TILBURG UNIVERSITY

Understanding Society

Master Thesis

Law and Technology LLM

Tilburg Law School

2022-2023

The IoT era, the notion of vulnerability, and the appropriate principles for vulnerable data subjects under the GDPR

Vanina Pashova

SNR: u1272203

Supervisor: Dr. Lorenzo Dalla Corte

Second Reader: Tjaša Petročnik

Table of contents

Chapter 1- Introduction

1.Background

Technology continues to improve.[1] In the vast landscape of connected technologies, the Internet of Things (IoT)[2] represents a revolutionary concept that facilitates our lives, by enabling the communication between electronic devices and sensors through the internet.[3] The concept of the IoT constitutes of a net of physical devices, as well as vehicles, appliances, and other objects equipped with sensors, software, and connectivity, that can collect and exchange data over the Internet.[4]

The IoT incorporates the idea of a seamlessly interconnected ecosystem in which everyday objects can communicate with each other, creating a web of information that facilitates automation, efficiency, and improved decision-making.[5] These objects, often referred to as *"smart[6] devices"* or *"smart objects,"* can[7] include everything, from wearable fitness trackers, smartphones, and household appliances to smart city infrastructure, industrial equipment, and environmental sensors.[8] The impetus for IoT is the rapid increase in computing power, miniaturization of electronic components, and the increasing availability of Internet connectivity. These advances have made it possible to embed sensors, processors, and network connectivity into previously mundane objects, empowering them to sense, analyse, and transmit data.

The potential applications of the IoT encompass various domains.[9] For instance, in the field of healthcare, these devices are able to observe the vital signs of patients in real-time, allowing for remote patient monitoring, personalized healthcare plans, and prompt intervention in critical situations.[10] Another application could be found in agriculture, where smart sensors placed in fields can keep track on the moisture of the soil and temperature, enabling farmers to maximize irrigation, conserve water, and enhance crop yield. In transportation, IoT enables the communication of connected

[1] Vermesan, Ovidiu, and Peter Friess, eds. *Internet of things: converging technologies for smart environments and integrated ecosystems*. River publishers, 2013, p. 3.

[2] Hassan, Qusay F., and Sajjad A. Madani, eds. "Internet of things: Challenges, advances, and applications." (2017), p.1.

[3] Kumar, Sachin, Prayag Tiwari, and Mikhail Zymbler. "Internet of Things is a revolutionary approach for future technology enhancement: a review." *Journal of Big data* 6, no. 1 (2019): 1-21.

[4] Meneghello, Francesca, Matteo Calore, Daniel Zucchetto, Michele Polese, and Andrea Zanella. "IoT: Internet of threats? A survey of practical security vulnerabilities in real IoT devices." *IEEE Internet of Things Journal* 6, no. 5 (2019): 8182-8201.

[5] Vermesan, Ovidiu, and Friess. *Building the Hyperconnected Society-Internet of Things Research and Innovation Value Chains, Ecosystems and Markets*. Taylor & Francis, 2015, p 15.

[6] Sunyaev, Ali and A. Sunyaev. *Internet computing.* New York, NY, USA: Springer International Publishing,2020.

[7] Sunyaev and Sunyaev. *Internet computing*

[8] Ovidiu and Friess, *Building the Hyperconnected Society* (n'18).

[9] Gubbi, Jayavardhana, Rajkumar Buyya, Slaven Marusic, and Marimuthu Palaniswami. "Internet of Things (IoT): A vision, architectural elements, and future directions." *Future generation computer systems* 29, no. 7 (2013): 1645-1660, p 1.

[10] Gubbi, Buyya, Marusic, and Palaniswami, *Future generation computer systems* (n'8).

vehicles with traffic infrastructure and other vehicles, leading to improved traffic flow, reduced congestion, and enhanced road safety.[11] Despite the wide range that the IoT devices encompass, this thesis will focus mainly on IoT wearable devices for health purposes, and in chapter 4 the range of the research will come down to fitness trackers. In the healthcare domain, IoT devices play a vital role in remote data subject monitoring and personalised healthcare plans. Real-time monitoring of significant signs empowers healthcare providers to intervene promptly in critical situations.

However, despite the enormous potential in healthcare, IoT devices also pose challenges.[12] Security and privacy are major concerns since IoT devices collect, transmit, and operate enormous quantities of personal data to function properly and efficiently. Furthermore, as more devices become connected, this increases the potential attack surface and raises questions about the protection of sensitive data. Additionally, the extensive amount of data that IoT devices generate, requires an adequate data management and analytics solutions to extract valuable insights and ensure data-driven decision-making. Further, aggravating the problem leads to leaving data subjects' data transmitting freely in cyberspace. Among the most serious concerns about the usage of the IoT, 28% of consumers indicate that they are disturbed that someone may hack into the device and do something malicious.[13] Another 26% of the consumers are concerned because they are unfamiliar of how their data is processed by the devices, and how this data will be used.[14] It has been indicated that wearable devices collect and store health data continuously.[15] The data collected is often stored either on a cloud, (which might be either public or private), or on other kinds of distributed systems, constituting of a node that acts autonomously, while being interconnected with all other nodes of the network.[16] In practice, the node stipulates each connected device in the network.[17] Hence, the issue becomes more problematic, since the heterogeneity of this data may give rise to misuse of health information by unauthorized users, because the security issues are always at stake and going with pace, whereas the privacy of data subjects might be considered as being always at risk.[18]

[11] Gubbi, Buyya, Marusic, and Palaniswami, *Future generation computer systems* (n'8).

[12] Borgia, Eleonora. "The Internet of Things vision: Key features, applications and open issues." *Computer Communications* 54 (2014): 1-31.

[13] Ching, Ke Wan, and Manmeet Mahinderjit Singh. "Wearable technology devices security and privacy vulnerability analysis." *International Journal of Network Security & Its Applications* 8, no. 3 (2016): 19-30, p.24.

[14] Ching, Wan and Singh. "Wearable technology devices security, (n'24).

[15] Kapoor, Vidhi, Rishabh Singh, Rishabh Reddy, and Prathamesh Churi. "Privacy issues in wearable technology: An intrinsic review." In *Proceedings of the International Conference on Innovative Computing & Communications (ICICC)*. 2020, p.1.

[16] Jiang, Yichuan. "A survey of task allocation and load balancing in distributed systems." *IEEE Transactions on Parallel and Distributed Systems* 27, no. 2 (2015): 585-599, p. 585.

[17] Tech4Good, IoT node, accessed on 19/08/2022, https://marketplace.intelligentcitieschallenge.eu/en/solutions/iot-node#:~:text=In%20other%20words%2C%20the%20IoT,multiple%20sensors%20with%20diverse%20origins.

[18] Kapoor, Vidhi, Singh, Reddy, and Churi, *Proceedings of the International Conference on Innovative Computing & Communications.*

Since the focus of the thesis is shifted towards IoT wearable devices for health purposes, it is crucial to mention that data breaches in the healthcare sector could result in stigmatization, discrimination, or direct harm to data subjects. Consider the scenario where someone interferes with the data in your interconnected device, causing it to administer an incorrect lung saturation, leading to potentially wrong diagnosis, or a similar adverse event. Therefore, the European Union[19]**,** known for its stringent data protection regulations, particularly the General Data Protection Regulation (GDPR),[20] places a strong prominence on safeguarding the rights and privacy of data subjects within the IoT ecosystem.[21] Regulatory frameworks such as the GDPR, are extremely reliable in such scenarios because it grants data subjects a range of rights to exercise control over their personal data. These include the right to be informed about the collection and use of their data,[22] the right to access their data,[23] the right to rectify inaccuracies, the right to erasure (also known as the *"right to be forgotten"*),[24] and the right to object to certain processing activities.[25] Additionally, there must be transparent information to data subjects, on how their data is collected, shared, and used.[26] Furthermore, ensured mechanisms must be in place, so data subjects can easily exercise these rights. Furthermore, the GDPR's principle of *"privacy by design and by default*"[27] is particularly relevant in the IoT landscape.

Data collection in unprecedented volumes gives rise to privacy and security concerns for the data subject.[28] Researchers consider that some data subjects are more likely to be mistreated, abused, exploited, or harmed:[29] they are, in other words, vulnerable[30] data subjects. Under the EU data protection legal framework, some examples of vulnerable data subjects might be elderly people, people

[19] Alesina, Alberto, Ignazio Angeloni, and Ludger Schuknecht. "What does the European Union do?." *Public Choice* 123, no. 3-4 (2005): 275-319.

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

[21] Georgiou, Dimitra, and Costas Lambrinoudakis. "Compatibility of a security policy for a cloud-based healthcare system with the EU general data protection regulation (GDPR)." *Information* 11, no. 12 (2020): 586, p.9.

[22] General Data Protection Regulation, Article 13, and Article 14.

[23] General Data Protection Regulation, Article 15 (1).

[24] General Data Protection Regulation, Article 17.

[25] General Data Protection Regulation, Article 21.

[26] General Data Protection Regulation, Article 12 (1).

[27] Article 29 Data Protection Working Party. (2014). Opinion 8/2014 on the Recent Developments on the Internet of Things., p.19.

[28] Martínez-Pérez, Borja, Isabel De La Torre-Díez, and Miguel López-Coronado. "Privacy and security in mobile health apps: a review and recommendations." *Journal of medical systems* 39, no. 1 (2015): 1-8, p.5.

[29] Malgieri and Niklas, "Vulnerable data subjects." (n'1).

[30] Vulnerability Registration Service, *"Data, Vulnerability & GDPR: Considerations for Businesses",* accessed on 22.08.2023 https://www.vulnerabilityregistrationservice.co.uk/data-protection-gdpr-and-vulnerability/

with mental disorders, or mental health conditions[31], asylum seekers, people with disabilities, or injured or chronically ill people.[32] In addition, these are data subjects, who may lack the capacity to act for themselves, for instance by giving explicit consent, without the interference of a guardian. However, the concept of vulnerability is not a term expressing only a black or white perspective.

According to Piasecki and Chen, classifying data subjects as vulnerable requires an assessment based on various factors and contexts.[33] There is no universal definition for a vulnerable data subject, neither on an international level nor on the EU level under the GDPR. The Regulation does not explicitly define vulnerability as a distinct category. However, the GDPR briefly alludes to the existence of such a group of data subjects, referring to them in the context of "*special categories of personal data"* [34], which in fact leaves room for interpretation, and for the extent to which a data subject might be considered as vulnerable. This leads to the idea that vulnerability cannot be precisely defined, however, it can have layers.[35]

On European Union level, one of the applicable legal instrument on which this thesis will emphasis is the GDPR, which entered into force in 2016 and became applicable on the 25th of May 2018[36]. The Regulation laid the groundwork for the most powerful and significant change in terms of data protection in the last 20 years. The GDPR provides to data subjects preferences over how their data is accessed and processed and requires data subjects'authorisation before any data alteration is done to their (personal) data..[37] On European Union level there are also other legal instruments which safeguards personal data, such as the ePrivacy Directive,[38] and the Directive on Processing of Personal Data for Law Enforcement Purposes.[39] The former directive[40] encompasses the processing of

[31] Vulnerability Registration Service, *"Data, Vulnerability & GDPR: Considerations for Businesses",* accessed on 22.08.2023 https://www.vulnerabilityregistrationservice.co.uk/data-protection-gdpr-and-vulnerability/

[32] General Data Protection Regulation, Article 6(1) (f), Article 8, Article 12, Recital 75.

[33] Piasecki, S., & Chen, J. (2022). Complying with the GDPR when vulnerable people use smart devices. *International Data Privacy Law*, *12*(2), 113-131, p.117.

[34] Dimitra and Lambrinoudakis, "*Compatibility of a security with the EU)"*, 586 (n'9)

[35] Luna, Florencia. "Elucidating the concept of vulnerability: Layers not labels." IJFAB: International Journal of Feminist Approaches to Bioethics 2, no. 1 (2009): 121-139.

[36] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, Article 99 (1).

[37] Barati, Masoud, Omer Rana, Ioan Petri, and George Theodorakopoulos. "GDPR compliance verification in Internet of Things." *IEEE access* 8 (2020): 119697-119709, p. 1.

[38] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).

[39] Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data.

[40] ePrivacy Directive, Article 1 (1).

personal "*data in the electronic communication sector*"[41], and the latter one[42] emphasises on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of preventing, investigating, discovering, or carrying out criminal offences or the imposition of criminal penalties, including preventing and securing against threats to public security.[43] Despite the above-mentioned information, it is crucial to mention that the European Union has its roots in the idea of a common market, providing four freedoms,[44] different national data protection laws- or the lack of them would conflict with these freedoms. Therefore, the GDPR has twin objectives, which are stated under Article 1(1) of the Regulation. On the one hand, the GDPR protects personal data as a fundamental right. On the other hand, the GDPR recognizes the EU's internal market interests in the free flow of such data. One of the fundamental concepts of data protection legislation is personal data, which established the substantive idea of the Regulation. According to Article 2(1) of the GDPR[45], the data protection rights obligation, and principles only apply when personal data is processed. Based on the wording of the GDPR, Article 4(1), personal data is considered as "*any information relating to an identified or identifiable person ('data subject') …*".[46] Regardless of where the data processing activities take place, the GDPR applies to all organisations, both inside and outside the EU, that process the personal data of EU data subjects.[47]

However, the GDPR is still roughly based on the structure and content of the Data Protection Directive, which was drafted well before the '*IoT age'*. Therefore, a question arises whether data protection rules on the EU level are comprehensive enough to satisfy the safeguarding of vulnerable data subjects in relation to personal data processed by IoT wearable devices for healthcare purposes. Moreover, considering that the information from wearables is uploaded to a cloud, there is an inherent risk that it could be jeopardized or misused by an unauthorized user.

2. Problem statement

According to Ryan Calo, *"the more vulnerable a person is, the less privacy"*[48] the data subject tends to enjoy. Moreover, he indicates that the lack of privacy shall be seen as a portal to greater

[41] ePrivacy Directive, Article 1 (1).
[42] Directive on Processing of Personal Data for Law Enforcement Purposes, Article 1 (1).
[43] ICO. Information Commissioner's Office, "When do we need to do a DPIA?" https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/data-protection-impact-assessments-dpias/ , accessed on 22.08.2023.
[44] Namely: the free movement of goods, capital, people, and services.
[45] General Data Protection Regulation, Article 2(1).
[46] General Data Protection Regulation, Article 4(1).
[47] General Data Protrction Regulation, Article 3.
[48] Calo, Ryan. "Privacy, vulnerability, and affordance." *DePaul L. Rev.* 66 (2016): 591, p.1.

vulnerability and exploitation.[49] The thesis's aim is to inspect whether the development of wearable Internet of Things (IoT) devices for healthcare purposes represents a substantial challenge to data protection law, which is written without the wearables in mind, with respect to the level of protection afforded to[50] vulnerable data subjects. As the IoT ecosystem continues to expand, wearable devices have enlarged their scope, offering individuals seamless integration of technology in various fields. However, the distribution of wearable IoT devices raises concerns regarding the privacy and security of vulnerable data subjects.[51] Given the above, it will be examined whether the development of wearable IoT[52] devices for health purposes (with an emphasis on fitness trackers), represents a substantial challenge[53] to the protection of vulnerable data subjects.

The rapid growth of wearable IoT devices, such as health monitoring equipment, is resulting in the collection of sensitive data on a massive scale. Such devices are designed to collect and transmit data such as biometric information, hearth rate, health condition, that could give insights into data subjects' lives.[54] Despite offering potential benefits in areas such as healthcare, fitness tracking, etc., by their pervasive nature, these wearables pose some significant issues in terms of protection of vulnerable data subjects who may be particularly susceptible to privacy infringements, security breaches, or discriminatory practices.

To understand the potential challenges associated with fitness trackers and the protection of vulnerable data subjects, a comprehensive analysis of the potential security risks (e.g., unauthorized access, data breach, identity theft, misused or exploited data, lack of awareness) and privacy challenges, such as third-part risks, consent and the collection of sensitive data, and the adequacy of existing legal frameworks and technical principles has to be conducted. Additionally, this thesis aims to identify the specific vulnerabilities faced by different categories of data subjects, including individuals with potential health conditions who rely on IoT devices for health purposes, or children who may lack the capacity to fully comprehend the implications of their data being collected and processed.

