment there is not one specific regulatory framework within the EU that applies to the DTC genetic testing, but the provisions of several other legal instruments and documents can be used to provide a level of protection and guidance to this innovative tool.

Firstly, there is the Unfair Commercial Practices Directive 2005/29 EC[71] regarding the protection of consumers from misleading actions and omissions but also from the use of technics from the traders' part that results in psychological pressure or deception in the advertisement[72]. Moreover, this kind of genetic testing is considered an IVD medical device, as seen above from the US regulation, meaning that it is subject to stricter conditions than other products. That is precisely depicted within the scope of Directive 93/42/EEC[73] concerning medical devices and Directive 98/79 EC on In Vitro Diagnostic Medical Devices[74], which provides with the provisions related to the level of safety and efficiency requirements those devices need to meet before they can be approved for the European Market.

Apart from the regulated aspect of DTCs as products, there is also a side of them that can not fit into the above framework and can be more accurately appointed to the healthcare service context (e.g. genetic counseling, rules of informed consent). As the healthcare services in relation to genetic testing has not been regulated as a

---

[69] U.S. FOOD & DRUG ADMIN., FDA-2011-D-0577, GUIDANCE FOR INDUSTRY AND FOOD AND DRUG ADMINISTRATION STAFF: FACTORS TO CONSIDER WHEN MAKING BENEFIT-RISK DETERMINATIONS IN MEDICAL DEVICE PREMARKET APPROVAL AND DE Novo CLASSIFICATIONS 4 (2016) https://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM517504.pdf (online), accessed: 20 Nov.2019.

[70] Press Release, U.S. Food & Drug Admin., Statement from FDA Commissioner Scott Gottlieb, M.D., on Implementation of Agency's Streamlined Development and Review Pathway for Consumer Tests That Evaluate Genetic Health Risk (Nov. 6, 2017), https://www.fda.gov/NewsEvents/Newsroom/PressAnnouncements/ucm583885.htm.(online), accessed: 20 Nov.2019.

[71] European Parliament and the Council of the EU (2005) Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 Concerning unfair business-to-consumer commercial practices in the internal market and amending council directive 84/450/EEC, directives 97/7/EC, 98/27/EC and 2002/65/EC of (2005).

[72] European Commission (2016) The Black List: banned commercial practices - European Commission – DGhttp://ec.europa.eu/justice/consumer-marketing/unfair-trade/unfair-practices/is-it-fair/blacklist/index_en.htm (online), accessed: 22 Nov.2019.

[73] COUNCIL DIRECTIVE 93/42/EEC of 14 June 1993 concerning medical devices (OJ L 169, 12.7.1993, p. 1)

[74] European Parliament and Council (1998) Directive 98/79/EC of the European Parliament and of the Council of 27 October 1998 on in vitro diagnostic medical devices.http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31998L0079:EN:HTML (online), accessed: 22 Nov.19.

whole by the EU and usually it is left for the Member States to decide, this legal practice leaves enough space for the national legislators to step in and establish their own regulation on a national level, which varies from one jurisdiction to another.[75]

However, coalition and accordance with international legal documents should be established, such as the Convention on Human Rights and Biomedicine (Oviedo Convention)[76] of the Council of Europe and its Additional Protocol on Genetic Testing for Health Purposes[77]. The Convention together with the Additional Protocol, ratified and now into force, touch upon topics such as human dignity and fundamental principles for medical practice (e.g. informed consent) but also specific aspects of the context of genetic testing, like medical supervision and genetic counseling. [78]

2. MOBILE HEALTH APPLICATIONS/ BIOMETRIC DATA

According to the World Health Organisation Mobile Health (henceforth "m-health") constitutes: "medical and public health practice supported by mobile devices, such as mobile phones, patient monitoring devices, personal digital assistants (PDAs), and other wireless devices"[79] Adding to this new term, there are also lifestyle and well-being applications, that provide with a variety of information, relating to the connection of sensors and the produced biometric data. Their existence is based on an alternate offer of guidance and the increase of involvement of the public in their own quality of life but also the raising of awareness and promotion of preventive approaches relating to the health status of individuals.[80]

Alongside the numerous potentials of the procurement of such an empowering choice and tool to the public, there are several issues and challenges that need to be tackled, one of the primary ones being the issue of privacy. A major concern of consumers relate to the sharing of the data from m-health applications to third parties (e.g employers, insurance companies), which is proven by the results of a study indicating

---

[75] Godard B, Kääriäinen H, Kristoffersson U, Tranebjaerg L, Coviello D, Aymé S (2003) Provision of genetic services in Europe: current practices and issues. Eur J Hum Genet 11(S2):S13–S48. https://doi.org/10.1038/sj.ejhg.5201111 (online), accessed: 22 Nov.19

[76] Council of Europe (1997) Convention for the Protection of Human Rights and Dignity of the Human Being with regard to the Application of Biology and Medicine: Convention on Human Rights and Biomedicine. Council of Europe, Oviedo, 4.I.V.1997.

[77] Council of Europe (2008). Additional Protocol to the Convention on Human Rights and Biomedicine, concerning Genetic Testing for Health Purposes., 01/07/2018- 5 Ratifications including 4 member States. https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/203 (online), accessed: 22 Nov.2019.

[78] Kalokairinou, L., Howard, H.C., Slokenberga, S. et al. J Community Genet (2018) 9: 117. https://doi.org/10.1007/s12687-017-0344-2 (online), accessed: 22 Nov.19.

[79] World Health Organisation "mHealth – New horizons for health through mobile technologies, Global Observatory for eHealth series – Volume 3", page 6

[80] EU Commission's GREEN PAPER on mobile Health ("mHealth"),COM(2014)219 10.4.2014, final.

that 45% of consumers share such a concern about the unwanted use of their data, in the context of using m-health applications.[81]

The increased concern is logically met with relevant protective measures from the EU's side. In fact, in Article 8 of the Charter of Fundamental Rights of the European Union, as well as in Article 16(1) of the Treaty on the Functioning of the European Union (TFEU), there is an establishment of the right to the protection of personal data. Pursuant to the fundamental nature of the above-mentioned provision the EU demands compliance with the applicable provisions deriving from the GDPR (especially principles applying to processing sensitive data and the opt-in & opt-out rights). Furthermore, issues might occur depending on which scope each m-health application best fits in to. More specifically, judging from the nature of each application, ad hoc, manufacturers might find their products falling either within the scope of the Medical Devices Directive (Directive 93/42/EEC) or In vitro diagnostic medical devices Directive (Directive 98/79 EC). To that extent the Green Paper on m-health from the European Commission is accompanied by the Staff Working Document on the existing EU legal framework applicable to lifestyle and wellbeing apps, aiming to offer guidance upon the legal framework related to the m-health apps.[82]

In association with data privacy and security there comes also the need for safety and efficiency relating to the content of each m-health app, meaning its function and trustworthiness. To that end, several standards of safety must be met, which can be proven through the acquiring of certifications. Such kind of programs and initiatives are, amongst others, the National Health Service[83], an online Health Apps library in the United Kingdom, the Happtique in the US[84], a specialized platform for selling certified health apps and the European Directory of Health Apps[85], striving for the transparency and reliability of the recommended health apps.

2.1 Regulated & Unregulated Cases

On the other hand, there is the issue of m-health applications from a more medical and sensitive point of view as it appears that an increasing number of consumers opt for such technological services in order to deal with mental health problems. Indeed, more than 10,000 available apps today regard mental health[86] when the number of downloads of this kind of applications has doubled in 2016, according to statistic

---

[81] Blue Chip Patient Recruitment. Leveraging Mobile Health Technology for Patient Recruitment, October 2012

[82] COMMISSION STAFF WORKING DOCUMENT on the existing EU legal framework applicable to lifestyle and wellbeing apps, accompanying the document GREEN PAPER on mobile Health ("mHealth"), SWD(2014), 10.04.2014.

[83] The New England Center for Investigative Reporting, Boston University, "Lacking regulation, many medical apps questionable at best", 18.11.2012

[84] https://www.happtique.com/ (online), accessed: 24 Nov.2019

[85] https://ec.europa.eu/digital-single-market/en/news/first-european-directory-health-apps-recommended-patients-and-consumers (online),accessed: 24 Nov.19.

[86] J. Torous, L.W. Roberts,(2017), Needed innovation in digital health and smartphone applications for mental health transparency and trust JAMA Psychiatry, 74 (5) (2017), pp. 437-438, 10.1001/jamapsychiatry.2017.0262

reports[87]. The majority of those apps use informative and educating to the user content in order to allow a comprehensive and interactive experience and observation of one's progress dealing with several mental struggles, the most common being depression (e.g. at the 18% of mental health app targets depression while being on the top 3 of the mental health apps with the most market potential for 2017).[88]

The popularity and quick emergence of the extensive use of mobile health applications and platforms for mitigating mental health issues lead the FDA in the US to issue a policy relating to three distinctive categories of mental health apps: a) those that do not constitute a medical device, b) those that are medical devices according to the FDA but it upholds the right to exercise enforcement discretion (that are not regulated), c) those that do constitute medical devises and fall under FDA's regulatory jurisdiction.[89] As a result, the majority of such applications in the US are not regulated which means that they are under no serious inspection and control. In an effort to provide with some guidance the Federal Trade Commission came up with a list of suitable practices that should be taken under consideration from the manufacturers of mental health apps, amongst them being the collection of the minimum amount of data from the user and limiting the access and permission to the user's mobile device.[90]

Consequently, upon the absence of federal regulation or an inclusive legal framework, such kinds of applications often lack in privacy policies, which appear to be insufficient or completely non-existent. Such is the outcome of a study conducted in regard to the mental health apps provided to patients suffering from dementia. The results pointed out that the apps using a privacy policy were below 50% and even if they did it was also lacking in information about the handling of the user's data.[91] However, this research was based only upon a certain kind of application, specified for dementia as a condition, while at the same time extensive research on the field with a central focus on depression, due to its widespread nature, was performed to provide with answers to major issues, like privacy and security. The results of the review of a quarter of the available mental health apps for depression were alarmingly displaying the fact that only 4% of those apps had a complete with sufficient information privacy

---

[87] mHealth app development economics 2016: the current status and trends of the mHealth app market, http://research2guidance.com/r2g/r2g-mHealth-App-Developer-Economics-2016.pdf (online), accessed: 24 Nov. 19.

[88] Top 3 therapy fields with the best market potential for digital health apps (2017)https://research2guidance.com/top-3-therapy-fields-with-the-best-market-potential-for-digital-health-apps (online), accessed: 24 Nov.19. & IMS Institute for Healthcare Informatics Patient Adoption of mHealth: Use, Evidence and Remaining Barriers to Mainstream Acceptance,(2015),https://www.iqvia.com/-/media/iqvia/pdfs/institute-reports/patient-adoptionofmhealth.pdf?la=en&hash=B3ACFA8ADDB143F29EAC0C33D533BC5D7AABD689 (online), accessed: 24. Nov.19.

[89] Policy for Device Software Functions and Mobile Medical Applications Guidance for Industry and Food and Drug Administration Staff Document issued on September 27, 2019. Document originally issued on September 25, 2013.

[90] Federal Trade Commission (2016, June 24) Mobile Health App Developers: FTC Best Practices, Federal Trade Commission, www.ftc.gov/tips-advice/business-center/guidance/mobile-health-app-developers-ftc-best-practices (online), accessed: 24 Nov.19.

[91] L. Rosenfeld, J. Torous, I.V. Vahia Data security and privacy in apps for dementia: an analysis of existing privacy policies Am. J. Geriatr. Psychiatry, 25 (8) (2017), pp. 873-877, 10.1016/j.jagp.2017.04.009

policy, whereas 68% of them were not adequately transparent with their handling of users data. At the same time, a little bit more than 50% did not possess a privacy policy at all and from the apps that did have one it was usually provided to the user after the collection of information, resulting in the acquiring of data without priory alerting the user on the manner in which they will be used.[92]

3. ARTIFICIAL INTELLIGENCE/AI

According to the definition in the Oxford Dictionary AI is considered: "the theory and development of computer systems able to perform tasks normally requiring human intelligence, such as visual perception, speech recognition, decision-making, and translation between languages." In the era of big data, AI can contribute to the early prediction and response to disease predisposition and spreading, has the ability to detect patterns and educate itself from prior experience, ameliorating and altering its reaction to future cases.[93]

AI alongside robotics constitutes a revolutionary and promising technology capable of adding to the progress of humankind, while at the same time exists right at the centre of new challenges and questions, regarding its lawful function, ethical nature, and economical prospect. More specifically, in the healthcare sector the capacity to analyse a vast collection of patient data and produce automatically tailored made decisions, usually from a distance, not only can facilitate the process of medical decision making but also democratise it, as an increasing number of patients will have access to more personalised medicine, especially on the medical field of oncology.[94] However, this also raises ethical questions, regarding informed consent, and the right to have the information explained in a comprehensive way, as well as rights of privacy and in relation to processing sensitive information.

3.1 AI AND THE EU

The initiating step in the EU was made in 2016 when the European Parliament's Committee on Legal Affairs (JURI) published the draft report on "Civil Law Rules on Robotics",[95] which was later adopted by the European Parliament in 2017 with recommendations to the European Commission.[96] The latter in April 2018 took a

---

[92] • Kristen O'Loughlinab , Martha Nearybc , Elizabeth C.Adkinsb , Stephen M.Schueller, (2019), Reviewing the data security and privacy policies of mobile apps for depression, Internet Interventions, Volume 15, March 2019, Pages 110-115, https://doi.org/10.1016/j.invent.2018.12.001

[93] https://www.lexology.com/library/detail.aspx?g=4284727f-3bec-43e5-b230-fad2742dd4fb (online) accessed: 26 Nov 19.