[49] Calo, "Privacy, vulnerability, and affordance." (n'1).

[50] COMMISSION IMPLEMENTING REGULATION (EU) 2021/1772 of 28 June 2021 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by the United Kingdom.

[51] Chacko, Anil, and Thaier Hayajneh. "Security and privacy issues with IoT in healthcare." *EAI Endorsed Transactions on Pervasive Health and Technology* 4, no. 14 (2018).

[52] Rolf H.Weber, 'Internet of Things- New security and privacy challenges' (2010) 26 Computer Law & Security Review 23

[53] Rolf H Weber, 'Internet of Things – Need for a New Legal Environment?' (2009) 25 Computer Law & Security Review 522

[54] Psychoula, Ismini, Liming Chen, and Oliver Amft. "Privacy risk awareness in wearables and the internet of things." *IEEE Pervasive Computing* 19, no. 3 (2020): 60-66.

The findings of this thesis will provide insight into the addressed challenges. They will conclude whether the development of wearable Internet of Things (IoT) devices in the healthcare system represents a substantial challenge to data protection law, which is written without the wearables in mind, concerning the level of protection afforded to vulnerable data subjects.

3. Research question and sub-questions

The central research question of this thesis is: "*Do the rules and principles under the General Data Protection Regulation aimed at protecting vulnerable data subjects sufficiently perform their task when applied to personal data processing by IoT wearable devices for health purposes*?".

To address the research question effectively, the following sub-questions will be examined:

1. What are wearable IoT devices? This sub-question aims to comprehensively understanding wearable IoT devices, their characteristics, functionalities, and the types of personal data they collect. By exploring their features, capabilities, architecture, and ecosystem, it will be possible to assess the potential risks and implications for data subjects, especially the vulnerable ones.

2. Who are vulnerable data subjects and how does the GDPR deal with vulnerability? This sub-question focuses on examining the vulnerability as a concept, and to situate the vulnerability in the EU data protection framework. Here, the analysis will involve relevant articles, literature, and articles addressing vulnerable data subjects' rights and principles.

3. Can the provisions of the GDPR be interpreted in terms of wearables IoT to protect vulnerable data subjects? This sub-question aims to evaluate the effectiveness of the provisions under the GDPR in protecting vulnerable data subjects in the context of wearable IoT devices.

4. Literature review

This chapter presents a comprehensive review of the existing literature related to this thesis's main research question and sub-questions. It explores scholarly articles, academic papers, etc. to gain insights into the effectiveness of the rules and principles under the GDPR in protecting vulnerable data subjects in the context of personal data processing by IoT wearables.

By conducting research scholars have concluded that wearable devices collect personal and/or sensitive data daily.[55] These data constitute blood pressure, heart rate, and blood sugar levels in patients suffering from diseases such as diabetes, etc. An interesting part of the IoT devices is their

[55] Vidhi, Singh, Reddy, and Churi. "Privacy issues in wearable technology" 2020.

architecture[56] and how they evolved during the decades, which will be discussed later on in the thesis.[57] Another intriguing topic that will be discussed in the thesis is the IoT ecosystem. More precisely, what are the data protection roles (e.g., the data subject, controller, processor) vis-à-vis the stakeholders of the IoT ecosystem (e.g., manufacturer, third party).[58] Furthermore, these devices tend to lack satisfactory privacy and data protection measures due to their nature. Based on that, numerous security and data protection threats[59] may occur relevant for vulnerable data subjects, while using the IoT devices. Furthermore, the IoT differs from traditional computing, by its complex nature and billions of sensors embedded in common in order to operate.[60] Experts in research ethics have established that some participants have stronger chances than others of being mistreated, abused, exploited, or harmed.[61] This group of participants is called the vulnerable data subjects. When a controller collects and processes personal data, the data subjects whose data is processed are exposed to risks.[62] Therefore, it would be more difficult for the group of vulnerable data subjects to track if unauthorized person got access to their data.

Many researchers outline how the use of data-driven technology may result in social exclusion or prejudice.[63] Calo believes that the privacy protection rationale addresses individuals' vulnerability. According to Malgieri and Jedrzej, there is tension between particularistic and universalistic approaches regarding vulnerability in data protection and privacy. Based on the "*universalistic approach, privacy and data protection*"[64] shall protect all human beings equivalently,[65] due to the fact everyone is equally exposed to violations. Unfortunately, this is not the case, since every data subject has a different level of understanding and awareness.[66] Therefore, here the issue is raised regarding the protection of vulnerable data subjects and whether the principles of the EU would be satisfactory enough to protect them. Therefore, this paper will be used to situate vulnerable data subjects through the prism of the data protection field, and more precisely the General Data Protection Regulation.

[56] Ikrissi, Ghizlane, and Tomader Mazri. "IOT-BASED SMART ENVIRONMENTS: STATE OF THE ART, SECURITY THREATS AND SOLUTIONS." *ISPRS Annals of Photogrammetry, Remote Sensing & Spatial Information Sciences* (2021).

[57] Alshohoumi, Sarrab, AlHamadani, and Al-Abri, "Systematic review of existing IoT architectures " (n'234).

[58] Hadzovic, Suada, Sasa Mrdovic, and Milutin Radonjic. "Identification of IoT actors." *Sensors* 21, no. 6 (2021): 2093.

[59] Mohamed and Køien. "Cyber security and the internet of things" 65-88, p. 74.

[60] Article 29 Data Protection Working Party. (2014). Opinion 8/2014 on the Recent Developments on the Internet of Things.

[61] Malgieri and Niklas, "Vulnerable data subjects." (n'2)

[62] Data protection Commission (2019). Guidance Note: Guide to Data Protection Impact Assessments (DPIAs).

[63] Malgieri and Niklas, "Vulnerable data subjects." (n'3).

[64] Malgieri and Niklas, "Vulnerable data subjects." (n'4).

[65] Malgieri and Niklas, "Vulnerable data subjects." (n'4).

[66] Malgieri and Niklas, "Vulnerable data subjects." (n'5).

The argument of Malgieri and Niklas is in line with the one of Martha Fineman, by stating that vulnerability should be considered universal and constant.[67] The thesis delves into the relevant articles of the GDPR, analyzing their intent and scope, and with the support of the relevant sources, which discuss the importance of the GDPR's principles (lawfulness, fairness, transparency, etc.) it will be examined the GDPR's recognition of vulnerable data subjects.

Nevertheless, some authors take another approach. One of them is Luna who suggests a theory of layered vulnerabilities.[68] Based on her theory, the author claims that vulnerability is a universal condition, but it does not exclude the approach that there are conditions that differ from one individual to another, by creating different degrees of vulnerability, *which in fact will be the approach pursued in the thesis*. By collecting all the relevant information from the articles, the main research question[69] will be answered, providing arguments supported by more literature.[70] Authors argue that the rules and principles embedded in the GDPR[71] are strong enough to serve as safeguards[72] for vulnerable data subjects. However, at the end of the thesis, it will be clear if these principles are still applicable and effective[73] in the world of wearable IoT devices.

5. Methodology

To conduct this thesis, I will use legal research. More precisely, relying on a hermeneutic discipline,[74] which emphasis is on texts and documents and their interpretation, according to standard methods. The backbone of this research will be based on primary sources, mainly the General Data Protection Regulation.[75] I narrowed down the scope of this research to the European level, because

[67] Fineman, Martha Albertson. "The vulnerable subject: Anchoring equality in the human condition." In *Transcending the boundaries of law*, pp. 177-191. Routledge-Cavendish, 2010, p.1.

[68] Luna, "Elucidating the concept of vulnerability", 121-139.

[69] Livingstone, Sonia. "Children: a special case for privacy?." *Intermedia* 46, no. 2 (2018): 18-23.

[70] Crepax, Tommaso, Victor Muntés-Mulero, Jabier Martinez, and Alejandra Ruiz. "Information technologies exposing children to privacy risks: domains and children-specific technical controls." *Computer Standards & Interfaces* 82 (2022): 103624.

[71] General Data Protection Regulation, Article 8(1).

[72] The principles are as follows: lawfulness, fairness and transparency, purpose limitation, data minimization, accuracy storage limitation, integrity and confidentiality and accountability

[73] Krivokapic, Dorde, and Jelena Adamovic. "Impact of General Data Protection Regulation on children's rights in digital environment." *Annals Fac. L. Belgrade Int'l Ed.* (2016): 205.

[74] Van Hoecke, Mark. "Legal doctrine: Which method (s) for what kind of discipline?." In *Methodologies of legal research: which kind of method for what kind of discipline?*, pp. 1-18. Hart Publishing, 2011.

[75] Outside the scope of the General Data Protection Regulation (GDPR), there are other aspects of vulnerability addressed within the EU data protection framework. However, as well as the GDPR, the ePrivacy directive does not explicitly define vulnerability, but it contains provisions that aim at protecting data subjects 'privacy and address some vulnerabilities in the context of electronic communications. Another provision is the Directive on Processing of Personal Data for Law Enforcement Purposes, which again does not indicate a unified definition of vulnerability, but it contains provisions that recognize the importance of protecting the rights and interests of data subjects, including those who may be vulnerable in the context of law enforcement activities.

Europe provides strict rules in terms of data protection, accounts privacy, and data protection as fundamental rights. In addition to the hermeneutic discipline, a doctrine can be used. A doctrine includes legal concepts and principles of cases, statutes, and rules. Moreover, this thesis will also focus on secondary research, which will constitute papers written by scholars, mainly on wearable devices, and data protection rules.

6. Chapters overview

After this introduction, the second chapter of the thesis will introduce the reader to wearable IoT devices, their architecture, and their roles in that ecosystem. Furthermore, it will explain the security and privacy threats that might affect vulnerable data subjects, while using these devices.

The third chapter will serve as an explanation of the term vulnerability, and what is considered a vulnerable data subject in the scope of the GDPR, and in the EU data protection framework. Furthermore, the reader will be introduced to what norms these vulnerable data subjects have under the laws of the legal scope of the GDPR.

Chapter four will denote whether these norms are enough to serve as safeguards for vulnerable data subjects if wearables are in breach of their rights. If necessary, based on the whole research, recommendations will be made. Finally, chapter 5 will serve as a conclusion. It is important to note that other legal frameworks besides GDPR will be mentioned throughout the research as part of the EU data protection framework. However, the emphasis will be on the GDPR, since it is primary legislation that sets the overarching framework for data protection within the EU.

Chapter 2 - What are IoT devices and the challenges they pose for data subjects?

2.1 Chapter overview

This chapter introduces the reader to the wearable Internet of Things (IoT) devices, IoT wearable devices for health purposes, their architecture, different layers, how they differ from the traditional computing system, and the data protection roles in the IoT ecosystem. In addition, the chapter will introduce the reader to some the challenges that the wearables IoT may pose to vulnerable data subjects. The term vulnerable data subject will be discussed and explained in details in Chapter 3. However, since the Chapter 2 refers to it throughout the chapter, it is worth it to mention that vulnerable data subjects are often defined as data subjects at higher risks that may be restricted from their capacity to freely consent or object to or comprehend the implications of the use of their personal data.[76]

2.2 What are wearables Internet of Things (IoT) devices?

A brand-new era of the Internet of Things has been ignited by the popularity of smart devices[77] in combination with concepts like cloud computing and Big Data,[78] offering a "*strong framework for the networking of smart devices, including wearable sensors and smartphones, through cloud computing*".[79] "*The International Telecommunication Union (ITU) defines*"[80] the Internet of Things (IoT) as the worldwide infrastructure that permits cutting-edge services to connect objects based on interoperable information and communication technologies.[81] Another definition, suggested by Mohd Muntjir, Mohd Rahul, and Hesham A. Alhumyani, identifies the Internet of Things as a network of electronic devices with Internet access, including smartphones and tablets, as well as almost anything with a sensor, such as cars, machinery in manufacturing facilities, jet engines, oil drills, wearable

[76] ICO. Information Commissioner's Office, "When do we need to do a DPIA?" https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/data-protection-impact-assessments-dpias/ , accessed on 22.08.2023.
[77] Ioannidou and Sklavos, "On General Data Protection Regulation Vulnerabilities and Privacy Issues " (n'5).
[78] Ioannidou and Sklavos, "On General Data Protection Regulation Vulnerabilities and Privacy Issues " (n'5).
[79] Ioannidou and Sklavos, "On General Data Protection Regulation Vulnerabilities and Privacy Issues " (n'5).
[80] Zivkovic, Carna, Yajuan Guan, and Christoph Grimm. "IoT Platforms, Use Cases, Privacy, and Business Models." (2021).
[81]Biggs, Philippa, John Garrity, Connie LaSalle, and Anna Polomska. "Harnessing the Internet of Things for global development." (2016) ,p.10.

technology and more,[82] (smart glasses, smartwatch, fitness trackers, virtual reality headsets, smart clothing, medical wearables, smart jewelry, smart homes).[83] Some of these wearable IoT devices enable the monitoring of human aspects, such as health, wellbeing, behaviors, and other data, on between electronic devices and sensors through the internet in order to facilitate everyday life.[84]

The Article 29 Data Protection Working Party's Opinion on wearable computing states that the IoT devices make it possible for third parties to create applications and thus access to the personal data of individuals collected by these devices.[85] Therefore, an issue might be at stake since some of these third parties might be intruders that aim at accessing and collecting personal data for malicious purposes. The WP29 continues by discussing another type of IoT device which is classified as quantified self. In the context of IoT, the quantified self involves the use of interconnected devices equipped with sensors and software to gather and monitor data about an individual's activities, biometrics, and behaviours. The aim of quantified self-devices is to enable data subjects who are interested in tracking information about their own routines and lifestyles to do so.[86] For instance, someone may wish to wear a sleep monitor constantly to have a comprehensive understanding of their sleeping habits.[87] As another example, it could be indicated by the reports which include the physical activity of the data subject such as calories burned, or the distance walked by using tracking movements. In addition, these IoT devices may measure either pulse, weight or be used for indicating other health indicators. Quantified Self raises some challenges due to the types of health-related data collected, which may be sensitive, as well as the large amount of data acquired.[88]

Indeed, wearables find their application in many parts of everyday life. For instance, in healthcare, where the wearable IoT allows healthcare providers to monitor patient's health conditions in cases such as chronic disease management, elderly care, etc.[89] Furthermore, wearable IoT devices' application can also be found in sports, where through fitness tracking a person may monitor their

[82] Muntjir, Mohd, Mohd Rahul, and Hesham A. Alhumyani. "An analysis of Internet of Things (IoT): novel architectures, modern applications, security aspects and future scope with latest case studies." *Int. J. Eng. Res. Technol* 6, no. 6 (2017): 422-447, p.422.

[83] Jin, Chun Yu. "A review of AI Technologies for Wearable Devices." In *IOP Conference Series: Materials Science and Engineering*, vol. 688, no. 4, p. 044072. IOP Publishing, 2019, p. 2.

[84] Chun Yu, "A review of AI Technologies for Wearable Devices", (n'1).

[85] Article 29 Data Protection Working Party. "Opinion 8/2014 on the Recent Developments on the Internet of Things." (2014), p.5

[86] WP29. "Opinion 8/2014" (n'5).

[87] WP29. "Opinion 8/2014" (n'5).

[88] WP29. "Opinion 8/2014" (n'17).

[89] Banerjee, Syagnik, Thomas Hemphill, and Phil Longstreet. "Wearable devices and healthcare: Data sharing and privacy." *The Information Society* 34, no. 1 (2018): 49-57, p. 50

performance, based on real-time data.[90] In addition, these *"things"* collect and exchange data, involving the use of data storage, processing, and acquisition technologies for embedded systems.[91] actually raise security and data privacy concerns for the vulnerable data subjects using them. For instance, if personal data is exposed to threats and if this data is stolen or processed for the wrong purposes (e.g., selling information to third parties), this may jeopardize the well-being of these vulnerable data subjects.

The concept of the IoT and traditional computing systems differs. Compared to the traditional computing system, the Internet of Things (IoT) is an infrastructure that enables billions of sensors embedded in common *'things".*[92] Here lies one of the main differences- the scope. The IoT encompasses all these sensors as *"things",* allowing them to collect, exchange and analyse data, whereas the traditional computing system involves desktops, laptops, and servers.[93] Architecture is another fundamental difference between the two systems. The traditional computing one usually follows a centralized architecture, where processing and data storage occurs on a single device or a network of connected device.[94] In contrast, the form of the IoT system is a distributed computing, that enables the user to access data from a remote server than a computer. One more crucial differentiation between the two concepts is connectivity. On one hand, IoT systems leverage wireless connectivity technologies, such as WI-FI, Bluetooth, or cellular networks, allowing devices to communicate with each other and the internet. On the other hand, traditional computing systems often rely on wired connecting (for instance cables) or local area networks for communication.[95]

Wearable IoT devices are an integral part of the larger IoT ecosystem, which is characterized by interconnected devices that communicate and interact with each other. There are some features that describe how wearable IoT fits into the ecosystem: first and foremost, through connectivity.[96] Since wearable IoT devices are equipped with wireless connectivity capabilities (e.g., Bluetooth, cellular), these wearables can establish connections with other IoT devices (e.g., smartphones, tablets),

[90] Chun Yu, A review of AI Technologies for Wearable Devices, (n'2)

[91] Ioannidou and Sklavos. "On General Data Protection Regulation Vulnerabilities and Privacy Issues " (n'5).

[92] WP29. "Opinion 8/2014" (n'4).

[93] Simplilearn. "Cloud Computing vs Traditional Computing", https://www.simplilearn.com/cloud-computing-vs-traditional-computing-article#:~:text=services%20and%20storage.-,What%20is%20Traditional%20Computing%3F,to%20manage%20and%20maintain%20them

[94] Simplilearn. "Cloud Computing vs Traditional Computing", https://www.simplilearn.com/cloud-computing-vs-traditional-computing-article#:~:text=services%20and%20storage.-,What%20is%20Traditional%20Computing%3F,to%20manage%20and%20maintain%20them

[95] Simplilearn. "Cloud Computing vs Traditional Computing", https://www.simplilearn.com/cloud-computing-vs-traditional-computing-article#:~:text=services%20and%20storage.-,What%20is%20Traditional%20Computing%3F,to%20manage%20and%20maintain%20them

[96] Poongodi, T., Anu Rathee, R. Indrakumari, and P. Suresh. "IoT sensing capabilities: Sensor deployment and node discovery, wearable sensors, wireless body area network (WBAN), data acquisition." *Principles of internet of things (IoT) ecosystem: Insight paradigm* (2020): p. 144.

which enables this connectivity to exchange data seamlessly, and allows interaction within the IoT ecosystem. The second feature is data collection.[97] Being embedded with sensors, wearable IoT devices capture data such as biometric data, environmental data, location, etc. In that manner the collection of data is efficient. The next feature derives from the fact that wearable IoT devices can transmit the collected data to other devices or platforms within the IoT ecosystem. For instance, a smartwatch that collects biometric data (e.g., heartrate) can share that data with a smartphone app, which in turn, can sync the data to a cloud-based health management platform. Another fundamental feature of the ecosystem itself is interoperability, and wearables are designed to seamlessly interact with other IoT devices and services.[98] This interoperability guarantees that data from wearables can be utilized by other devices, applications, or systems for enhanced functionality and insights.

2.3 What are IoT wearable devices for healthcare purposes?

A specific type of IoT devices, that falls under its scope are the IoT wearable devices for healthcare purposes, designed to monitor and collect various health-related data from data subjects.[99] These devices are equipped with sensors, processors, and communication capabilities, allowing them to gather information about the data subject's physical activity, vital signs, and other health metrics.[100] The collected data is then typically transmitted to a smartphone, computer, or cloud-based platform for analysis and further insights.[101] IoT wearable devices for health purposes offer users the convenience of real-time health monitoring and can assist in promoting healthier lifestyles, managing medical conditions, and providing healthcare professionals with valuable information These include devices that track real-time health information or devices that continuously monitor health indicators.[102] The following paragraph discusses some common examples of IoT wearable devices for health purposes.

[97] Poongodi, Rathee, Indrakumari, and Suresh, *Principles of internet of things (IoT) ecosystem: Insight paradigm* (n'129).

[98] Ometov, Aleksandr, Viktoriia Shubina, Lucie Klus, Justyna Skibińska, Salwa Saafi, Pavel Pascacio, Laura Flueratoru et al. "A survey on wearable technology: History, state-of-the-art and current challenges." *Computer Networks* 193 (2021): 108074.

[99] Li, Wei, Yuanbo Chai, Fazlullah Khan, Syed Rooh Ullah Jan, Sahil Verma, Varun G. Menon, fnm Kavita, and Xingwang Li. "A comprehensive survey on machine learning-based big data analytics for IoT-enabled smart healthcare system." *Mobile networks and applications* 26 (2021): 234-252.

[100] Al-Khafajiy, Mohammed, Thar Baker, Carl Chalmers, Muhammad Asim, Hoshang Kolivand, Muhammad Fahim, and Atif Waraich. "Remote health monitoring of elderly through wearable sensors." *Multimedia Tools and Applications* 78, no. 17 (2019): 24681-24706.

[101] Ko, JeongGil, Chenyang Lu, Mani B. Srivastava, John A. Stankovic, Andreas Terzis, and Matt Welsh. "Wireless sensor networks for healthcare." *Proceedings of the IEEE* 98, no. 11 (2010): 1947-1960.

[102] Dimitrov, Dimiter V. "Medical internet of things and big data in healthcare." *Healthcare informatics research* 22, no. 3 (2016): 156-163.

Wearable fitness trackers are one example.[103] Here would be worth to briefly distinguish wellness and healthcare IoT devices, by still keeping fitness trackers as part of the devices for healthcare purposes. Basically, wellness wearable IoT devices have their focus primarily on tracking general lifetime metrics (e.g., steps taken, calories burned, sleep patterns), in order to promote overall well-being.[104] Whereas IoT wearable devices for healthcare purposes tend to monitor numerous health metrics such as heart rate, blood pressure, blood glucose levels, by syncing the data to smartphones and/or computers in order to analyse and provide health insights.[105] Additionally, fitness trackers often offer more accurate health data measurements, compared to general wellness devices. Therefore, fitness tackers fall under the scope of IoT for health purposes, since they do collect health-related data, which can provide valuable insights for health monitoring, management, and potential medical interventions. Furthermore, fitness trackers may be compatible with healthcare platforms, enabling data sharing with medical professionals for diagnosis and treatment. In fact, wellness and healthcare IoT device overlap to some extent. For instance, in terms of the common data collection, where both types of devices can gather heart rate, steps taken, etc. However, while wellness IoT devices emphasizes on general lifestyle tracking, some of the collected data can also have health implications. Another intersection point is the dual-purpose of the devices. For example, some IoT devices may serve both wellness and health purposes, by monitoring heart rate during exercise which could also be used to track resting heart rate, providing insights into cardiovascular health.

Another example of such IoT devices are remote patient monitoring devices,[106] such as ECG patches, glucose monitors, and blood pressure monitors, enabling healthcare facilities to observe the health conditions of their patients in real-time, without the need for a patient to be present in the moment of monitoring.[107] Health and wellness monitors also fall under the scope of IoT devices for health purposes. These devices are designed to monitor specific health parameters, such as oxygen saturation ad body temperature.[108] Smart health scales are another variety. These scales may evaluate not just weight but other parameters related to body composition, including age, muscular mass, and body fat. Furthermore, the data can be stored and tracked over time to monitor progress. Sleep monitors for instance, are designed for sleep tracking and monitoring sleep patterns, quality and duration,

[103] Haghi, Mostafa, Kerstin Thurow, and Regina Stoll. "Wearable devices in medical internet of things: scientific research and commercially available devices." *Healthcare informatics research* 23, no. 1 (2017): 4-15.
[104] Wickramasinghe, Nilmini, and Freimut Bodendorf, eds. *Delivering superior health and wellness management with IoT and analytics*. Springer Nature, 2019.
[105] Kaiser, Daniel W., Robert A. Harrington, and Mintu P. Turakhia. "Wearable fitness trackers and heart disease." *JAMA cardiology* 1, no. 2 (2016): 239-239.
[106] Ibid.
[107] Ibid.
[108] Mittelstadt, Brent. "Designing the health-related internet of things: ethical principles and guidelines." *Information* 8, no. 3 (2017): 77.

facilitating data subjects to improve their sleep habits.[109] Last but not least, biofeedback devices are the last one mentioned in the section. These devices provide real-time feedback on physiological processes, helping data subjects manage stress, anxiety, and other emotional states.[110]

IoT wearable devices for health purposes offer the potential to enhance personal health, management, enable remote patient monitoring, and contribute to medical research. However, addressing data privacy and security concerns associated with these devices is essential to protect sensitive health information and ensure compliance with data protection regulations.

The next section of the chapter will introduce the reader to the IoT architecture, and the security threats for data subjects.

2.4 IoT Architecture and the security threats for (vulnerable) data subjects, posed by IoT devices for health purposes

The idea of connecting devices together has been around since the 1980s.[111] Since then, the architecture of the IoT has been evolving. This section of the chapter will introduce the reader briefly to the architecture of the IoT from the period of 2008[112] until 2020.[113] Furthermore, this section aims at discussing the potential threats which the IoT architecture conceals regarding vulnerable data subjects and the different roles in the IoT ecosystem.

2.4.1 IoT Architecture

Alshoumi pointed out "*sixteen different IoT architectures*"[114] that were established throughout the period from 2008 to 2020.[115] Based on the findings of the study, it has been claimed that the IoT architecture extends from a "*three-layer architecture model to the eight-layer model*".[116] The

[109] Kelly, Jessica M., Robert E. Strecker, and Matt T. Bianchi. "Recent developments in home sleep-monitoring devices." *International Scholarly Research Notices* 2012 (2012).
[110] Yu, Bin, Mathias Funk, Jun Hu, Qi Wang, and Loe Feijs. "Biofeedback for everyday stress management: A systematic review." *Frontiers in ICT* 5 (2018): 23.
[111]Alshohoumi, Sarrab, AlHamadani, and Al-Abri, "Systematic review of existing IoT architectures " (n'234).
[112] This is the exact chosen year, because in 2008 the first IoT architecture was presented, source Alshohoumi, Fatma, Mohammed Sarrab, Abdulla AlHamadani, and Dawood Al-Abri. "Systematic review of existing IoT architectures security and privacy issues and concerns." *International Journal of Advanced Computer Science and Applications* 10, no. 7 (2019).
[113] According to the source, the next evolutionary year in which the IoT devices will develop again is in 2025. Therefore, the IoT architecture will be examined until 2020, source Ibid.
[114] Hadzovic, Suada, Sasa Mrdovic, and Milutin Radonjic. "Identification of IoT actors." *Sensors* 21, no. 6 (2021): 2093, p. 2.
[115] Hadzovic, Mrdovic, and Radonjic. "Identification of IoT actors." (n'2).
[116] Hadzovic, Mrdovic, and Radonjic. "Identification of IoT actors." (n'2).

three-layer model [117] consisted of (1) a physical layer [118](2) a network layer [119] and (3) an application layer.[120] The latter (eight-layer) model extended with the following layers:(1) a communication layer,[121] (2) an edge (fog) computing layer,[122] (3) a data storage layer,[123] (4) a collaboration and processes layer,[124] and (5) a security level.[125] Some IoT architectures, such as those published in 2008 and 2010, are relatively generic and just briefly describe the IoT layers. In contrast, architectures proposed after 2010 provide more specific information on each layer.[126] However, it became evident by comparing all these architectures that the early models, which were put forth at the beginning of IoT development, have several drawbacks. For instance, the IoT design was suggested in 2008 and did not consider the processing and storage in their tiers.

The earlier IoT design, in which the storage and processing layers were presented, received greater detail with the architecture that was proposed in 2010.[127] The architectures that were put forth after 2010 depicted the IoT in its entirety, beginning with the data collection layer and moving through the network layer, processing layer, and application layer. Prior to 2011, none of the IoT architectures took security into account. According to estimates, there were 12.5 billion Internet of Things (IoT) devices in use in 2010, which led to more people being concerned about security threats to the IoT.[128] As a result, the IoT design proposed in 2011 began to take security into account in IoT levels. It included security methods that can aid in lowering network dangers that could result from unauthorized users' access. The proposed IoT architectures between 2014 and 2015[129] took scalability and interoperability difficulties into account. The integration of cloud computing with IoT architecture offers a solution to the scalability issue in IoT. Since 2016, academics have focused increasingly on

[117] Kotha, Harika Devi, and V. Mnssvkr Gupta. "IoT application: a survey." *Int. J. Eng. Technol* 7, no. 2.7 (2018): 891-896, p. 892.

[118] Also called as perception layer, containing sensors, RGID tags and other essential components. THis layer senses and collect the necessary information from the connected devices.

[119] Acts as a getaway, taking care of routing protocols, server related infromation and transmission of data. On this layer data is transferred via logical network paths.

[120] The top layer is accountable for forwarding the data to the required destination.

[121] Consisting of two sub-layers. (1) Direct Device to Device (D2D) Communication sub-layer, which possesses and produces its own identity and personality, and (2) Connectivity sub-layer, on which level, devices are connected to communication centers, transmitting and processing data via the storage unit's Internet connection through the data centers.

[122] In order to make decisions at this level, nodes process the data at the edge.

[123] Contains data storage units that store both raw data and information that has been collected via edge processing of the physical devices. Additionally, responsive to future applications' massive data volume and traffic

[124] To make IoT usable, people must be able to cooperate and communicate through the use of this layer.

[125] It protects and covers the layers before it, however, the sections on this level have their own functionality. Data encryption, user authentication, network access control, and cloud security are just a few of the security elements included in that layer.

[126]Alshohoumi, Sarrab, AlHamadani, and Al-Abri, "Systematic review of existing IoT architectures" (n'244).

[127] Fremantle, P. "A reference architecture for the internet of things,‖ vol. 0." (2015): 21.

[128] Alshohoumi, Sarrab, AlHamadani and Al-Abri. “Systematic review of existing IoT architectures security and privacy issues and concerns."

[129] Alshohoumi, Sarrab, AlHamadani, and Al-Abri, "Systematic review of existing IoT architectures " (n'241).

IoT security concerns.[130] Some more recent architectures presented in 2017 include additional specifics regarding the threats and requirements, as well as how to cope with such threats. During this time, all the security concerns and issues in each IoT layer were discussed.[131] As seen in recently proposed architectures for 2018, scalability in IoT was addressed using a variety of technologies, including block chain, 5G, and cloud-based micro services.[132] Finally, in 2020 some of the IoT architecture overlaps with the one in 2018. However, in 2020, as the number of devices increased, so did the concern for security and privacy, and IoT architecture shifted the focus more on implementing security measures (such as encryption, authentication, and access control), in order to protect data from potential cyber threats.[133]

2.4.2 Different roles in the IoT ecosystem

In the IoT ecosystem, various roles play vital functions to design, develop, implement, and operate IoT devices and systems. Each role contributes to the successful deployment and utilization of IoT technology. Therefore, some of the key roles in the IoT ecosystem will be briefly introduced to the reader. One of the stakeholders in the IoT ecosystem is the device manufacturers, which are responsible for designing, manufacturing, and producing these devices.[134] These companies are accountable for developing hardware components, embedded sensors, and creating devices with connectivity features enabling data collection and transmission. Another stakeholder is the IoT platform providers, which offer cloud-based platforms and services that facilitate data storage, processing, and analytics for IoT devices.[135] These providers allow seamless integration and management of data from multiple IoT devices. Additionally, network providers are also part of the stakeholders in the IoT ecosystem. Network providers offer connectivity infrastructure, such as cellular networks, and Wi-Fi, to enable communication between IoT devices and back-end systems. Regulators and standard organizations[136] hold another significant role in the IoT ecosystem, They develop and enforce guidelines and regulations related to IoT technology, as well as ensure compliance with data protection,

[130] Alshohoumi, Sarrab, AlHamadani, and Al-Abri, "Systematic review of existing IoT architectures" (n’242).