[94] Furlow, B. (2016, March 2015). IBM Watson Collaboration Aims to Improve Oncology Decision Support Tools.http://www.cancernetwork.com/mbcc-2016/ibm-watson-collaboration-aims-improve-oncologydecision-support-tools (online) accessed: 26 Nov.19

[95] EU Committee on Legal Affairs. (2016). Draft report with recommendations to the Commission on Civil Law Rules on Robotics. May 31

[96] European Parliament resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL)), http://www.europarl.europa.eu/doceo/document/TA-8-2017-0051_EN.html (online) accessed: 26 Nov.19

leading step towards the development of a framework for AI in the EU and established a strategy (pursuant to the agreement of 24 Member States and Norway on AI - European Commission Communication on "Artificial Intelligence for Europe[97]) to establish the principles and values upon which AI should be based upon, with explicit reference to the GDPR and Article 2 of the Treaty on EU, focusing on a humanitarian approach, based on justice, non- discrimination and freedom.

Through that Communication, the Commission announced the creation of an independent High – Level Expert Group on AI (AI HLEG)[98] and an initiative called AI Alliance.[99] The AI HLEG produced documents concerning ethical principles that should determine the AI's function together with a definition for this kind of technology. The first document on trustworthy AI by the AI HLEG, and the ethical guidelines for it, is the "Ethics Guidelines for Trustworthy AI"[100] and it also constitutes a part of the latest Communication of the EU Commission (Communication: Building Trust in Human-Centric Artificial Intelligence[101]), both published on 8th of April 2019. The guidelines point out three fundamental components for the achievement of trustworthy AI: a) compliance with the law, b) fulfillment of ethical principles and c) robustness.
Apart from these key factors, the AI HLEG produced 7 key principles and requirements relating to ethical and trustworthy AI.
These requirements are:

1. Human agency and oversight
2. Technical robustness and safety
3. Privacy and data governance
4. Transparency
5. Diversity, non-discrimination, and fairness
6. Societal and Environmental well-being
7. Accountability

In relation to the general launching of the EU's strategy for the emerging technological innovation that is AI technology, the AI HLEG proposed also a definition for this kind of technology, with its document "A definition of AI: Main capabilities and scientific disciplines"[102], taking into account both its role as a software but also as a scientific discipline, . The definition proposed is the following:
"Artificial intelligence (AI) systems are software (and possibly also hardware) systems designed by humans that, given a complex goal, act in the physical or digital dimension by perceiving their environment through data acquisition, interpreting the collected structured or unstructured data, reasoning on the knowledge, or processing the

[97] European Commission https://ec.europa.eu/digital-single-market/en/news/communication-artificial-intelligence-europe(online) accessed: 226 Nov.19

[98] AI HLEGhttps://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai (online) accessed: 26 Nov 19.

[99] https://ec.europa.eu/digital-single-market/en/european-ai-alliance (online) accessed: 26 Nov 19.

[100] https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai (online) accessed: 26 Nov 19

[101] https://ec.europa.eu/digital-single-market/en/news/communication-building-trust-human-centric-artificial-intelligence (online) accessed: 26 Nov 19.

[102] https://ec.europa.eu/digital-single-market/en/news/definition-artificial-intelligence-main-capabilities-and-scientific-disciplines (online) accessed: 26 Nov 19

information, derived from this data and deciding the best action(s) to take to achieve the given goal. AI systems can either use symbolic rules or learn a numeric model, and they can also adapt their behavior by analyzing how the environment is affected by their previous actions.
As a scientific discipline, AI includes several approaches and techniques, such as machine learning (of which deep learning and reinforcement learning are specific examples), machine reasoning (which includes planning, scheduling, knowledge representation and reasoning, search, and optimization), and robotics (which includes control, perception, sensors and actuators, as well as the integration of all other techniques into cyber-physical systems)".

Last but not least, the independent advisory body to the President of the European Commission, the European Group on Ethics in Science and New Technologies, created also a document on Artificial Intelligence, Robotics and "Autonomous Systems"[103], highlight similar principles together with safety, security, physical and mental integrity, and sustainability.

3.2 AI AND THE US

The US's approach to Artificial Intelligence is more business orientated, favorizing private stakeholders in the field, such as leading tech giants and innovative universities. It's AI policy is base on Research & Development, since in October 2016 the White House issued a report on USA's strategy for AI, "Preparing for the Future of Artificial Intelligence"[104], followed by two additional reports, one on R&D[105] and one on Economics. Its overall tone is confident, addressing both the public and the technological sector, stressing the need for " a good AI society", where AI works for the benefit of the people and the government appears not to provide with federal regulation, but a rather peripheral scope of action, not wanting to hamper the progress of innovation and research, which will boost the US economy to the future. Instead, even though not explicitly mentioned in the report, the US government's strategy is in favor of a more self- regulatory approach, according to which the institutionalization of members of the private sector will aid in formin the necessary values and ethical principles for AI's proper use. However, with the absence of federal regulation, the ability of one to self-regulate raises a concern for the lack of inclusivity and protection of all parties concerned in the process, as such a strategy appears more favorable only to large private tech corporations, to regulate themselves at their own discretion.

---

[103] https://ec.europa.eu/info/sites/info/files/european_group_on_ethics_ege/ege_ai_statement_2018.pdf (online) accessed: 26 Nov 19

[104] Executive Office of the President National Science and Technology Council Committee on Technology. (2016). Preparing for the Future of Artificial Intelligence. Washington D.C. USA. https://www.whitehouse.gov/sites/default/files/whitehouse_files/microsites/ostp/NSTC/preparing_for_the_future_of_ai.pdf (online) accessed: 27 Nov 19

[105] The OSTP's companion document, entitled the "National Artificial Intelligence Research and Development Strategic Plan", details how R&D investments can be used to advance policies that have a positive long term impact on society and the world. 2016, pp. 7-10.

A similar intent and tactic continue in May 2018[106] with the announcement of the White House to sustain the American Leadership on the field of AI through the promotion of public R&D and the removing of obstacles to innovative efforts. Consequently, the reluctance of federal legislators to produce a solid regulatory framework on AI lead in January 2019 the private sector to take up the initiative. Accenture[107], an American company, published a report drafting the framework needed to aid the federal agencies in the evaluation, development, and monitoring of systems such as AI. In addition, US's Defense Advanced Research Projects Agency (DARPA), launched a programme/ campaign called " AI Next"[108] in order to tackle issues impeding the progress of AI technology, such as extreme dependence on data, incapacity of explaining the results and obstacles relating to lack of understanding of the overall context provided by AI systems.

The data privacy concerns, although, are usually dealt with through the fractional US data protection system, one that is appointed to two different bodies. The Federal Communications Commission (FCC) and the Federal Trade Commission (FTC) are responsible for sanctions relating to privacy rights infringement[109] while at the same time seek out to eliminate unjustly and deceiving practices from the market, which due to its duality as a system hampers the general function of the industry.

3.3 AI AND ETHICS

In the last five years, and especially from 2016 and after, according to the results of a study published in *nature machine intelligence,* there is an increasing number of guidelines issued (soft-law), concerning the ethical aspect of AI technology.[110] According to the study, conducted on 84 documents relating to ethical guidelines on AI, there is a mutual interest that it is emerging in the global community, deriving both from the private and the public sector.