[131] Alshohoumi, Sarrab, AlHamadani, and Al-Abri, "Systematic review of existing IoT architectures" (n’242).

[132] Alshohoumi, Sarrab, AlHamadani, and Al-Abri, "Systematic review of existing IoT architectures" (n’243).

[133] Hadzovic, Suada, Sasa Mrdovic, and Milutin Radonjic. "Identification of IoT actors." *Sensors* 21, no. 6 (2021): 2093, p. 2.

[134] Schladofsky, Werner, Jelena Mitic, Alfred Paul Megner, Claudia Simonato, Luca Gioppo, Dimitris Leonardos, and Arne Bröring. "Business models for interoperable IoT ecosystems." In *Interoperability and Open-Source Solutions for the Internet of Things: Second International Workshop, InterOSS-IoT 2016, Held in Conjunction with IoT 2016, Stuttgart, Germany, November 7, 2016, Invited Papers 2*, pp. 91-106. Springer International Publishing, 2017.

[135] Schmid, Stefan, Arne Bröring, Denis Kramer, Sebastian Käbisch, Achille Zappa, Martin Lorenz, Yong Wang, Andreas Rausch, and Luca Gioppo. "An architecture for interoperable IoT ecosystems." In *Interoperability and Open-Source Solutions for the Internet of Things: Second International Workshop, InterOSS-IoT 2016, Held in Conjunction with IoT 2016, Stuttgart, Germany, November 7, 2016, Invited Papers 2*, pp. 39-55. Springer International Publishing, 2017.

[136] King, Andrew A., and Michael J. Lenox. "Industry self-regulation without sanctions: The chemical industry's responsible care program." *Academy of management journal* 43, no. 4 (2000): 698-716.

safety, and interoperability standards. The next crucial role is of the data analysts, which analyze the collected data from IoT devices to derive insights and make data-driven decisions.[137] End-users[138] occupy another key role in the IoT system. They utilize IoT devices and systems for specific purposes. In the upcoming chapter, the reader will be introduced to the same roles, but in the context of data protection law, analyzing them from a legal perspective.

2.4.3 Security threats

The IoT poses a number of security difficulties because device manufacturers must balance battery efficiency and device security due to resource and security restrictions.[139] It is yet unclear how manufactures will balance and optimise how objects and sensors consume computer resources (and energy) while implementing confidentiality, integrity, and availability metrics at every stage of the processing flow.[140] Therefore, there is a posibility that the IoT will transform everyday objects into potential targets for privacy and information security, spreading these targets much more widely than the current version of the Internet.[141] Insecure connected devices represent potentially efficient new attack[142] vectors, such as facilitating surveillance practices and data breaches that lead to the theft and breach of personal data, as well as personal awareness of vulnerable data subjects[143]' rights and IoT security.

Since the emphasis of the thesis is on IoT wearable devices for health purposes, security threats will be discussed in their respect, more particularly to fitness trackers. For instance, vulnerable data subjects might not be aware of the importance of updating firmware[144] and software[145] on their fitness trackers, because if outdated, a device could have unpatched security vulnerabilities that attackers could exploit. This may lead to unauthorized access, which may lead to potential misuses or

[137] Yu, Bin, Jarod Wright, Surya Nepal, Liming Zhu, Joseph Liu, and Rajiv Ranjan. "Iotchain: Establishing trust in the internet of things ecosystem using blockchain." *IEEE Cloud Computing* 5, no. 4 (2018): 12-23.
[138] Individuals or organizations
[139] Article Data Protection Working Party. 'Opinion 8/204 on the Recent Developments on the Internet of Things'. *European Commission* (2014), p.3
[140] Article Data Protection Working Party. 'Opinion 8/204 on the Recent Developments on the Internet of Things'. *European Commission* (2014), p.3
[141] Article Data Protection Working Party. 'Opinion 8/204 on the Recent Developments on the Internet of Things'. *European Commission* (2014), p.3.
[142] Article Data Protection Working Party. 'Opinion 8/204 on the Recent Developments on the Internet of Things'. *European Commission* (2014), p.3.
[143] Vulnerable data subject:
[144] Firmware refers to the embedded software that is permanently programmed into a hardware device, such as a fitness tracker. It provides instructions for the hardware to perform specific tasks and functions. Firmware is stored in non-volatile memory and remains on the device even when it's powered off. Fitness trackers rely on firmware to operate their sensors, collect data, display information, and communicate with other devices.
[145] Software in the context of fitness trackers refers to the applications, programs, and interfaces that run on the device or are used to interact with it. This includes the mobile apps that sync with the fitness tracker, display data, and provide user controls. Software also includes the algorithms that process raw data from the sensors to calculate metrics like steps taken, heart rate, calories burned, and sleep patterns.

tampering with sensitive health data.[146] Another security threat which vulnerable data subject may experience is data breaches,[147] since they may not have the capacity or knowledge to detect or report data breaches promptly, leading to exposure of their personal health information. Additionally, identity theft is also frequent security threat, regarding IoT wearable devices for health purposes.[148] Vulnerable data subjects may be at higher risk of such theft, if their personal health data (e.g., medical details, medical records), is compromised through the device. Another issue arises when data subjects' personal health data can be misused or exploited by malicious actors for various purposes, such as fraud, harassment, or discrimination.[149] Hackers will take advantage, due to the limited capacity of these data subjects, to deceive them into disclosing sensitive data or compromising their IoT devices. Furthermore, lack of awareness about data security practices can leave vulnerable data subjects more vulnerable to unintentionally exposing sensitive health information. Additionally, vulnerable data subject might be more targeted to attacks that manipulate the functionality of IoT devices, leading to inaccurate health readings. Finally, wearable IoT devices for health purposes used by vulnerable data subjects may be more prone to security vulnerabilities, as they may lack robust security features or have outdated firmware.[150]

Deriving from the discussion in the previous section, IoT devices for health purposes collect and transmit sensitive personal data, such as health information or location data. Thus, if these devices are not properly secured, they can be exposed to data breaches, leading to unauthorized access and exposure of personal information. Additionally, wearable IoT devices rely on wireless communication to transmit data. Without adequate security measures, attackers can intercept and capture data packets, potentially gaining access to sensitive information, potentially leading to data interception. Physical access to wearable IoT devices can allow attackers to tamper with the device's firmware or hardware components. Furthermore, data subjects may be unaware of the security risks associated with wearable IoT devices. They may inadvertently share sensitive information or fail to follow best practices for securing their devices, making them more susceptible to security threats. The thesis will address those threats under the GDPR framework in the upcoming chapters.

[146] Sametinger, Johannes, Jerzy Rozenblit, Roman Lysecky, and Peter Ott. "Security challenges for medical devices." *Communications of the ACM* 58, no. 4 (2015): 74-82, p.74.
[147] Moganedi, Sophia. "Undetectable data breach in iot: Healthcare data at risk." In *17th European Conference on Cyber Warfare and Security*, vol. 2, p. 296. 2018.
[148] Ibid.
[149] Ibid.
[150] Sametinger, Rozenblit, Lysecky and Ott. "Security challenges for medical devices (n'80).

2.5. Privacy challenges related to the IoT devices for health purposes (fitness trackers)

At the beginning of the chapter, the reader was presented with the idea that the IoT poses not only security but also challenges to the privacy of the data subject. Respectively, by this part of the chapter, the reader will be introduced to some of these challenges. Here again, the data protection and privacy challenges will be discussed in terms of fitness trackers.

2.5.1 Third-party risks

One type of risk that is often neglected is the fact that outside applications are usually given access to data subjects data. In order for a third party application to obtain authorization to access, for instance for Fitbit data subject data, the consent of the data subject is necessary.[151] Fitness trackers enable data subjects to specify what they want to record (e.g., weight, the number of steps, heart rate, and when they sleep). This stored information is clear to the data subjects, however, further information about the data subjects is accumulated from the trackers,[152] which data subjects might be unware of. For instance, their location, saturation, when they wake up and when they go to bed.[153] The Symantec specialists claim that it is simple for unauthorised third parties to modify the majority of fitness trackers into monitoring tools.[154] Additionally, a study done between an activity tracker and an online web server exposes weaknesses that might endanger data subjects.[155] An experiment conducted on one the most famous fitness trackers, Fitbit, researchers found that data subjects can grand access to third party apps to access data prom theor devices including metadata which is unknown to the data subjects using the application.[156] In fact, these third parties have access and they can manipulate the personal data of the data subjects.

2.5.2 Consent and inadequate consent management

Vulnerable data subjects, such as data subjects with cognitive impairments or mental disorders, may face challenges in providing informed consent for the use of IoT wearable devices for healthcare purposes. Their limited understanding of the technology and its applications could lead to

[151] Orlosky, Jason, Onyeka Ezenwoye, Heather Yates, and Gina Besenyi. "A look at the security and privacy of Fitbit as a health activity tracker." In *Proceedings of the 2019 ACM Southeast Conference*, pp. 241-244. 2019.

[152] Dini Kounoudes, Alexia, Georgia M. Kapitsaki, and Ioannis Katakis. "Enhancing user awareness on inferences obtained from fitness trackers data." *User Modeling and User-Adapted Interaction* (2023): 1-48.

[153] Dini Kounoudes, Alexia, Georgia M. Kapitsaki, and Ioannis Katakis. "Enhancing user awareness on inferences obtained from fitness trackers data." *User Modeling and User-Adapted Interaction* (2023): 1-48.

[154] Pingo, Zablon, and Bhuva Narayan. "Users’ responses to privacy issues with the connected information ecologies created by fitness trackers." In *Maturity and Innovation in Digital Libraries: 20th International Conference on Asia-Pacific Digital Libraries, ICADL 2018, Hamilton, New Zealand, November 19-22, 2018, Proceedings 20*, pp. 240-255. Springer International Publishing, 2018.

[155] Dobreva, Milena, Annika Hinze, and M. Zumer. "Maturity and Innovation in Digital Libraries." (2018).

[156] Torre, Ilaria, Odnan Ref Sanchez, Frosina Koceva, and Giovanni Adorni. "Supporting users to take informed decisions on privacy settings of personal devices." *Personal and Ubiquitous Computing* 22 (2018): 345-364.

consent-related issues. Furthermore, this type of data subject may experience difficulties in managing their consent preferences for data sharing or revoking consent if necessary. Ensuring clear and accessible consent management processes is vital to respect their privacy choices and provided them with control over their health information. Therefore, ensuring that consent is obtained clearly and understandably becomes crucial to protect their data protection rights.[157]

2.5.3 Sensitive health data

IoT wearable devices for health purposes collect sensitive health data (e.g., heart rate, sleep patterns, or medication schedule). This data is highly personal and requires strong safeguards to prevent unauthorized access or misuse, as it can reveal sensitive information about a vulnerable data subject health condition. Consequently, this may lead to security breaches and unauthorized access to vulnerable data subjects' personal and sensitive data. Their limited ability to understand and manage security settings or detect malicious activities increases the potential for exploitation by malicious actors, leading to privacy breaches and potential harm. Furthermore, the data collected by wearable IoT devices can be used for profiling purposes, possibly leading to discrimination against vulnerable data subjects. Profiling based on health or behavior patterns could result in adverse decisions related to insurance, employment, even there is a strong potential for actual physical harm (e.g., third-party messing with another individual's implanted pacemaker).

In the upcoming chapters, having these data protection and privacy challenges related to the IoT in mind, the thesis will resolve the issue if the rules and principles under the General Data Protection Regulation aimed at protecting vulnerable data subjects perform their task when applied to personal data processing by wearables.

2.6 Conclusion

In conclusion, this chapter introduced wearable Internet of Things (IoT) devices, IoT devices for health purposes, their architecture, and the security and privacy threats they pose to vulnerable data subjects. The chapter also highlighted the differences between wearable IoT devices and traditional computing systems.

Luna's theory of vulnerability is intertwined with the essence of the chapter. Her approach provides a framework that enables comprehending how certain data subjects are more exposed to risks and challenges by IoT devices for health purposes, due to factors beyond their control. In the context of IoT devices for health purposes, this vulnerability perspective clears up some potential

[157] Article 29 Data Protection Working Party. (2014). Opinion 8/2014 on the Recent Developments on the Internet of Things.

threats faced by data subjects that may lack technical knowledge, cognitive abilities, or awareness of the intricate data protection and security landscape. Additionally, the chapter set the stage for further exploration of the GDPR effectiveness in protecting vulnerable data subject when applied to personal data processing by IoT devices. Understanding and addressing these challenges are crucial to ensure that wearables continue to provide valuable services, without compromising the privacy and security of their users, especially the vulnerable data subjects.

Chapter 3 - Who are vulnerable data subjects and how does the GDPR deal with vulnerability?

3.1. Chapter overview

Experts in research ethics have long believed that some individuals are more likely than others to experience mistreatment, abuse, exploitation, or damage.[158] Such groups tend to have a higher level of vulnerability.[159] The concept of vulnerability is present in numerous fields of life, and is well-known subject of discussion in the sphere of data protection. However, one specific group of data subjects requires more attention and careful observation, the group of vulnerable data subjects. A variety of EU legislative instruments recognize their existence, and aim at providing safeguards towards data subjects's part of such groups.[160] This chapter introduces the reader to the concept of vulnerable data subjects. Furthermore, the third chapter will discuss the GDPR norms that are relevant for vulnerable data subjects.

3.2. What is a vulnerable data subject?

Vulnerability is considered as a concept with many layers. For instance, Malgieri and Niklas[161] have analysed what is the role[162] and the potential consequences of the notion of vulnerable data subjects.[163] The authors took an approach by claiming that vulnerability can be viewed[164] either as universal[165] (everyone is "*equally vulnerable*"),[166]or "*particular*"[167] ("*some individuals are more vulnerable than others*").[168] Other authors, such as Martha Fineman, argued that vulnerability shall be understood by society as universal and constant, inherent in the human condition.[169]

Other authors, such as Luna, take another approach to defining vulnerability and who can be considered as a vulnerable data subject, by suggesting a theory of layered vulnerability.[170] The pur-

[158] Malgieri and Niklas. "Vulnerable data subjects" (n'2).
[159] Malgieri and Niklas. "Vulnerable data subjects" (n'2).
[160] Waddington, Lisa. "Exploring vulnerability in EU law: An analysis of "vulnerability" in EU criminal law and consumer protection law"." *European Law Review* 45, no. 6 (2020): 779-801.
[161] Piasecki Tadeusz, Stanislav "Complying with the GDPR When Vulnerable People Use Smart Devices", p.18.
[162] Piasecki, "Complying with the GDPR When Vulnerable People Use Smart Devices" (n'18).
[163] Piasecki, "Complying with the GDPR When Vulnerable People Use Smart Devices" (n'18).
[164] Piasecki, "Complying with the GDPR When Vulnerable People Use Smart Devices" (n'18).
[165] Piasecki, "Complying with the GDPR When Vulnerable People Use Smart Devices" (n'18).
[166] Piasecki, "Complying with the GDPR When Vulnerable People Use Smart Devices" (n'18).
[167] Piasecki, "Complying with the GDPR When Vulnerable People Use Smart Devices" (n'18).
[168] Piasecki, "Complying with the GDPR When Vulnerable People Use Smart Devices" (n'18).
[169] Fineman, "The vulnerable subject" (n'1).
[170] Luna, " Layers not label." 121-139.

pose Luna's research was to address various concerns by implementing new perspectives of vulnerability as layers.[171] Layers of vulnerability, in her opinion, are not perceived as permanent characteristics of certain people or groups. They do, however, have characteristics that are based on place, time, and status. In this way, the idea of layering emphasizes its potential for accumulation and ephemerality while opening the door to a more intersectional approach.[172] As Luna points out, indeed, vulnerability is a universal condition of human beings,[173] but this does not preclude the possibility that different data subjects may experience these weaknesses in varying degrees of severity and due to a variety of other causes.[174] In other words, according to Luna's hypothesis, everyone is vulnerable, but some people have more vulnerability layers than others,[175] which is the approach followed in the thesis. Additionally, Luna's vulnerability approach, in the context of IoT wearable devices for health purposes, identifies multiple layers of vulnerability that data subjects may experience regarding data protection and security issues. Her approach indicates how different factors can impact a data subjects' vulnerability to such challenges. In the following paragraph, the thesis will emphasize on some of the layers of vulnerability in the context of IoT wearable devices, and why some groups of data subjects might be more vulnerable than others.

One example could be the technological vulnerability, where data subjects, by using wearable IoT devices are susceptible to technological vulnerabilities, such as data breaches, hacking, etc. In that context, however, data subjects with limiting understanding of technology, such as elderly data subjects or the ones with low digital literacy, are at higher risk, due to their reduced ability to navigate and respond to technical challenges. Since wearable devices collect physiological data, they make all data subjects physically vulnerable to potential misuse or even exposure of health-related information. Here again, we have more vulnerable data subjects than others, due to the fact that data subjects with pre-existing health condition may have sensitive health data, which if compromised, may lead to significant consequences for their well-being. Another layer of vulnerability in the context of wearable IoT devices is the cognitive vulnerability, which complexity of data collection, processing, and sharing can pose cognitive challenges to any data subject.

Further aggregating the problem, those with cognitive impairments or limited understanding of data privacy may face some challenges in comprehending the implications of using wearable devices and the risks associated with sharing their health data. Furthermore, data privacy and security

[171] Luna, " Layers not label." 121-139.
[172] Malgieri and Niklas. "Vulnerable data subjects" (n'4).
[173] Malgieri and Niklas. "Vulnerable data subjects" (n'4).
[174] Malgieri and Niklas. "Vulnerable data subjects" (n'4).
[175] Piasecki, "Complying with the GDPR When Vulnerable People Use Smart Devices" (n'18).

concerns can evoke emotional stress in any data subject using wearable devices. Thus, the ones already experiencing emotional distress, such as patients managing chronic illness, might be more affected by the emotional toll of potential breaches or misuse of their data. The societal vulnerability should not be disregarded as well, since the broader societal context, including regulations and norms, impacts on everyone's vulnerability. Therefore, disadvantaged data subjects may face additional societal vulnerability due to disparities in access to healthcare, legal protection, or technological resources. Nevertheless, they might also be less informed about their rights and protections. Last but not least, adhering to data protection regulations affects every data subject using wearable devices. Therefore, the ones unaware of their legal rights or lack the means to advocate for themselves might face legal and regulatory vulnerabilities when using wearable IoT devices.

3.3. Vulnerability under the GDPR

Even though under the GDPR, vulnerable data subjects are not explicitly defined as a distinct category, the Regulation recognizes the need for specific protection for certain data subjects, due to their particular vulnerabilities and the sensitivity of their personal data involved.[176] Overall, the Regulations' recognition of the need for specific protection for certain data subjects is grounded in the desire to strike a balance between enabling data processing for legitimate purposes and safeguarding data subjects' privacy and rights, especially those who may be more vulnerable in the digital age.[177]

Data subjects are not a homogenous group of individuals, and it is possible to make distinctions with respect to their position and status under data protection law.[178] Quelle indicates that the approach suggested by Luna is in conformity with the GDPR's risk-based approach, as formulated e.g. by Articles 25(1) and Article 24 of the Regulation.[179] This approach embodies the notion that vulnerability exists for everyone, albeit in varying degrees and situation.[180] The GDPR emphasizes the protection of all data subjects' personal data but indicates additional provisions to safeguards the right of specific groups**.** For instance, explicit consent is required in certain situations when processing personal data of vulnerable data subjects. The processing of health information or information

[176] Bugeja, Joseph, Désirée Jönsson, and Andreas Jacobsson. "An investigation of vulnerabilities in smart connected cameras." In *2018 IEEE international conference on pervasive computing and communications workshops (PerCom workshops)*, pp. 537-542. IEEE, 2018.

[177] Livingstone, Sonia, and Amanda Third. "Children and young people's rights in the digital age: An emerging agenda." *New media & society* 19, no. 5 (2017): 657-670.

[178] Blume, Peter. "The data subject." *Eur. Data Prot. L. Rev.* 1 (2015): 258, p. 259.

[179] Quelle, Claudia. "Enhancing compliance under the general data protection regulation: the risky upshot of the accountability-and risk-based approach." *European Journal of Risk Regulation* 9, no. 3 (2018): 502-526.

[180] Piasecki, "Complying with the GDPR When Vulnerable People Use Smart Devices" (n'18).

pertaining to criminal convictions are two examples of such circumstances.[181] In such cases, consent must be given explicitly and unambiguously, leaving no room for doubt or misinterpretation.[182] Another GDPR provision that protects the personal data of vulnerable data subject is the parental consent for children, under Article 8(1) of the Regulation.[183] When a child is under the age of 16 (or lower, determined by individual EU MS), under the GDPR the parental consent is necessary. Thus, service providers must use reasonable are obliged to make reasonable diligence to confirm that parental or guardian authorization for consent has been obtained.[184] Another additional provision under the GDPR is the Data Protection Impact Assessment (DPIAs),[185] under which when processing personal data that may lead to higher risks to the right and freedoms of vulnerable data subjects, data controllers are required to conduct DPIA.[186] The next vital additional provision imposed by the Regulation is data protection by design and default.[187] This principle requires data controllers to incorporate data protection and privacy measures into the design of their processing activities. For instance, this entails applying organizational and technical safeguards that protect be default the personal information of data subjects who are vulnerable. Furthermore, the GDPR identifies certain categories of data (sensitive) which deserves enhanced protection, due to the highly sensitive data it carries. If distributed or used for malicious purposes, it may affect seriously data subject’s life.[188] These data include heath data, biometric data, generic data and data related to criminal conviction.

The GDPR applies another approach to defining vulnerability. For instance, there are cases where someone cannot be characterized immediately as a vulnerable data subject. However, in the framework of the GDPR, a power imbalance in the relationship of a vulnerable data subject with another person may give rise to vulnerable situations. Employees who may be considered weak in situations of power imbalance and find it challenging to express opposition to their employer’s use of their personal information is an example of a such scenario.[189] Power imbalance means that a data

[181] Seyyar, M. Bas, and Zeno JMH Geradts. "Privacy impact assessment in large-scale digital forensic investigations." *Forensic Science International: Digital Investigation* 33 (2020): 200906, p.4

[182] General Data Protection Regulation, Article 4(11).

[183] General Data Protection Regulation, Article 8 (1).

[184] Panasonic, Privacy Policy, https://www.tvpa.panasonic.com/voice/policies/privacy?region=eea , accessed on 22.08.2023.

[185] General Data Protection Regulation, Article 35.

[186] DPIAs are systematic assessments of the potential impact of data processing activities on data subjects’ privacy and rights. They help identify and mitigate risks before processing begins.

[187] General Data Protection Regulation, Article 25(2).

[188] General Data Protection Regulation, Article 9(1).

[189] Party, Data Protection Working. "Guidelines on data protection impact assessment (DPIA) and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679 (WP29). Artic. 29 Data Prot. Work. Party. WP 248 rev 22 (2017)." (2017).

subject may experience difficulties to consent easily, or to object to, or exercise their rights with respect to the processing of their data.[190]

Furthermore, WP29 considers power imbalance as the key factor in identifying individual vulnerability, by providing guidelines on Data Protection Impact Assessment (DPIA). These guidelines indicate that vulnerable data subjects may include children, due to the fact that they are deemed incapable of deliberately and thoughtfully objecting to or giving their consent to the processing of their data.[191] Under the scope of vulnerability, requiring special safeguards, also fall employees, mentally ill people, asylum seekers, or elderly patients.[192] WP29 indicates that the link between power imbalance and vulnerability is clear. The WP29 affirms that when the data controllers are in a position of power imbalance[193] towards the data subjects, the data subjects should be considered as vulnerable. Even though the GDPR does not have a specific article stating who shall be considered as vulnerable data subject under its scope, the next sections of the chapter will provide an overview of certain categories of data subjects, that are considered as vulnerable ones under the GDPR.

3.3.1 Children

In terms of the safeguarding of natural people, concerning the processing of personal data,[194] the Regulation serves as a legal instrument, under which children are recognized as a vulnerable data subject group. The GDPR introduces specific provisions to ensure that the personal data of children is given extra protection. This is due to their potential lack of awareness, understanding, and capacity to provide informed consent in relation to data processing activities serving as a legal instrument concerning the safeguarding of natural people in terms of the processing of personal data. Children are considered a vulnerable group due to their limited understanding and implicit incapability to make informed opinions regarding their personal data. The GDPR recognizes this and provides specific protections for children's personal data. The Regulation introduces the conception of the" *age of consent,"* where the processing of personal data of children under the age of 16 (or a lower age if Member States determine) requires maternal or guardian consent.[195] Organizations must take special care when collecting and processing children's' personal data, ensuring that it's done in a transparent and age-applicable manner, and considering the child's best interests.

[190] Malgieri and Niklas. "Vulnerable data subjects", (n'6).

[191] Art 29 Working party, "Guidelines on Data Protection Impact Assessment (DPIA) (n'9).

[192] Art 29 Working party, "Guidelines on Data Protection Impact Assessment (DPIA) '(n9).

[193] Malgieri and Niklas. "Vulnerable data subjects", (n'6).

[194] And rules relating to the free movement of that data: GDPR, art 1(1).

[195] General Data Protection Regulation, Article 40 (2) (g)

3.3.2 Sensitive data and patients

When dealing with vulnerable data subjects, the approach of the GDPR towards vulnerability is particular, and not universal.[196] In other words, only children are explicitly mentioned as vulnerable.[197] However, in the above-mentioned sections it was discussed that children are not the only group with great risk, but also groups such as elderly, mentally ill, or hospitalized data subjects, may experience similar risks. Patients are often in vulnerable situations due to their physical or mental health conditions. The GDPR acknowledges the sensitive nature of personal health data and mandates stronger protections for its processing. It requires explicit consent from patients for the processing of their health data and imposes strict security measures to safeguard its confidentiality and integrity. Generally, the processing of sensitive personal data requires more safeguards, and under Article 9 the GDPR refers to it as *"special categories of personal data"*.[198] Another legal framework which mentions and regulates data protection is Convention 108.[199] Here again, the sensitive data is defined as "*special category of data"*. Therefore, personal data is considered as sensitive, when it is more presumably to influence the fundamental rights and freedoms of a data subject.[200] That type of data may reveal particularly delicate information about data subjects, in terms of racial or ethnic origin, political opinions, religious or philosophical beliefs, biometric data, data concerning health, or sexual orientation.

An example of a field in which a data subject may fall under the category of the vulnerable data subject through the leakage of sensitive data is the field of healthcare systems. Due to its sensitive nature, the Regulation recognizes the need for enhanced protection of this type of data. Processing such data requires a higher level of safeguards to ensure privacy and security. These principles will be introduced and explained in the next chapter, where it will be concluded if they are sufficient enough to fulfil their purpose in terms of wearable IoT devices for health purposes on EU level.

3.3.3 Employees, elderly data subjects and data subjects with disabilities

In the context of employment, employees can also fall under the scope of vulnerability, due to the power imbalance between employers and employees.[201] The GDPR recognizes that employees may face potential risks and disadvantages if their personal data is mishandled. It places obligations

[196] Malgieri and Niklas. "Vulnerable data subjects", (n'6).
[197] Malgieri and Niklas. "Vulnerable data subjects", (n'6).
[198] Georgiou and Lambrinoudakis. "Compatibility of a security policy." 586, p.2.
[199] Convention for the protection of individuals with regard to automatic processing of personal data [1981] ETS No. 108 (CM/Inf(2018)15-final).
[200] Mulder, Trix, and Melania Tudorica. "Privacy policies, cross-border health data and the GDPR." *Information & Communications Technology Law* 28, no. 3 (2019): 261-274, p. 264.
[201] Art 29 Working party, "Guidelines on Data Protection Impact Assessment (DPIA) '(n9).

on employers to ensure the fair and lawful processing of employee data, including providing clear information about data processing activities, respecting the principles of purpose limitation and data minimization, and implementing appropriate security measures to protect employee data.[202]

Elderly individuals may be deemed vulnerable due to factors such as potential cognitive or physical impairments that can affect their ability to understand and make informed decisions regarding their personal data.[203] They may require additional support to ensure their data protection rights are respected. Organizations processing personal data of elderly individuals should consider their unique circumstances and provide accessible information and user-friendly mechanisms to exercise their rights. Practically, elderly individuals are not specifically given extra protection under EU privacy legislation. Despite explicitly acknowledging children as a vulnerable group of data subjects,[204] the GDPR does not, exclude recognizing older data subject as in need of extra protection.[205] This indicates one more time that the Regulation supports the vulnerability theory of Luna, in which data subjects may find themselves in a vulnerable position, and may need extra protection, even if they are not explicitly mentioned under the GDPR.

People with disabilities may face challenges in understanding and exercising their data protection rights, particularly if the processing involves complex technical or legal concepts. The GDPR acknowledges that certain disabilities may impact an individual's ability to provide informed consent or exercise control over their personal data.[206] Organizations should adopt measures to ensure accessibility, such as providing clear and easy-to-understand privacy notices, offering alternative formats for information, and accommodating specific needs when obtaining consent or responding to data subject requests.

3.4 Conclusion

In conclusion, vulnerable data subjects are recognized and addressed within the General Data Protection Regulation (GDPR). While the GDPR does not specifically define vulnerable data subjects as a distinct category, it acknowledges the need for specific protections for certain groups of individuals.[207] Vulnerability is viewed from different perspectives, including the universal vulnerability of

[202] General Data Protection Regulation, Art 88 (1).

[203] Malgieri and Niklas. "Vulnerable data subjects".

[204] General Data Protection Regultion, Art 8.

[205] Tupasela, Aaro, Juanita Devis Clavijo, Marjut Salokannel, and Christoph Fink. "Older people and the smart city: Developing inclusive practices to protect and serve a vulnerable population." *Internet policy review* 12, no. 1 (2023): 1-21, p. 9.

[206] General Data Protection Regulation, Article 7(1).

[207] General Data Protection Regulation, Recital 75, the only provision where vulnerability was explicitly mentioned.

all individuals and the notion of layered vulnerability, where some individuals possess more vulnerability layers than others.

The GDPR's risk-based approach recognizes that vulnerability can exist at various levels and in different contexts.[208] The approach puts an emphasis on the fundamentality of transparency in communication with data subjects, ensuring that information is provided in an intelligible and accessible form. Children are explicitly recognized as a vulnerable group under the GDPR, given their limited understanding and potential inability to make informed decisions regarding their personal data.[209] Special protections are in place for the processing of children's personal data, including the requirement for parental or guardian consent. Patients (e.g. those receiving medical treatment or participating in clinical trials) are often in vulnerable situations due to their health conditions. The GDPR acknowledges the sensitive nature of personal health data and imposes stricter principles for its processing.[210] Explicit consent is required, as well as strong security measures are put in place, to protect the confidentiality and integrity of this sensitive information. Due to the power imbalance that exists between employers and employees, the latter might be viewed as being vulnerable in their place of employment.[211] Elderly individuals and people with disabilities may also be deemed vulnerable due to factors that can affect their understanding and decision-making regarding their personal data.[212] Additional support and accommodations should be provided to ensure their data protection rights are respected.

While the GDPR provides a framework for addressing vulnerability, further guidance and measures may be necessary to fully protect vulnerable data subjects. It is essential for organizations to consider the unique circumstances and needs of these individuals, provide accessible information and mechanisms for exercising their rights, and implement appropriate principles to protect their personal data.

[208] General Data Protection Regulation, Articles 25(1) and Article 24.

[209] General Data Protection Regulation, Article 12, Recital 58.

[210] General Data Protection Regulation, Article 9.