To elaborate more, there can be observed an increase in the number of documents referring to ethical issues of AI technology produced by various important stakeholders such as private companies, governmental committees, academic and research institutes, as well as non-governmental organizations. Based on the study, the result was that the majority of the above-mentioned documents derive from the most developed countries, able to sustain the largest economies. First, amongst them, is the US, followed by the UK, Japan, Germany, France, and Finland.[111] However, there is a

[106] https://www.whitehouse.gov/ai/ (online) accessed: 27 Nov 19

[107] https://www.accenture.com/_acnmedia/pdf-92/accenture-afs-responsible-ai.pdf (online) accessed: 27 Nov 19

[108] https://www.darpa.mil/work-with-us/ai-next-campaign (online) accessed: 27 Nov 19

[109] FTC Act/ Section 5/ Unfair practices: "to cause or is likely to cause substantial injury to consumers or cannot reasonably be avoided by consumers' and deceptive practices as 'practices that likely are misleading or actually misleading to consumers".

[110] Jobin, A., Ienca, M. & Vayena, E. The global landscape of AI ethics guidelines. Nat Mach Intell 1, 389–399 (2019),doi:10.1038/s42256-019-0088-2

[111] Jobin, A., Ienca, M. & Vayena, E. The global landscape of AI ethics guidelines. Nat Mach Intell 1, 389–399 (2019), pp 5: "geographical representation shows: US 23.8% , UK 16.7%, Japan 4.8% , Germany, France and Finland 3.6% each.

lack of inclusivity in the representation coming from the global community, like Africa and in general, the South American and the countries in Asia are not represented in the international debate for ethics and AI. As a result, an environment of imbalance of power is created and maintained in the international forum, which not only does not promote convergence towards a united global approach but also leaves little space to local knowledge and cultural pluralism to develop, resulting in fostering inequality worldwide

As far as it comes to the much-needed convergence, as a phenomenon, in fact, it can be traced to a global level. Under thorough examination of the documents produced as guidelines, one can reach to two major conclusions, relating to how the international community handles and approaches technological breakthroughs, like AI technology. Firstly, there can be observed a visible according and convergence as five dominant principles emerge, from the comparison of the guideline documents. These are a) the principle of transparency, b) the principle of justice, c) the principle of non-maleficence, d) the principle of responsibility and e) the principle of privacy.
On the other hand, several other issues seem to be emerging, concerning an alarming contradiction and divergence related to several aspects of these principles. The first of them relates to the problem of how to interpret the principles that have been produced. Second, a controversy has arisen regarding why those principles are considered valuable and important. Third, there exists an obstacle that has to do with what domain, topic or factor these principles should be thought in relation with. Lastly, an important barrier and concern refer to their implementation in general.
Consequently, there derives a need for a global consensus and coordination on these matters, relating to the ethical aspect and questions produced from AI technology. In this effort, a critical and central role must be given to the international organizations, responsible for the promoting of cooperation and mutual understanding, while at the same time the cultural and ethical plurality should not be sacrificed in the process of achieving total uniformity.

3.4 AI AND ROBOTICS IN HEALTHCARE

Robots and robotics, in general, have become a part of everyday life, being increasingly incorporated in every sector and the healthcare sector is no exception. With the significant progress of medicine and the overly challenging working life of adults, there is a need to find new ways to care for the elderly and children in our society. Personal Care robots have been proposed as an innovative solution, able to care for the aforementioned groups of the population, providing assistance, nurturing practices and having anti-stress effects[112].
Personal care robots and companion robots have many uses. They can be providers of assistance for clinical and rehabilitation purposes and serve as an aid to memory, as well as play the role of caretakers responsible for bringing medicine and food to the

[112] Alemi, M., Meghdari, A. & Saffari, E. (2017). RoMa: A hi-tech robotic mannequin for the fashion industry. Lecture Notes in Computer Science (LNCS): Social Robotics, 10652, 209-219.

elderly. Such cases of innovative machinery are the RI-MAN, PaPeRo, and the Care-O-bot.[113]The latter[114] is designed to navigate itself around the house, to facilitate opening doors and to be able to complete tasks such as the procurement of drinks and beverages. Robert[115] is also an example of a care nursing robot, of an experimental nature, which has the size of a human and the appearance of a teddy-bear and can lift patients from their beds in order to place them in their wheelchair.

Apart from these types of advanced robots, robotics in healthcare has already been dominated by other types of technological innovations, such as prostheses but most importantly surgical robots, the most famous amongst them being the da Vinci system, created by Intuitive Surgical Inc. The da Vinci system[116] allows the doctor, through the use of a console, to have a 3D image of the patient and control of three surgical instruments and a forth which is used as a camera, allowing for a more precise, less restricted and safe movement of the operator's hands. However, this is not without its challenges, as operating such a machine needs training and time to master and a 3D image is also significantly different than the real-life experience of a doctor able to actually feel the patient.

Consequently, concern has risen from the incorporation of AI in healthcare, as healthcare will be dehumanized if machines are to replace human contact and communication. In addition, there are some legal issues to be examined from this shift towards a more AI and robotic dominated the healthcare sector. For instance, it is quite clear in the cases of prosthetics and surgical robots that specific Directives can be applied, such as the Council Directive 93/42/EEC concerning medical devices (as amended by Directive 2007/47/EC) ("Medical Device Directive"[117]) and the Council Directive 90/385/EEC on the approximation of the laws of the Member States relating to active implantable medical devices ("AIMDD"). On the contrary, the legal framework for care robots is not so clear. More specifically, some of them, depending on the service that they provide, could be regulated by the Medical Device Directive, as their aim is to provide with services of medicinal nature (e.g. reminding elders to take their medication), but others with a more general use, as movement facilitators, might not fit the definition of a medical device, thus they will be excluded from the Directive's scope.

The major problem with the aforementioned categories of robots and AI systems is that while their owner uses them, they keep collecting and processing data of that specific user. The storage of such sensitive information (e.g. a patient's medication, health status, and biometric information), might be necessary for the robot to process and to use in making suggestions or producing desirable results, while simultaneously

---

[113] Meghdari, A. & Alemi, M. (2018). Recent advances in social & cognitive robotics and imminent ethical challenges. Proceedings of the 10th International RAIS Conference on Social Sciences and Humanities organized by Research Association for Interdisciplinary Studies (RAIS) at The Erdman Center at Princeton University, Princeton, New Jersey, United States.Cambridge, MA: The Scientific Press

[114] http://www.care-obot.de/content/dam/careobot/en/documents/Download/PB_300_309e.pdf (online) acesseed: 26 Nov 19

[115] http://www.riken.jp/en/pr/press/2015/20150223_2/ (online) accessed: 26 Nov 19

[116] http://www.intuitivesurgical.com/ (online) accessed: 26 Nov 19

[117] REGULATION (EU) 2017/745 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 5 April 2017,on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC, implementation date: 26 May 2020

the cloud storage of such data might be perilous in terms of safeguarding one's privacy.
In the Civil Law Rules on Robotics, adopted by the European Parliament in 2017, there are specific references made on how care and medical, as well as human repair and enhancement robotics, should be properly handled. Emphasis is given, in the cases of care robots, in the need for the human factor to remain present and in charge of the care of patients, without allowing the robots to replace human care and interaction. Regarding medical robots, the focus of the framework was on the specific training and certification of the sergeants in order to be able to operate with the aid of robotics safely. Finally, the purpose of human prosthetics is to ameliorate human life and facilitate it, while ensuring that any mechanism introduced into the human body cannot harm its host and that all members of society have proper and equal access to them.