[211] Aloisi, Antonio, and Elena Gramano. "Artificial intelligence is watching you at work: Digital surveillance, employee monitoring, and regulatory issues in the EU context." *Comp. Lab. L. & Pol'y J.* 41 (2019): 95.

[212] Malgieri and Niklas. "Vulnerable data subjects".

Chapter 4 - Can the provisions of the GDPR be interpreted with reference to IoT devices for healthcare purposes to protect vulnerable data subjects?

4.1 Chapter overview

Chapter 2 introduced the roles in the IoT ecosystem, and the following chapter's focus shifted towards understanding these roles in the context of the General Data Protection Regulation (GDPR) and its legal analysis. This chapter explores the legal responsibilities of IoT stakeholders – manufacturers, third-party software providers, and data subjects – under the GDPR, focuses on the alignment of the GDPR's data protection principles with healthcare IoT data processing, and examines how fitness trackers approach vulnerability of data subjects. The approaches include informed consent, transparency, user control, and data security measures. However, challenges arise due to varying cognitive capacity, technical complexity, and power imbalances faced by vulnerable data subjects. Finally, the chapter addresses vulnerability using GDPR provisions, and if these provisions and rules sufficiently safeguard vulnerable data subjects, IoT devices for health purposes do data processing.

4.2 The IoT roles: legal analysis

In chapter 2 the reader was introduced to the different roles in the IoT ecosystem. Here, the reader will be introduced to the same roles, but in respect to the GDPR, by providing legal analysis. The Article 29 Data Protection Working Party adopted a specific Opinion, emphasizing that IoT stakeholders (such as manufacturer or third party software provider) are responsible for making sure that the data is used for purposes that the data subjects are aware of and that are fully consistent with the original purpose of the processing at every level.[213] It is crucial that the stakeholders involved are accurately identified. Since the IoT stakeholders must establish their legal status as data controllers and adhere to various requirements, this is a significant part of the processing .[214]

Data controllers, defined by Art. 4(7) of the Regulation must apply the necessary technological and organizational safeguards to secure personal data[215] throughout the IoT ecosystem. Per definition, the controller is an body which either "*alone or jointly with others*"[216] identifies the objectives

[213] Hadzovic, Mrdovic, and Radonjic. "Identification of IoT actors." (n'15).
[214] Hadzovic, Mrdovic, and Radonjic. "Identification of IoT actors" (n'15).
[215] Tikk, Eneken. "Privacy online: up, close and personal." *Health and Technology* 7, no. 4 (2017): 489-499.
[216] Paola, Iamiceli, Cafaggi Fabrizio, and CHIARA SILVIA Angiolini. "Casebook Effective Data Protection and Fundamental Rights." (2022), p. 78.

and means of personal data processing.[217] Furthermore, the controller must inform supervisory authority in the case of breach or misuse of data, by preventing transfers to insecure processors. In the context of wearable IoT devices for healthcare purposes, the care providers (such as hospital and clinics) are considered as controllers, as they establish the objective of the processing (e.g., monitoring patient's heart rate).[218]

Within the IoT context, the GDPR also imposes specific obligations on data processors. Respectively, data processors are defined by the Regulation under Art. 4(8),[219] as a *"natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller."*[220] A data processor must adhere to strict contractual requirements and maintain a high level of security[221] and confidentiality, as well as to have an agreement in writing, and after the services are concluded, to delete the data.[222] In the world of IoT devices for healthcare purposes, a processor could be a cloud service provider, which establishes the connection between the patient home and the healthcare provider.[223]

The other data protection role is the data subject one. Under Article 4(1)[224] of the Regulation, *"data subject is an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person*".[225] In the context of IoT devices, this could be an individual using a connected device (e.g., smartwatch, fitness tracker). The term 'data subject' refers to a person who may be directly or indirectly[226] identified.[227] Data subjects have rights

[217] Lynskey, Orla. "Grappling with "data power": normative nudges from data protection and privacy." *Theoretical Inquiries in Law* 20, no. 1 (2019): 189-220, p.203.

[218] Lindstad, Sarita, and Kaspar Rosager Ludvigsen. "When is the processing of data from medical implants lawful? The legal grounds for processing health-related personal data from ICT implantable medical devices for treatment purposes under EU data protection law." (2022): 1-36, p. 8.

[219] General Data Protection Regulation, Article 4(8).

[220] Zekos, Georgios I. "Digital Politics, GDPR, and AI." In *Political, Economic and Legal Effects of Artificial Intelligence: Governance, Digital Economy and Society*, pp. 473-511. Cham: Springer International Publishing, 2022.

[221] Voigt, Paul, and Axel Von dem Bussche. "The eu general data protection regulation (gdpr)." *A Practical Guide, 1st Ed., Cham: Springer International Publishing* 10, no. 3152676 (2017): 10-5555.

[222] Hon, W. Kuan, Christopher Millard, and Ian Walden. "Negotiating cloud contracts: Looking at clouds from both sides now." *Stan. Tech. L. Rev.* 16 (2012): 79, p. 104.

[223] Lindstad and Ludvigsen. "When is the processing of data from medical implants lawful? " (n'8).

[224] General Data Protection Regulation, Article 4(1).

[225] McMahon, Aisling, Alena Buyx, and Barbara Prainsack. "Big data governance needs more collective responsibility: the role of harm mitigation in the governance of data use in medicine and beyond." *Medical law review* 28, no. 1 (2020): 155-182, p.177.

[226] Georgiou, Dimitra, and Costas Lambrinoudakis. "Compatibility of a security policy for a cloud-based healthcare system with the EU general data protection regulation (GDPR)." *Information* 11, no. 12 (2020): 586, p. 2.

[227] Ibid.

including consent, access data, knowledge of where the data are, how in fact were that data processed, communicated, and the right to request erasure of that data.[228]

One example of an IoT stakeholder is the manufacturer, which is responsible for ensuring data protection.[229] Manufacturers are liable for embedding privacy and security features into the devices. In the IoT ecosystem, manufacturers are sometimes considered controllers (as well as joint controllers),[230] thus they may have some additional obligations, such as providing clear privacy notices and obtaining consent where required. On this subject, A29WP stated its opinion, by clarifying that joint controllership does not have to be equally distributed among the parties, but they may distribute and determine the obligations and the responsibilities amongst themselves.[231] However, overall compliance with the data protection obligations must be assured.[232]

Another stakeholder in the IoT ecosystem is the third-party provider, usually responsible for developing applications or services that run on IoT devices.[233] Compared to the manufacturer, the third-party provider acts as a processor, by processing data on behalf of the controller. These stakeholders shall have adequate and appropriate data protection measures and comply with the instructions provided by the controller.

4.3 How do the data quality principles of the GDPR align with IoT devices for health purposes data processing?

The data quality principles[234] outlined in the GDPR are vital in order to guarantee that personal data is protected.[235] When applied to the data processing by IoT devices for health purposes, these principles aim to establish a balance between the benefits derived from the devices and the privacy rights of vulnerable data subjects.[236] The data privacy rights of data subjects include: right to

[228] Koops, Bert-Jaap. "The trouble with European data protection law." *International data privacy law* 4, no. 4 (2014): 250-261.
[229] Khan, Atta Ur Rehman, and Raja Wasim Ahmad. "A blockchain-based IoT-enabled E-Waste tracking and tracing system for smart cities." *IEEE Access* 10 (2022): 86256-86269, p. 3.
[230] Hadzovic, Suada, Sasa Mrdovic, and Milutin Radonjic. "Identification of IoT actors." *Sensors* 21, no. 6 (2021): 2093.
[231] A29WP's Opinion 1/2010 (WP 169), 19.
[232] A29WP's Opinion 1/2010 (WP 169), p. 19.
[233] Mazhelis, Oleksiy, Eetu Luoma, and Henna Warma. "Defining an internet-of-things ecosystem." In *Conference on Internet of Things and Smart Spaces*, pp. 1-14. Berlin, Heidelberg: Springer Berlin Heidelberg, 2012.
[234] Principles: lawfulness, fairness and transparency, purpose limitation, data minimization, accuracy storage limitation, integrity and confidentiality and accountability
[235] Lachaud, Eric. "What could be the contribution of certification to data protection regulation?." PhD diss., Tilburg University, 2019.
[236] Bell, Jessica, Stergios Aidinlis, Hannah Smith, Miranda Mourby, Heather Gowans, Susan E. Wallace, and Jane Kaye. "Balancing data subjects' rights and public interest research." *Eur. Data Prot. L. Rev.* 5 (2019): 43.

information and transparency[237], right to access,[238] right to erasure (right to be forgotten),[239] right to data portability,[240] right to object,[241] right to restriction of processing,[242] and right to non-discrimination.[243]

The first principle, transparency, requires that data subjects have clear and accessible information about how their personal data is collected process and used.[244] Art29WP also indicates that transparency is about engendering trust in the process which affect the data subjects by enabling them to understand, and if necessary, challenge those process.[245]. In the context of IoT devices for health purposes, this principle requires that data subjects are informed about the processing of their data in a transparent manner.[246] This includes providing privacy notices or disclosures that explain the purposes of data processing, the legal basis for processing, the categories of personal data collected, the retention periods, and the rights of the data subjects. Article 12 of the GDPR[247] is one of the articles addressing the right to transparent information, ensuring that individuals have access to clear and intelligible information on how their personal data is processed. In accordance with Articles 13 and 14 of the GDPR, data subjects have the right to be notified in cases in which their personal information was either directly or indirectly gathered from them.[248]

Next, we have purpose limitation as the other principles which indicates that personal data[249] should be *"collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes…".*[250] "*Purpose limitation*"[251] is necessary when using IoT devices for health-related objectives since it stipulates that information obtained through wearables can only be utilised for those purposes for which it was initially obtained. Any further processing of the data must be compatible with the initial purposes and be based on a valid legal

[237] General Data Protection Regulation, Article 12.
[238] General Data Protection Regulation, Article 15.
[239] General Data Protection Regulation, Article 17.
[240] General Data Protection Regulation, Article 20.
[241] General Data Protection Regulation, Article 21.
[242] General Data Protection Regulation, Article 23.
[243] General Data Protection Regulation, Article 22.
[244] Article 5 (1) (a), GDPR.
[245] Milkaite, Ingrida, and Eva Lievens. "Child-friendly transparency of data processing in the EU: from legal requirements to platform policies." *Journal of Children and Media* 14, no. 1 (2020): 5-2, p. 8.
[246] Mulder, Trix, and Melania Tudorica. "Privacy policies, cross-border health data and the GDPR." *Information & Communications Technology Law* 28, no. 3 (2019): 261-274, p. 262.
[247] General Data Protection Regulation, Article 12.
[248] Vorras, Apostolos, and Lilian Mitrou. "Unboxing the black box of artificial intelligence: algorithmic transparency and/or a right to functional explainability." In *EU Internet Law in the Digital Single Market*, pp. 247-264. Cham: Springer International Publishing, 2021.
[249] Bakhoum, Mor, Beatriz Conde Gallego, Mark-Oliver Mackenrodt, and Gintarė Surblytė-Namavičienė, eds. *Personal data in competition, consumer protection and intellectual property law*. Berlin: Springer, 2018.
[250] Leenes, Ronald, and Aaron Martin. "Technology and regulation 2021." (2022), p.17.
[251] Leenes and Martin. "Technology and regulation 2021.", p17.

basis.[252] Data controllers must clearly define the purposes for which personal data is collected and ensure that the data is not used for unrelated activities without obtaining explicit consent from the data subject**.** Article 6 of the GDPR indicates the lawful bases for processing personal data. These bases consist of the following: consent, contractual necessity, "*compliance with legal obligations, protection of the vital interests of the data subject, performance of a task carried out in the public interest or in the exercise of official authority, and legitimate interests*"[253], pursued by the data controller or a third party.[254]

Furthermore, data minimization is the principle indicating that personal data should be relevant and constrained to what is required for the processing's purposes.[255] Having IoT devices for health purposes in mind, data minimization requires that only the minimum amount of personal data necessary to fulfil the intended purposes is collected and processed. Wearables shall avoid collecting excessive or unnecessary data that is unrelated to the device's functionality.[256] Data minimization assists in mitigating privacy risks by reducing the quantity of[257] personal data that is stored and processed,[258] minimizing the potential impact of a data breach or unauthorized access. Article 5(1)(c) of the GDPR puts an emphasis of the need for data minimization as a fundamental principle of data protection.

The next principle outlined in the GDPR is the lawfulness one, "*which states that personal data must be processed lawfully*".[259]According to it, a legitimate legal basis must be used before processing personal data.[260] For the purpose of collecting and processing personal data, wearables must have a legal basis, such as obtaining explicit consent from the data subject, for instance for complying with a legal requirement, protecting vital interests, performing a task in the public interest, or exercising official authority, or pursuing legitimate interests. Article 6 of the GDPR outlines the lawful bases for processing personal data. Additionally, the accuracy principle requires that personal data be accurate and kept up to date.[261] Therefore, this is also the criteria in the context of wearables,

[252] General Data Protection Regulation, Article 5(1)(a).

[253] Jasmontaite, Lina, and Paul De Hert. "The EU, children under 13 years, and parental consent: a human rights analysis of a new, age-based bright-line for the protection of children on the Internet." *International Data Privacy Law* 5, no. 1 (2015): 20-33, p.2.

[254] Osano, "What is a privacy notice, and how does it protect your data?" JDSUPRA, last accessedon 22.08.2023 https://www.jdsupra.com/legalnews/what-is-a-privacy-notice-and-how-does-8218009/

[255] Bincoletto, Giorgia. "Data Protection by Design in the E-Health Care Sector." (2021), p. 131.

[256] Alharbi, Rawan, and Haya Almagwashi. "The Privacy requirments for wearable IoT devices in healthcare domain." In *2019 7th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW)*, pp. 18-25. IEEE, 2019, p.3.

[257] Samaila, Musa Gwani. "Internet of Things Hardware Platform Security Advisor.".

[258] Samaila, Musa Gwani. "Internet of Things Hardware Platform Security Advisor."

[259] Piasecki, "Complying with the GDPR When Vulnerable People Use Smart Devices" (n'60).

[260] General Data Protection Regulation, Article 5.

[261] General Data Protection Regulation, Article 5(1) (d).

ensuring that the processing of data is reliable. Article 5(1)(d) of the GDPR emphasizes the importance of data accuracy.

Next, the principle of storage limitation indicates that personal data should be *"kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data is processed"*.[262] Basically, this means that wearables must not retain personal data longer than necessary.[263] Organizations should establish appropriate data retention periods and regularly review and delete personal data that is no longer required. Article 5(1)(e)[264] of the GDPR emphasizes the need to limit the storage of personal data. The integrity and confidentiality principle requires that personal data be processed in a manner that ensures its security, including protection against unauthorized or unlawful processing, loss, destruction, or damage.[265] Wearables must implement appropriate measures to safeguard the[266] integrity and confidentiality of the personal data they collect and process. This includes encryption, access controls, regular security assessments, and the ability to restore data in case of a security incident. Article 5(1)(f) of the GDPR addresses personal data confidentiality and integrity.[267]

The last principle, the principle of accountability emphasizes the responsibility of organizations to demonstrate compliance with the GDPR and[268] to be accountable for their data processing activities.[269] This includes implementing appropriate data protection policies, conducting data protection impact assessments (DPIAs), maintaining records of processing activities, and ensuring that data subjects' rights are respected.[270] Accountability is a fundamental principle that underlies the entire GDPR framework. Article 5(2) and Article 24 of the GDPR outline the principle of accountability and the obligations of data controllers to demonstrate compliance. In the next section of the chapter, it will be discussed how fitness trackers approach vulnerability of data subjects.

[262] General Data Protection Regulation, Article 5(1) (e).
[263] Rawan and Almagwashi. "The Privacy requirements for wearable IoT devices in healthcare domain." (n'3).
[264] General Data Protection Regulation, Article 5(1) (e).
[265] Article 5(1)(f), GDPR.
[266] Voigt and Von dem Bussche. "The EU General Data Protection Regulation (GDPR)".
[267] Bincoletto. "Data Protection by Design in the E-Health." (n'263).
[268] Voigt and Von dem Bussche. "The EU General Data Protection Regulation (GDPR)".
[269] Article 5(2), Article 24, GDPR.
[270] Rawan and Almagwashi. "The Privacy requirements for wearable IoT devices in healthcare domain." (n'3).