Conclusions

In a world of opportunity and innovation, cutting-edge research and technological advancement are only but natural to develop at the same time a lot of concerns regarding towards what direction this progress can lead to. Without a doubt, the ever-changing world of technology and the growing industry by itself are what alarmed European and national legislators, guiding them to re-evaluate existing norms and legal frameworks. The General Data Protection Regulation was the product of such a need, of the law to be in sync with the modern era and not fall behind, risking to leave a great part of society unprotected. However, historically legislation was never so fast in updating itself to meet the demands of its time. Today constitutes no exception.
Modern technology has provided numerous possibilities, previously dwelling only in the realm of science fiction. Direct-to-consumer genetic testing, mobile health applications, serving various purposes and directed even to mental health conditions, as well as big data analysis and AI technology successfully applicable in healthcare, are only some of the pioneering ways technological progress has influenced the lives and most importantly the health status of billions. The legal framework following this progress appears to be less prepared to cover the novelties emerging every day. On the contrary, legislators opt for a soft-law approach to the issue, fearing to impede the process of research and development, while there is still a need for a solid legal foundation, countries and the public can depend upon.

Regarding ethics and guidelines, a serious effort has been made, in the past few years, towards international coordination and acceptance of the same principles, even though there is much more to be achieved towards that direction. Privacy, in fact, appears to be a key principle for the majority of the global community, hence the need to regulate it further. However, judging from the fact that new ways for infringing this

right occur with the creation of technological projects, surpassing the capacities of the previous ones (e.g. big data analysis in health care, robotics storing sensitive information), specialization and updating of the legal framework is more than necessary, if true protection of privacy is to be achieved.

Bibliography

- 21 C.F.R. § 809.3 (2018), Overview of IVD Regulation, U.S. FOOD & DRUG ADNMwN., https://www.fda.gov/MedicalDevices[DeviceRegulationandGuidance/IVDRegulatoryAssistance (online) accessed : 20 Nov.19.
- 21 U.S.C. § 321(h), (h)(2) (2012).
- 21 U.S.C. § 360c(a)(1)(C)(ii)(I)-(II) (2012).
- 740 ILCS 14/ Biometric Information Privacy Act.
- A description of any reasonably foreseeable risks or discomforts to the subjects (45 CFR 46.116(a)(2)); and A statement describing the extent, if any, to which confidentiality of records identifying the subject will be maintained (45 CFR 46.116(a)(5), GINA, 2008.
- A. Tanner, Strengthening Protection of Patient Medical Data The Century Foundation (2017), https://tcf.org/content/report/strengthening-protection-patient-medical-data , accessed 26/11/19)
- AI HLEGhttps://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai (online) accessed: 26 Nov 19.
- Alemi, M., Meghdari, A. & Saffari, E. (2017). Roma: A hi-tech robotic mannequin for the fashion industry. Lecture Notes in Computer Science (LNCS): Social Robotics, 10652, 209-219.
- Anna Jobin, Marcello Inca & Effy Vayena, (02/09/ 2019), The global landscape of AI ethics guidelines, Nature Machine Intelligence ,volume 1, pages389–399 (2019), https://www.nature.com/articles/s42256-019-0088-2
- Anna Jobin, Marcello Inca & Effy Vayena, (02/09/ 2019), The global landscape of AI ethics guidelines, Nature Machine Intelligence, volume 1, pages389–399 (2019), https://www.nature.com/articles/s42256-019-0088-2
- anonymous in such a way that the data subject is no longer identifiable; whereas codes of conduct within the meaning of Article 27 may be a useful instrument for providing guidance as to the ways in which data may be rendered anonymous and retained in a form in which identification of the data subject is no longer possible;".
- Art. 22 of the German Federal Data Protection Act (BDSG).
- Art. 89 §1, GDPR
- ARTICLE 29 - Data Protection Working Party, Working document on biometrics, Adopted on 1 August 2003, 12168/02/EN
- ARTICLE 29 DATA PROTECTION WORKING PARTY, Opinion 3/2012 on developments in biometric technologies, 00720/12/EN
- Article 29 Working Party. Opinion 4/2007 on the concept of personal data, 2007.
- Article 29 WP: "Anonymization constitutes further processing of personal data; as such, it must satisfy the requirement of compatibility by having regard to the legal grounds and circumstances of the further processing".
- Article 4 §15 of the GDPR: data concerning health' means personal data related to the physical or mental health of a natural person, including the

provision of health care services, which reveal information about his or her health status;
- Article 5 (1b) of the GDPR: collected for specified, explicit and legitimate purposes… not be considered to be incompatible with the initial purposes ('purpose limitation');
- Article 8 of Directive 95/47/EC: The processing of special categories of data "The Member States shall prohibit the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life."
- Article 9 (4), GDPR: "The Member States may maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or data concerning health."
- Article 9 of the GDPR: Processing of special categories of personal data "Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the 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 shall be prohibited."
- Article 9 of the General Data Protection Regulation (EU) 2016/679.
- Article 9 par. 2 of the GDPR.
- Assembly Bill No. 375, California Consumer Privacy Act, Date Published:06/29/2018.
- Beyleveld D, Townend D. When is personal data rendered anonymous? Interpreting recital 26 of Directive 95/46/EC. Med Law Int. 2004;6:73–86.
- Blue Chip Patient Recruitment. Leveraging Mobile Health Technology for Patient Recruitment, October 2012
- California Consumer Privacy Act of 2018 (CCPA), effective into force on January 1, 2020, Assembly Bill No. 375, CHAPTER 55An act to add Title 1.81.5 (commencing with Section 1798.100) to Part 4 of Division 3 of the Civil Code, relating to privacy.
- Case C101-01, Bodil Lindqvist, 6 November 2003.
- Centre for Data Ethics and Innovation, (12/09/2019), Snapshot Paper - AI and Personal Insurance, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/831181/Snapshot_Paper_-_AI_and_Personal_Insurance.pdf [Accessed Online on 22/09/2019].
- Centre for Data Ethics and Innovation, (12/09/2019), Snapshot Paper - AI and Personal Insurance, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/831181/Snapshot_Paper_-_AI_and_Personal_Insurance.pdf
- Chara D. Zerva (Nicolas Kanellopoulos-Chara Zerva and Associates Law Firm Health),(2019), Biometric and Genetic Data Under GDPR, Greek Law Digest the official guide to Greek Law, http://www.greeklawdigest.gr/topics/data-protection/item/304-health-biometric-and-genetic-data-under-gdpr [Accessed Online on 20/05/2019].

- Chara D. Zerva (Nicolas Kanellopoulos-Chara Zerva and Associates Law Firm Health),(2019), Biometric and Genetic Data Under GDPR, Greek Law Digest the official guide to Greek Law, http://www.greeklawdigest.gr/topics/data-protection/item/304-health-biometric-and-genetic-data-under-gdpr [Accessed Online on 20/10/2019].

- Chara D. Zerva (Nicolas Kanellopoulos-Chara Zerva and Associates Law Firm Health),(2019), Biometric and Genetic Data Under GDPR, Greek Law Digest the official guide to Greek Law, http://www.greeklawdigest.gr/topics/data-protection/item/304-health-biometric-and-genetic-data-under-gdpr [Accessed Online on 20/10/2019].

- COMMISSION STAFF WORKING DOCUMENT on the existing EU legal framework applicable to lifestyle and wellbeing apps, accompanying the document GREEN PAPER on mobile Health ("mHealth"), SWD(2014), 10.04.2014.
- COUNCIL DIRECTIVE 93/42/EEC of 14 June 1993 concerning medical devices (OJ L 169, 12.7.1993, p. 1)
- Council of Europe (1997) Convention for the Protection of Human Rights and Dignity of the Human Being with regard to the Application of Biology and Medicine: Convention on Human Rights and Biomedicine. Council of Europe, Oviedo, 4.I.V.1997.
- Council of Europe (2008). Additional Protocol to the Convention on Human Rights and Biomedicine, concerning Genetic Testing for Health Purposes., 01/07/2018- 5 Ratifications including 4 Member States. https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/203 (online), accessed: 22 Nov.2019.
- Darius Štitilis, Marius Laurinaitis,(2017), Treatment of biometrically processed personal data: Problem of uniform practice under EU personal data protection law, Computer Law & Security Review, Volume 33, Issue 5, October 2017, Pages 618-628, https://doi.org/10.1016/j.clsr.2017.03.012
- Directive 2011/24/EU of the European Parliament and of the Council of 9 March 2011 on the application of patients' rights in cross-border healthcare (OJ L 88, 4.4.2011, p. 45).
- 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, Official Journal L 281, 23/11/1995 P. 0031 – 0050.
- EU Commission's GREEN PAPER on mobile Health ("mHealth"),COM(2014)219 10.4.2014, final.
- EU Committee on Legal Affairs. (2016). Draft report with recommendations to the Commission on Civil Law Rules on Robotics. May 31
- European Commission (2016) The Black List: banned commercial practices - European Commission – DGhttp://ec.europa.eu/justice/consumer-marketing/unfair-trade/unfair-practices/is-it-fair/blacklist/index_en.htm (online), accessed: 22 Nov.2019.
- European Commission https://ec.europa.eu/digital-single-market/en/news/communication-artificial-intelligence-europe(online) accessed: 226 Nov.19

- EUROPEAN DATA PROTECTION SUPERVISOR The History of the General Data Protection Regulation: “EC proposal to strengthen online privacy rights and digital economy the European Commission proposes a comprehensive reform of the EU's 1995 data protection rules to strengthen online privacy rights and boost Europe's digital economy.” (https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en accessed online 11/10/2019).
- EUROPEAN DATA PROTECTION SUPERVISOR, The History of the General Data Protection Regulation: “It replaces the1995 Data Protection Directive which was adopted at a time when the internet was in its infancy”.(https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en accessed online 11/10/2019).
- EUROPEAN DATA PROTECTION SUPERVISOR, The History of the General Data Protection Regulation: “In 2016, the EU adopted the General Data Protection Regulation (GDPR) … The timeline below contains key dates and events in the data protection reform process from 1995 to 2018”. (https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en accessed online 11/10/2019).
- European Parliament and Council (1998) Directive 98/79/EC of the European Parliament and of the Council of 27 October 1998 on in vitro diagnostic medical devices.http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31998L0079:EN:HTML (online), accessed: 22 Nov.19.
- European Parliament and the Council of the EU (2005) Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 Concerning unfair business-to-consumer commercial practices in the internal market and amending council directive 84/450/EEC, directives 97/7/EC, 98/27/EC and 2002/65/EC of (2005).
- European Parliament resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL)), http://www.europarl.europa.eu/doceo/document/TA-8-2017-0051_EN.html (online) accessed: 26 Nov.19
- Executive Office of the President National Science and Technology Council Committee on Technology. (2016). Preparing for the Future of Artificial Intelligence. Washington D.C. USA. https://www.whitehouse.gov/sites/default/files/whitehouse_files/microsites/ostp/NSTC/preparing_for_the_future_of_ai.pdf (online) accessed: 27 Nov 19
- Federal Act concerning the Protection of Personal Data (DSG), Part 2 §2 & §3.
- Federal Data Protection Act of 30 June 2017 (Federal Law Gazette I p. 2097, (BDSG), Sub-chapter 1, Section 22§2 and Sub-chapter 2, Section 27.
- Federal Trade Commission (2016, June 24) Mobile Health App Developers: FTC Best Practices, Federal Trade Commission, www.ftc.gov/tips-advice/business-center/guidance/mobile-health-app-developers-ftc-best-practices (online), accessed: 24 Nov.19.
- FTC Act/ Section 5/ Unfair practices: “to cause or is likely to cause substantial injury to consumers or cannot reasonably be avoided by consumers' and

deceptive practices as 'practices that likely are misleading or actually misleading to consumers".

- Furlow, B. (2016, March 2015). IBM Watson Collaboration Aims to Improve Oncology Decision Support Tools.http://www.cancernetwork.com/mbcc-2016/ibm-watson-collaboration-aims-improve-oncologydecision-support-tools (online) accessed: 26 Nov.19
- Gemalto a Thales Company,(2019), Biometric data and the General Data Protection Regulation, https://www.gemalto.com/govt/biometrics/biometric-data [Accessed Online on 20/05/2019].
- Godard B, Kääriäinen H, Kristoffersson U, Tranebjaerg L, Coviello D, Aymé S (2003) Provision of genetic services in Europe: current practices and issues. Eur J Hum Genet 11(S2): S13–S48. https://doi.org/10.1038/sj.ejhg.5201111 (online), accessed: 22 Nov.19
- Gottlieb, M.D., on Implementation of Agency's Streamlined Development and Review Pathway for Consumer Tests That Evaluate Genetic Health Risk (Nov. 6, 2017), https://www.fda.gov/NewsEvents/Newsroom/PressAnnouncements/ucm583885.htm.(online), accessed: 20 Nov.2019.
- Guidance for Industry and Food and Drug Administration Staff Document issued on September 27, 2019. Document originally issued on September 25, 2013.
- Health Insurance Portability and Accountability Act (HIPAA)
- High-Level Expert Group on Artificial Intelligence, https://ec.europa.eu/futurium/en/ai-alliance-consultation/guidelines#Top [Accessed Online 22/09/2019].
- High-Level Expert Group on Artificial Intelligence, https://ec.europa.eu/digital-single-market/en/news/policy-and-investment-recommendations-trustworthy-artificial-intelligence [Accessed Online on 22/09/2019].
- http://www.care-obot.de/content/dam/careobot/en/documents/Download/PB_300_309e.pdf (online) acesseed: 26 Nov 19
- http://www.intuitivesurgical.com/ (online) accessed: 26 Nov 19
- http://www.riken.jp/en/pr/press/2015/20150223_2/ (online) accessed: 26 Nov 19
- https://ec.europa.eu/digital-single-market/en/european-ai-alliance (online) accessed: 26 Nov 19.
- https://ec.europa.eu/digital-single-market/en/news/communication-building-trust-human-centric-artificial-intelligence (online) accessed: 26 Nov 19.
- https://ec.europa.eu/digital-single-market/en/news/definition-artificial-intelligence-main-capabilities-and-scientific-disciplines (online) accessed: 26 Nov 19
- https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai (online) accessed: 26 Nov 19
- https://ec.europa.eu/digital-single-market/en/news/first-european-directory-health-apps-recommended-patients-and-consumers (online),accessed: 24 Nov.19.