4.4 How fitness trackers approach vulnerability of data subjects?

"Health data" is defined in the GDPR by Article 4 paragraph 15,[271] as *"personal data related to the physical or mental health of a person, including the provision of health care services, which reveal information about his or her health status"*.[272] Nevertheless, types of data such as the one from fitness trackers, are not rigorously define as belonging to this category.[273] Therefore, health data is further specified as: strictly medical data[274] - data in a formal medical setting, such as electronic health record (EHR) data,[275] and raw data – e.g., collected by fitness tracker's sensors – only when it's used to assess a person's health.[276] Pervasive collection and processing of personal data raises some concerns associated with the right to data protection, particularly those data subjects underlined as vulnerable under the GDPR, and those who experience layered vulnerability.[277] Therefore, the approach taken by fitness trackers in terms of vulnerability of data subject is by taking measures to protect data subjects' privacy and data security. In the following paragraphs the thesis will emphasizes on some of the common approaches for fitness tracers towards vulnerability of data subjects.

Informed consent[278] is one of the common approaches and principles that fitness trackers adopt to ensure the protection and privacy of vulnerable data subjects. However, some issues arise in terms of obtaining informed consent by vulnerable data subjects. For instance, this type of data subjects may have varying levels of cognitive capacity or understanding of complex data processing concepts. Consequently, this could hinder their ability to comprehend the potential risks, benefits, and implications of data sharing and processing.[279] Another obstacle could be the complexity of information, since data processing practices in the context of advanced technologies, can involve technical jargon and intricate details. Thus, presenting this information in a clear and understanding manner might be difficult for vulnerable data subjects to comprehend.[280] Power imbalance could also fall

[271] General Data Protection Regulation, Article 4(15).

[272] Koren, Ana, and Ramjee Prasad. "Iot health data in electronic health records (ehr): Security and privacy issues in era of 6g." *Journal of ICT Standardization* (2022): 63-84, p.70.

[273] Koren and Prasad. "Iot health data in electronic health records (ehr) " 63-84.

[274] Koren and Prasad. "Iot health data in electronic health records (ehr) " 63-84.

[275] Electronic Health Reports

[276] Koren and Prasad. "Iot health data in electronic health records (ehr) " 63-84.

[277] Milkaite, Ingrida, and Eva Lievens. "Child-friendly transparency of data processing in the EU: from legal requirements to platform policies." *Journal of Children and Media* 14, no. 1 (2020): 5-21, p. 7.

[278] General Data Protection Regulation, Art 6, Art 7.

[279] Wang, Yichuan, LeeAnn Kung, and Terry Anthony Byrd. "Big data analytics: Understanding its capabilities and potential benefits for healthcare organizations." *Technological forecasting and social change* 126 (2018): 3-13.

[280] Breuer, Jonas, Rob Heyman, and Rosamunde van Brakel. "Data protection as privilege—Factors to increase meaning of GDPR in vulnerable groups." *Frontiers in Sustainable Cities* 4 (2022): 977623.

under the obstacles of obtaining informed consent by vulnerable data subjects, due to the fact that they can find it challenging to provide truly autonomous and voluntary consent.

Transparency[281] is another common approach for ensuring data protection and privacy of vulnerable data subjects. This fundamental principle in data processing may also pose challenges for vulnerable data subjects. One example is the fact that vulnerability may lead to limited understanding, and difficulties comprehending technical terms. Information overload indicates for more obstacles, since privacy polices regularly contain detailed information that can be overwhelming or vulnerable data subjects. Furthermore, user control[282] is also used by fitness trackers, in order to empower data subjects to exercise their rights. Data subjects are enabled to access their data, request corrections, and delete their data when desired and requested. However, here again, vulnerable data subjects may face some difficulties. One such impediment is decision-making capacity, since some data subjects may experience limited decision-making capacity, making it challenging for them to provide meaningful consent or make choices about data sharing.

Data security measures under Article 32 of the Regulation,[283] is another approach fitness trackers takes to approach vulnerability in data subjects. Privacy policies outline the security measures implemented to protect user data, as required by GDPR. The obstacles under this approach are also not missing. Vulnerable data subjects, may be more susceptible to external influence, which may lead to inability of making independent decisions, regarding data sharing and control.

In relation to third-party sharing,[284] fitness tracker privacy policies serve as a conduit for informing users about any integrations with third-party apps or services. These integrations can have implications for data privacy, and the privacy policies provide transparent insights into these connections. Overall, each of these approaches towards vulnerability of the data subjects, pose some obstacles to them. In the following section the reader will be introduced how the GDPR overcomes these obstacles, and if the rules and principles of the Regulation towards the protection of vulnerable data subjects, perform their task when applied to personal data processing by IoT devices for healthcare purposes.

4.5 Addressing vulnerability

Each and any of the discussed approaches towards vulnerability of data subjects, has its obstacles which were presented to the reader in the previous section. In this section, the thesis addresses

[281] General Data Protection Regulation, Article 5, Article 12.
[282] General Data Protection Regulation, Article 15, Article 17.
[283] General Data Protection Regulation, Article 32.
[284] General Data Protection Regulation, Article 13, Article 14.

vulnerability, as well as if the provisions of the GDPR can be interpreted with reference to wearable IoT devices for health purposes to protect vulnerable data subjects, and if the rules and principles of the GDPR towards protecting vulnerable data subjects perform their task when applied to personal data processing by these IoT devices. In the last section of the chapter, the emphasis will be on transparency, fairness and purpose limitation principles.

The transparency[285] principle is one of the fundamental principles regarding data collection, processing, and its application is essential for ensuring the protection of vulnerable data subjects, and without its correct application, data subjects who are at higher risk will not be able to fully utilize their rights to data protection.[286] But is this principle suitable for protecting vulnerable data subjects when fitness trackers do processing of data? The transparency principle holds a vital role in overcoming different types of vulnerability. For instance, cognitive vulnerability, which is inherent for data subjects with varying capacity level of cognitive capacity. In this scenario, the terms of clear and plain language requirements ensure that vulnerable data subjects can comprehend how their health data is being used and make informed decisions about sharing it. However, it has been indicated that by facilitating the language in a clear and plain manner, this can often result in simple explanations which are not sufficient enough to reflect "*the actual reality of what is happening to personal data*".[287] Additionally, the criteria for "easily accessible" indicates that individuals who are vulnerable to identity theft should not have to look for information; for example, if fitness trackers just record heart rate or oxygen saturation levels, this information should be immediately visible.[288] Furthermore, in the context of healthcare devices, there could be a significant power imbalance between data subjects and technology providers. Transparent communication about data collection, storage, sharing and processing empowers individuals to understand the roles and responsibilities of all parties involved. Therefore, transparency helps mitigate information asymmetry and enables data subjects to exercise their rights more effectively. Transparency also helps overcoming vulnerability in terms of health data.

Same as transparency, the fairness principle is enshrined in Article 5.1(a) of the GDPR.[289] Some authors argue that fairness is politicized,[290] however, others believe that fairness is a broad

[285] General Data Protection Regulation, Article 5(1)(a).
[286] Piasecki and Chen. "Complying with the GDPR when vulnerable people use smart devices." (n'118).
[287] Piasecki, "Complying with the GDPR When Vulnerable People Use Smart Devices" (n'67).
[288] Piasecki and Chen. "Complying with the GDPR when vulnerable people use smart devices." (n' 122).
[289] General Data Protection Regulation, Article 5(1)(a).
[290] Abiteboul, Serge, and Julia Stoyanovich. "Transparency, fairness, data protection, neutrality: Data management challenges in the face of new regulation." *Journal of Data and Information Quality (JDIQ)* 11, no. 3 (2019): 1-9, p.5.

concept that depends on the context.[291] While all of this may be true, it is important to think about how data controllers should apply fairness in the context of vulnerable data subjects. The importance of the fairness principle in GDPR reflects a growing imbalance of power between controller and data subject. Despite the fact that GDPR does not define fairness, WP29, considered this principle to be related to awareness.[292] In other words, the principle of fairness stipulates that data is to be gathered only after informing the data subject of its intended use.[293] When it comes to fitness trackers, processing is deemed unfair, for instance, if the product monitors blood oxygen levels while also collecting heart rate data without appropriately telling the data subject via device interfaces or other means.[294]

Although they are related, fairness and transparency do not mean the same thing. Suppose a smart device provides transparent information to the general public of data subject but does not make it accessible to a small number of individuals with learning impairments who also use the product. In such situations, this should not be considered *"fair transparency".* It is important to note that anyone can become vulnerable at any time due to a sudden decline in health or other external factors. Just because a IoT device for healthcare purpose doesn't target vulnerable data subject, this is not an indication that these data subject will not acquire vulnerability at some point.

Additionally, fairness has objective of preventing the data controller from mishandling the data subject's data through balancing exercises. Usually, the balance exercise is explicitly required by the Regulation, to be performed by controller.[295] If an IoT device processes the data of vulnerable data subjects, the data controller will need to consider the "*increased power imbalance between them and the data subject to ensure that the process is fair*".[296] For instance, a fitness tracker that shares data subject's data with an external party has to explicitly states why it does it so. Fair processing relies on the context and many more IoT-related instances of fair balance would be beneficial for data controllers.

An interesting indication regarding third-party risk is the Xiaomi privacy policy. According to the privacy policy, the business does not disclose any personal data to outside parties. [297] However,

[291] Buitelaar, J. C. "Child's best interest and informational self-determination: what the GDPR can learn from children's rights." *International Data Privacy Law* 8, no. 4 (2018): 293-308, p.5

[292] Wachter, Sandra. "The GDPR and the Internet of Things: a three-step transparency model." *Law, Innovation and Technology* 10, no. 2 (2018): 266-294, p.9.

[293] Piasecki and Chen. "Complying with the GDPR when vulnerable people use smart devices." (n'123).

[294] Piasecki and Chen. "Complying with the GDPR when vulnerable people use smart devices." (n'124).

[295] Clifford, Damian, and Jef Ausloos. "Data protection and the role of fairness." *Yearbook of European Law* 37 (2018): 130-187, p. 8.

[296] Piasecki, "Complying with the GDPR When Vulnerable People Use Smart Devices" (n'74).

[297] Dini Kounoudes, Alexia, Georgia M. Kapitsaki, and Ioannis Katakis. "Enhancing user awareness on inferences obtained from fitness trackers data." *User Modeling and User-Adapted Interaction* (2023): 1-48.

here is the paradox, since the policy continues, by claiming that they may sometimes share the personal data of their users to third parties, only in cases where improving of Xiaomi’s services are needed.[298] The policy continues by stating that a data subject data might be shared with their third-party service providers and business partners[299] (e.g., delivery service providers, data centers, other business partners). The policy also mentions that these outside parties may handle data processing on Xiaomi's behalf.[300] However, the only clarification provided is that the data subjects would be notified; the policy does not clarify or explain what will happen to the data subjects' personal information in the event of a merger or sale.[301] Here again, there are issues at stake regarding third-party risks, that are higher for vulnerable data subjects, since they may not be fully aware or comprehend the implications of data sharing with these third parties. Additionally, data subjects’ health information could be misused if it falls into the hands of a party that has an aim to utilize the personal data for malicious purposes.

4.6. Conclusion

Despite the obstacles, the chapter argued that the provisions of the Regulation have the potential (to some extent) to overcome vulnerability and protect data subjects. It emphasizes the critical role of transparency and fairness principle. Overall, the rules and principles of the GDPR are a significant instrument when it comes to protecting data subjects’ personal data in today’s digital era. However, in the context of processing personal data by IoT devices for health purposes, particularly fitness trackers, it becomes evident that while the Regulation provides a foundational framework, it may not be fully equipped to address the challenges and complexities posed by these devices. For instance, in the example given with Xiaomi’s privacy policy, that policy falls short in explaining the specifics of data sharing with third parties, despite the existence of the transparency principle. Thus, the argument can be made that in fact the GDPR is a significant instrument, but it does not fulfil entirely it’s tasks in terms of safeguarding, while processing is done by IoT devices. Basically, obtaining meaningful informed consent from vulnerable data subject can be challenging, and potentially leading to scenarios where their privacy is compromised without their knowledge. While the GDPR’s provisions are without doubt well-intentioned, they may not address these vulnerabilities, as they assume a certain level of understanding that might not be present in all data

[298] Pingo, Zablon, and Bhuva Narayan. "Users’ responses to privacy issues with the connected information ecologies created by fitness trackers." In *Maturity and Innovation in Digital Libraries: 20th International Conference on Asia-*

[299] Pingo and Narayan, "Users’ responses to privacy issues with the connected information ecologies created by fitness trackers." (n’4).

[300] Kounoudes, Alexia, Kapitsaki and Katakis, "Enhancing user awareness on inferences obtained from fitness trackers data." 1-48.

[301] Kounoudes, Alexia, Kapitsaki and Katakis, "Enhancing user awareness on inferences obtained from fitness trackers data." 1-48.

subjects. Another aspect that supports the argument that GDPR's provisions may not efficiently protect data subjects when IoT are involved, it the rapid pace of technological advancement, which often outplaces regulatory updates. In fact, IoT devices for healthcare purposes, as any other IoT device, are continuously evolving, by introducing new capabilities and functionalities that may have unforeseen implications for data privacy. Thus, the GDPR's static nature does not make it facile to keep up with these changes and ensure that data protection measures remain relevant and effective. Referring back to Xiaomi's privacy policy, which states that sharing data may occur in terms of service improvement, which is incongruous with the purpose limitation principle, but still this is the policy, despite the existence of the purpose limitation. Indeed, the Regulation emphasizes strongly on transparency and informed consent, but the dynamic nature of IoT devices may potentially make it difficult to ensure that data subjects have a clear understanding of how their data is being used and processes, leading to potential privacy breaches.

5. Conclusion

This thesis argued that vulnerability may have many layers, and that the concept cannot be put in a universal framework. The lack of a concrete Article under the Regulation that explicitly frames which data subjects shall be considered as vulnerable, makes it even more difficult to assess who may need extra protection when data is being process by wearable devices. Therefore, one alleviation could be always assuming that an IoT device can be used by vulnerable data subjects. This will not only protect current vulnerable smart product data subjects, but also individuals who may become vulnerable in the future. In that case another provision could be added in the Regulation, that through more rules and principles to establish to some extent how and why data subjects shall be considered always as vulnerable. Additionally, the fairness principle could be more emphasized on. In order to convey data ethics initiatives, it is still necessary to clarify that notion. There is also a possibility to define it more generally and outside of stringent legal constraints.

Overall, there is a gap between the rules and principles established in the GDPR when protecting vulnerable data subjects in terms of processing data by fitness trackers. Firstly, it could be argued that the transparency principle, in the context of fitness trackers, is lacking. This is because these devices often collect and process data continuously, without the knowledge and understanding of the data subject, of the exact purpose of the collection and processing of their data. In fact, establishing transparency in the context of wearables is already not a facile task, but when vulnerable data subjects are involved, it could be argued that it is almost not accomplishable, since they may have limited understanding or cognitive abilities to comprehend the complexities of data processing by wearables.

Additionally, it is possible that wearable technology would allow the processing of personal data for purposes other than those for which it was originally obtained, as it was indicted in the Xiaomi privacy policy. Thus, this raises some issues about the potential misuse or excessive processing of personal data by fitness trackers, which in fact might be in contradiction with the outlined by the GDPR purpose limitation principle. This may lead to the use of personal data by wearables for unrelated activities. Additionally, these devices collect detailed and extensive personal data (e.g., location data, biometric data), which may lead to unnecessary collection of data, that goes beyond the intended purposes. Therefore, this raises concerns about the effectiveness of data minimization in protecting vulnerable data subjects when wearables do processing of their data.