- https://ec.europa.eu/info/sites/info/files/european_group_on_ethics_ege/ege_ai_statement_2018.pdf (online) accessed: 26 Nov 19
- https://www.accenture.com/_acnmedia/pdf-92/accenture-afs-responsible-ai.pdf (online) accessed: 27 Nov 19
- https://www.darpa.mil/work-with-us/ai-next-campaign (online) accessed: 27 Nov 19
- https://www.happtique.com/ (online), accessed: 24 Nov.2019
- https://www.lexology.com/library/detail.aspx?g=4284727f-3bec-43e5-b230-fad2742dd4fb (online) accessed : 26 Nov 19.
- https://www.whitehouse.gov/ai/ (online) accessed: 27 Nov 19
- Human Research Protection, Genetic Information Nondiscrimination Act Guidance (2009), March 24, 2009.
- J. Kulynych and Henry T. Greely, Clinical Genomics, Big Data, and Electronic Medical Records: Reconciling Patient Rights With Research When Privacy and Science Collide, 4 J. law. Biosci. 94, 132, 122 (2017).
- J. Torous, L.W. Roberts,(2017), Needed innovation in digital health and smartphone applications for mental health transparency and trust JAMA Psychiatry, 74 (5) (2017), pp. 437-438, 10.1001/jamapsychiatry.2017.0262
- Jobin, A., Inca, M. & Vayena, E. The global landscape of AI ethics guidelines. Nat Mach Intell 1, 389–399 (2019),DOI:10.1038/s42256-019-0088-2
- Jobin, A., Inca, M. & Vayena, E. The global landscape of AI ethics guidelines. Nat Mach Intell 1, 389–399 (2019), pp 5 : “ geographical representation shows: US 23.8% , UK 16.7%, Japan 4.8% , Germany, France and Finland 3.6% each.
- K. Benitez and B. Malin, Evaluating Re-identification Risks With Respect to the HIPAA Privacy Rule, 17 J. am. med. inform. assoc. 169, 177 (2010).
- Kalokairinou, L., Howard, H.C., Slokenberga, S. et al. J Community Genet (2018) 9: 117. https://doi.org/10.1007/s12687-017-0344-2 (online), accessed: 22 Nov.19.
- Kristen O'Loughlinab , Martha Nearybc , Elizabeth C.Adkinsb , Stephen M.Schueller, (2019), Reviewing the data security and privacy policies of mobile apps for depression, Internet Interventions, Volume 15, March 2019, Pages 110-115, https://doi.org/10.1016/j.invent.2018.12.001
- L. Rosenfeld, J. Torous, I.V. Vahia Data security and privacy in apps for dementia: an analysis of existing privacy policies Am. J. Geriatr. Psychiatry, 25 (8) (2017), pp. 873-877, 10.1016/j.jagp.2017.04.009
- L.Mitrou, The General Data Protection Regulation, Athens 2017, pp.25, etc.
- LAURA JEHL AND ALAN FRIEL, BAKERHOSTETLER LLP, A Chart comparing some of the key requirements of the California Consumer Privacy Act (CCPA) and the EU General Data Protection Regulation (GDPR), https://www.bakerlaw.com/webfiles/Privacy/2018/Articles/CCPA-GDPR-Chart.pdf, (Online), accessed on 26 Nov. 19.
- Law 2472/1997.
- LAw360 (Mar. 22, 2016, 11:47 AM), https://www.1aw360.com/articles/772679/fda-challenges-direct-to-consumer-genetic-tests. (Online) accessed: 20 Nov. 19.

- Mahsa Shabani & Pascal Borry, (2017), Rules for processing genetic data for research purposes in view of the new EU General Data Protection Regulation, European Journal of Human Genetics volume 26, pages149–156 (2018), https://www.nature.com/articles/s41431-017-0045-7 Accessed Online on 20/05/2019].
- Mahsa Shabani & Pascal Borry, (2017), Rules for processing genetic data for research purposes in view of the new EU General Data Protection Regulation, European Journal of Human Genetics volume 26, pages149–156 (2018), https://www.nature.com/articles/s41431-017-0045-7 [Accessed Online on 20/05/2019].
- Marie Figarella, (2017), Global consensus emerges on biometric data protection, Biometric Technology Today, Volume 2017, Issue 10, November–December 2017, Pages 5-7, https://doi.org/10.1016/S0969-4765(17)30152-2
- Meghdari, A. & Alemi, M. (2018). Recent advances in social & cognitive robotics and imminent ethical challenges. Proceedings of the 10th International RAIS Conference on Social Sciences and Humanities organized by Research Association for Interdisciplinary Studies (RAIS) at The Erdman Center at Princeton University, Princeton, New Jersey, United States.Cambridge, MA: The Scientific Press
- mHealth app development economics 2016: the current status and trends of the mHealth app market, http://research2guidance.com/r2g/r2g-mHealth-App-Developer-Economics-2016.pdf (online), accessed: 24 Nov. 19.
- Nancy K. Stade et al., FDA Challenges Direct-to-Consumer Genetic Tests,
- of 5 April 2017, on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC, implementation date: 26 May 2020
- Patient Adoption of mHealth: Use, Evidence and Remaining Barriers to Mainstream Acceptance,(2015),https://www.iqvia.com/-/media/iqvia/pdfs/institute-reports/patient-adoptionofmhealth.pdf?la=en&hash=B3ACFA8ADDB143F29EAC0C33D533BC5D7AABD689 (online), accessed: 24. Nov.19.
- Policy for Device Software Functions and Mobile Medical Applications
- Press Release, U.S. Food & Drug Admin., Statement from FDA Commissioner Scott
- Recital 26 of Directive 95/46/ EC: “Whereas the principles of protection must apply to any information concerning an identified or identifiable person; whereas, to determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify
- Recital 34 of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation- GDPR).
- Recital 35 of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation- GDPR).

- Recital 39 of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation- GDPR).
- Recital 51 of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation- GDPR).
- Recital 53 of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation- GDPR).
- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation- GDPR).
- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation- GDPR).
- REGULATION (EU) 2017/745 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL
- Robert Breedon and Jocelyn Paulley,(2019), What are the data protection challenges of using AI in healthcare?, www.lexology.com, https://www.lexology.com/library/detail.aspx?g=4c2d1c89-7be1-4a7c-958d-5112c84a18f9 [Accessed Online on 20/05/2019].
- Rosenbach v. Six Flags Entertainment Corp., 2019 IL 123186, Supreme Court, 25th of January.
- Schedule 3 of the UK Data Protection Act (2018).
- Sharkey, C. M. (2019). Direct-to-consumer genetic testing: The FDA's dual role as a safety and health information regulator. DePaul Law Review, 68(2), 343-384. https://heinonline.org/HOL/Page?collection=journals&handle=hein.journals/deplr68&id=372&men_tab=srchresults# (online) accessed: 20 Nov.2019).
- Stefanos Tsimikalis, 05/03/2019, GDPR & Employee Personal Data, by Tsimikalis Kalonarou Law Firm, http://www.greeklawdigest.gr/topics/data-protection/item/314-gpdr-and-employee-personal-data accessed online 11/10/19).
- Stop Secret Surveillance Ordinance (05/06/2019), Board of Supervisors.
- The Greek Constitution Article 9, Article 9A (right to privacy) & (right to protection of personal information, Article 2§1 (right to dignity) and Article 5 §1 (right to developing freely one's personality).
- The Health Insurance Portability and Accountability Act of 1996 (HIPAA). P.L. No. 104-191, 110 Stat. 1938 (1996).
- The New England Center for Investigative Reporting, Boston University, "Lacking regulation, many medical apps questionable at best", 18.11.2012

- The OSTP's companion document, entitled the "National Artificial Intelligence Research and Development Strategic Plan", details how R&D investments can be used to advance policies that have a positive long term impact on society and the world. 2016, pp. 7-10.
- the said person; whereas the principles of protection shall not apply to data rendered
- TITLE I—GENETIC NONDISCRIMINATION IN HEALTH INSURANCE, GINA 2008.
- TITLE II—PROHIBITING EMPLOYMENT DISCRIMINATION ON THE BASIS OF GENETIC INFORMATION, GINA 2008.
- Top 3 therapy fields with the best market potential for digital health apps (2017)https://research2guidance.com/top-3-therapy-fields-with-the-best-market-potential-for-digital-health-apps (online), accessed: 24 Nov.19. & IMS Institute for Healthcare Informatics
- U.S. FOOD & DRUG ADMIN., FDA-2011-D-0577, GUIDANCE FOR INDUSTRY AND FOOD AND DRUG ADMINISTRATION STAFF: FACTORS TO CONSIDER WHEN MAKING BENEFIT-RISK DETERMINATIONS IN MEDICAL DEVICE PREMARKET APPROVAL AND DE Novo CLASSIFICATIONS 4 (2016) https://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM517504.pdf (online), accessed: 20 Nov.2019.
- World Health Organisation "mHealth – New horizons for health through mobile technologies, Global Observatory for eHealth series – Volume 3", page 6
- WP 80.
- WP193.
- Νόμος 4624/2019, Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, μέτρα εφαρμογής του Κανονισμού (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και ενσωμάτωση στην εθνική νομοθεσία της Οδηγίας (ΕΕ) 2016/680 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 και άλλες διατάξεις.

- Νόμος 4624/2019, Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, μέτρα εφαρμογής του Κανονισμού (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και ενσωμάτωση στην εθνική νομοθεσία της Οδηγίας (ΕΕ) 2016/680 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 και άλλες διατάξεις.

Appendix

- Article 4 §15 of the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation- GDPR).
- Article 4 §13 of the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation- GDPR).
- Article 4 §14 of the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation- GDPR).
- Article 9 of the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation- GDPR).
- Recital 39 of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation- GDPR).
- Recital 35 of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation- GDPR).
- Directive 2011/24/EU of the European Parliament and of the Council of 9 March 2011 on the application of patients' rights in cross-border healthcare (OJ L 88, 4.4.2011, p. 45).
- Recital 34 of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation- GDPR).
- ARTICLE 29 - Data Protection Working Party, Working document on biometrics , Adopted on 1 August 2003, 12168/02/EN WP 80.
- Recital 51 of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation- GDPR).
- Article 5 (1b) of the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation- GDPR).

- Article 9 par. 2 of the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation- GDPR).
- Recital 53 of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation- GDPR).
- Art. 22 of the German Federal Data Protection Act (BDSG).
- Schedule 3 of the UK Data Protection Act (2018).
- 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, Official Journal L 281 , 23/11/1995 P. 0031 – 0050.
- Recital 26 of Directive 95/46/ EC
- Article 8 of Directive 95/47/ EC
- Art. 89 §1 , GDPR
- Federal Data Protection Act of 30 June 2017 (Federal Law Gazette I p. 2097, (BDSG) , Sub-chapter 1, Section 22§2 and Sub-chapter 2, Section 27
- Federal Act concerning the Protection of Personal Data (DSG), Part 2 §2 & §3.
- The Health Insurance Portability and Accountability Act of 1996 (HIPAA). P.L. No. 104-191, 110 Stat. 1938 (1996).
- 'Genetic Information Non-discrimination Act, PUBLIC LAW 110–233—MAY 21, 2008
- Assembly Bill No. 375, California Consumer Privacy Act, Date Published:06/29/2018
- Rosenbach v. Six Flags Entertainment Corp., 2019 IL 123186, Supreme Court, 25th of January, "*an individual need not allege some actual injury or adverse effect, beyond violation of his or her rights under the Act, in order to qualify as an "aggrieved" person and be entitled to seek liquidated damages and injunctive relief pursuant to the Act*." (The Biometric Privacy Information Act (740 ILCS 14/1 et seq. (West 2016)).
- 740 ILCS 14/ Biometric Information Privacy Act
- Stop Secret Surveillance Ordinance (05/06/2019), Board of Supervisors.
- 21 U.S.C. § 321(h), (h)(2) (2012).
- 21 U.S.C. § 360c(a)(1)(C)(ii)(I)-(II) (2012)
- U.S. FOOD & DRUG ADMIN., FDA-2011-D-0577, GUIDANCE FOR INDUSTRY AND FOOD AND DRUG ADMINISTRATION STAFF: FACTORS TO CONSIDER WHEN MAKING BENEFIT-RISK DETERMINATIONS IN MEDICAL DEVICE PREMARKET APPROVAL AND DE Novo CLASSIFICATIONS 4 (2016)
- European Parliament and the Council of the EU (2005) Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 Concerning unfair business-to-consumer commercial practices in the internal market and amending council directive 84/450/EEC, directives 97/7/EC, 98/27/EC and 2002/65/EC of (2005).
- COUNCIL DIRECTIVE 93/42/EEC of 14 June 1993 concerning medical devices (OJ L 169, 12.7.1993, p. 1)

- European Parliament and Council (1998) Directive 98/79/EC of the European Parliament and of the Council of 27 October 1998 on in vitro diagnostic medical devices.
- Council of Europe (1997) Convention for the Protection of Human Rights and Dignity of the Human Being with regard to the Application of Biology and Medicine: Convention on Human Rights and Biomedicine. Council of Europe, Oviedo, 4.I.V.1997.
- Council of Europe (2008). Additional Protocol to the Convention on Human Rights and Biomedicine, concerning Genetic Testing for Health Purposes., 01/07/2018- 5 Ratifications including 4 member States.
- COMMISSION STAFF WORKING DOCUMENT on the existing EU legal framework applicable to lifestyle and wellbeing apps, accompanying the document GREEN PAPER on mobile Health ("mHealth"), SWD(2014), 10.04.2014.
- EU Committee on Legal Affairs. (2016). Draft report with recommendations to the Commission on Civil Law Rules on Robotics. May 31
- European Parliament resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL))
- Federal Trade Commission Act/ Section 5/ Unfair practices.
- Article 7 of the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation- GDPR).
- Recital 33 of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation- GDPR