The lawfulness principle is also in question regarding its effectiveness, in the context of fitness trackers. While consent is one of the lawful bases for processing personal data, it could be argued that obtaining valid consent form vulnerable data subjects groups pose serious challenges, due to their limited understanding or capacity to provide meaningful consent. Wearable devices may face challenges in terms of the accuracy principle as well. This is because it is questionable if the vulnerable data subjects can establish full accuracy. For instance, data subjects with disabilities and patients may experience difficulties in provided accurate and reliable information. The reliance on data collected through fitness trackers may raise concerns about the inaccurate data, leading to potential wrong diagnosis in the future.

Lastly, fitness trackers devices may face some challenges in the storage limitation, integrity, and confidentiality principles. This is due to the fact that wearables collect vast amount of personal data, as well as sensitive one, which may often require extended storage length periods for ongoing monitoring analysis. The implementation of strict storage limitations, while ensuring effective healthcare support for vulnerable data subjects can be complex. Furthermore, the nature of wearables and their reliance on wireless communication may introduce security vulnerabilities, potentially compromising the completeness and confidentiality of personal data.

In conclusion, while the rules and principles under the GDPR aim to protect vulnerable data subjects, they may not effectively perform their task when applied to personal data processing IoT devices for healthcare purposes, in particular to fitness trackers.

Bibliography

1. Victor, Elizabeth, Florencia Luna, Laura Guidry- Grimes, and Alison Reiheld. "Vulnerability in practice: peeling back the layers, avoiding triggers, and preventing cascading effects." *Bioethics* 36, no. 5 (2022): 587-596.
2. Custers, B., F. Dechesne, A. M. Sears, T. Tani, and S. van der Hof. "A comparison of data protection legislation and policies across the EU. Computer Law & Security Review, 34 (2), 234-243." (2018).
3. Dimitrov, Dimiter V. "Medical internet of things and big data in healthcare." *Healthcare informatics research* 22, no. 3 (2016): 156-163.
4. Tupasela, Aaro, Juanita Devis Clavijo, Marjut Salokannel, and Christoph Fink. "Older people and the smart city: Developing inclusive practices to protect and serve a vulnerable population." *Internet policy review* 12, no. 1 (2023): 1-21.
5. Camara, Carmen, Pedro Peris-Lopez, and Juan E. Tapiador. "Security and privacy issues in implantable medical devices: A comprehensive survey." *Journal of biomedical informatics* 55 (2015): 272-289.
6. Chico, Victoria. "The impact of the general data protection regulation on health research." *British medical bulletin* 128, no. 1 (2018): 109-118.
7. Luna, Florencia. "Elucidating the concept of vulnerability: Layers not labels." *IJFAB: International Journal of Feminist Approaches to Bioethics* 2, no. 1 (2009): 121-139.
8. Lindstad, Sarita, and Kaspar Rosager Ludvigsen. "When is the processing of data from medical implants lawful? The legal grounds for processing health-related personal data from ICT implantable medical devices for treatment purposes under EU data protection law." (2022): 1-36.
9. Chassang, Gauthier. "The impact of the EU general data protection regulation on scientific research." *ecancermedicalscience* 11 (2017).
10. Chandra, Shekhar S., Jason A. Dowling, Peter B. Greer, Jarad Martin, Chris Wratten, Peter Pichler, Jurgen Fripp, and Stuart Crozier. "NOVA University of Newcastle Research Online nova. newcastle. edu. au."
11. Poyner, I. K., and R. S. Sherratt. "Privacy and security of consumer IoT devices for the pervasive monitoring of vulnerable people." In *Living in the Internet of Things: Cybersecurity of the IoT-2018*, pp. 1-5. IET, 2018.
12. Poyner, I. K., and R. S. Sherratt. "Privacy and security of consumer IoT devices for the pervasive monitoring of vulnerable people." In *Living in the Internet of Things: Cybersecurity of the IoT-2018*, pp. 1-5. IET, 2018.

13. Badii, Claudio, Pierfrancesco Bellini, Angelo Difino, and Paolo Nesi. "Smart city IoT platform respecting GDPR privacy and security aspects." *IEEE Access* 8 (2020): 23601-23623.
14. Piasecki, Stanislaw. "Expert perspectives on GDPR compliance in the context of smart homes and vulnerable persons." *Information & Communications Technology Law* (2023): 1-33.
15. Rose, Karen, Scott Eldridge, and Lyman Chapin. "The internet of things: An overview." *The internet society (ISOC)* 80 (2015): 1-50.
16. Williams, Ryan, Emma McMahon, Sagar Samtani, Mark Patton, and Hsinchun Chen. "Identifying vulnerabilities of consumer Internet of Things (IoT) devices: A scalable approach." In *2017 IEEE International Conference on Intelligence and Security Informatics (ISI)*, pp. 179-181. IEEE, 2017.
17. Koren, Ana, and Ramjee Prasad. "Iot health data in electronic health records (ehr): Security and privacy issues in era of 6g." *Journal of ICT Standardization* (2022): 63-84.
18. Ioannidou, Irene, and Nicolas Sklavos. "On general data protection regulation vulnerabilities and privacy issues, for wearable devices and fitness tracking applications." *Cryptography* 5, no. 4 (2021): 29.
19. REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
20. Arteaga-Falconi, Juan Sebastian, Hussein Al Osman, and Abdulmotaleb El Saddik. "ECG authentication for mobile devices." *IEEE Transactions on Instrumentation and Measurement* 65, no. 3 (2015): 591-600.
21. Bozzaro, Claudia, Joachim Boldt, and Mark Schweda. "Are older people a vulnerable group? Philosophical and bioethical perspectives on ageing and vulnerability." *Bioethics* 32, no. 4 (2018): 233-239.
22. Piasecki, Stanislaw, and Jiahong Chen. "Complying with the GDPR when vulnerable people use smart devices." *International Data Privacy Law* 12, no. 2 (2022): 113-131.
23. Moerel, Lokke, and Corien Prins. "Privacy for the homo digitalis: Proposal for a new regulatory framework for data protection in the light of Big Data and the internet of things." *Available at SSRN 2784123* (2016).
24. Mulder, Trix, and Nynke E. Vellinga. "Exploring data protection challenges of automated driving." *Computer Law & Security Review* 40 (2021): 105530.
25. Mitrou, Lilian. "Data protection, artificial intelligence and cognitive services: is the general data protection regulation (GDPR)'artificial intelligence-proof'?." *Artificial Intelligence and*

Cognitive Services: Is the General Data Protection Regulation (GDPR)'Artificial Intelligence-Proof (2018).

26. Kaewkannate, Kanitthika, and Soochan Kim. "A comparison of wearable fitness devices." *BMC public health* 16 (2016): 1-16.
27. Haghi, Mostafa, Kerstin Thurow, and Regina Stoll. "Wearable devices in medical internet of things: scientific research and commercially available devices." *Healthcare informatics research* 23, no. 1 (2017): 4-15.
28. Yetisen, Ali K., Juan Leonardo Martinez- Hurtado, Barış Ünal, Ali Khademhosseini, and Haider Butt. "Wearables in medicine." *Advanced Materials* 30, no. 33 (2018): 1706910.
29. Alshohoumi, Fatma, Mohammed Sarrab, Abdulla AlHamadani, and Dawood Al-Abri. "Systematic review of existing IoT architectures security and privacy issues and concerns." *International Journal of Advanced Computer Science and Applications* 10, no. 7 (2019).
30. Mazhelis, Oleksiy, Eetu Luoma, and Henna Warma. "Defining an internet-of-things ecosystem." In *Conference on Internet of Things and Smart Spaces*, pp. 1-14. Berlin, Heidelberg: Springer Berlin Heidelberg, 2012.
31. Sametinger, Johannes, Jerzy Rozenblit, Roman Lysecky, and Peter Ott. "Security challenges for medical devices." *Communications of the ACM* 58, no. 4 (2015): 74-82.
32. Livingstone, Sonia, and Amanda Third. "Children and young people's rights in the digital age: An emerging agenda." *New media & society* 19, no. 5 (2017): 657-670.
33. Jiang, Yichuan. "A survey of task allocation and load balancing in distributed systems." *IEEE Transactions on Parallel and Distributed Systems* 27, no. 2 (2015): 585-599.
34. Coorevits, Lynn, and Tanguy Coenen. "The rise and fall of wearable fitness trackers." In *Academy of Management*. 2016.
35. Stone, John. "Race and healthcare disparities: overcoming vulnerability." *Theoretical Medicine and Bioethics* 23 (2002): 499-518.
36. Malgieri, Gianclaudio. *Vulnerability and Data Protection Law*. Oxford University Press, 2023.
37. Clifford, Damian, and Jef Ausloos. "Data protection and the role of fairness." *Yearbook of European Law* 37 (2018): 130-187.
38. Wachter, Sandra. "GDPR and the internet of things: guidelines to protect users' identity and privacy." *Tillgänglig online: https://papers. ssrn. com/sol3/papers. cfm* (2018).
39. Vermesan, Ovidiu, and Peter Friess, eds. *Internet of things: converging technologies for smart environments and integrated ecosystems*. River publishers, 2013

40. Meneghello, Francesca, Matteo Calore, Daniel Zucchetto, Michele Polese, and Andrea Zanella. "IoT: Internet of threats? A survey of practical security vulnerabilities in real IoT devices." IEEE Internet of Things Journal 6, no. 5 (2019): 8182-8201.
41. Gubbi, Jayavardhana, Rajkumar Buyya, Slaven Marusic, and Marimuthu Palaniswami. "Internet of Things (IoT): A vision, architectural elements, and future directions." Future generation computer systems 29, no. 7 (2013): 1645-1660.
42. Borgia, Eleonora. "The Internet of Things vision: Key features, applications and open issues." *Computer Communications* 54 (2014): 1-31.
43. Ching, Ke Wan, and Manmeet Mahinderjit Singh. "Wearable technology devices security and privacy vulnerability analysis." *International Journal of Network Security & Its Applications* 8, no. 3 (2016): 19-30.
44. Kapoor, Vidhi, Rishabh Singh, Rishabh Reddy, and Prathamesh Churi. "Privacy issues in wearable technology: An intrinsic review." In *Proceedings of the International Conference on Innovative Computing & Communications (ICICC)*. 2020.
45. Jiang, Yichuan. "A survey of task allocation and load balancing in distributed systems." IEEE Transactions on Parallel and Distributed Systems 27, no. 2 (2015): 585-599, p. 585.
46. Tech4Good, IoT node, accessed on 19/08/2022, https://marketplace.intelligentcitieschallenge.eu/en/solutions/iot-node#:~:text=In%20other%20words%2C%20the%20IoT,multiple%20sensors%20with%20diverse%20origins.
47. Georgiou, Dimitra, and Costas Lambrinoudakis. "Compatibility of a security policy for a cloud-based healthcare system with the EU general data protection regulation (GDPR)." Information 11, no. 12 (2020): 586.
48. Ryan Calo, Privacy, Vulnerability, and Affordance, 66 DePaul L. Rev. (2017).
49. Chacko, Anil, and Thaier Hayajneh. "Security and privacy issues with IoT in healthcare." EAI Endorsed Transactions on Pervasive Health and Technology 4, no. 14 (2018).
50. Rolf H.Weber, ‘Internet of Things- New security and privacy challenges’ (2010) 26 Computer Law & Security Review 23.
51. Psychoula, Ismini, Liming Chen, and Oliver Amft. "Privacy risk awareness in wearables and the internet of things." *IEEE Pervasive Computing* 19, no. 3 (2020): 60-66.
52. Martínez-Pérez, Borja, Isabel De La Torre-Díez, and Miguel López-Coronado. "Privacy and security in mobile health apps: a review and recommendations." *Journal of medical systems* 39, no. 1 (2015): 1-8.
53. Vidhi, Singh, Reddy, and Churi. "Privacy issues in wearable technology” 2020.

54. Ikrissi, Ghizlane, and Tomader Mazri. "IOT-BASED SMART ENVIRONMENTS: STATE OF THE ART, SECURITY THREATS AND SOLUTIONS." *ISPRS Annals of Photogrammetry, Remote Sensing & Spatial Information Sciences* (2021).
55. Alshohoumi, Fatma, Mohammed Sarrab, Abdulla AlHamadani, and Dawood Al-Abri. "Systematic review of existing IoT architectures security and privacy issues and concerns." *International Journal of Advanced Computer Science and Applications* 10, no. 7 (2019), p.234.
56. Hadzovic, Suada, Sasa Mrdovic, and Milutin Radonjic. "Identification of IoT actors." *Sensors* 21, no. 6 (2021): 2093.
57. Data protection Commission (2019). Guidance Note: Guide to Data Protection Impact Assessments (DPIAs).
58. Mohamed and Køien. "Cyber security and the internet of things" 65-88, 74.
59. Article 29 Data Protection Working Party. (2014). Opinion 8/2014 on the Recent Developments on the Internet of Things.
60. Fineman, Martha Albertson. "The vulnerable subject: Anchoring equality in the human condition." In *Transcending the boundaries of law*, pp. 177-191. Routledge-Cavendish, 2010.
61. Luna, "Elucidating the concept of vulnerability", 121-139.
62. Livingstone, Sonia. "Children: a special case for privacy?" *Intermedia* 46, no. 2 (2018): 18-23.
63. Crepax, Tommaso, Victor Muntés-Mulero, Jabier Martinez, and Alejandra Ruiz. "Information technologies exposing children to privacy risks: domains and children-specific technical controls." *Computer Standards & Interfaces* 82 (2022): 103624.
64. Krivokapic, Dorde, and Jelena Adamovic. "Impact of General Data Protection Regulation on children's rights in digital environment." *Annals Fac. L. Belgrade Int'l Ed.* (2016): 205.
65. Van Hoecke, Mark. "Legal doctrine: Which method (s) for what kind of discipline?." In *Methodologies of legal research: which kind of method for what kind of discipline?*, pp. 1-18. Hart Publishing, 2011.
66. Banerjee, Syagnik, Thomas Hemphill, and Phil Longstreet. "Wearable devices and healthcare: Data sharing and privacy." *The Information Society* 34, no. 1 (2018): 49-57.
67. Jin, Chun Yu. "A review of AI Technologies for Wearable Devices." In *IOP Conference Series: Materials Science and Engineering*, vol. 688, no. 4, p. 044072. IOP Publishing, 2019.
68. Ioannidou and Sklavos. "On General Data Protection Regulation Vulnerabilities and Privacy Issues, for Wearable Devices and Fitness Tracking Applications.": 29.

69. Simplilearn. “Cloud Computing vs Traditional Computing”, https://www.simplilearn.com/cloud-computing-vs-traditional-computing-article#:~:text=services%20and%20storage.-,What%20is%20Traditional%20Computing%3F,to%20manage%20and%20maintain%20them

70. Poongodi, T., Anu Rathee, R. Indrakumari, and P. Suresh. "IoT sensing capabilities: Sensor deployment and node discovery, wearable sensors, wireless body area network (WBAN), data acquisition." *Principles of internet of things (IoT) ecosystem: Insight paradigm* (2020).

71. Ometov, Aleksandr, Viktoriia Shubina, Lucie Klus, Justyna Skibińska, Salwa Saafi, Pavel Pascacio, Laura Flueratoru et al. "A survey on wearable technology: History, state-of-the-art and current challenges." *Computer Networks* 193 (2021): 108074.

72. Dimitrov, Dimiter V. "Medical internet of things and big data in healthcare." *Healthcare informatics research* 22, no. 3 (2016): 156-163.

73. Haghi, Mostafa, Kerstin Thurow, and Regina Stoll. "Wearable devices in medical internet of things: scientific research and commercially available devices." *Healthcare informatics research* 23, no. 1 (2017): 4-15.

74. Kaiser, Daniel W., Robert A. Harrington, and Mintu P. Turakhia. "Wearable fitness trackers and heart disease." *JAMA cardiology* 1, no. 2 (2016): 239-239.

75. Minaam, Diaa Salama Abdul, and Mohamed Abd-ELfattah. "Smart drugs: Improving healthcare using smart pill box for medicine reminder and monitoring system." *Future Computing and Informatics Journal* 3, no. 2 (2018): 443-456.

76. Alexander, Bryce, Sohaib Haseeb, and Adrian Baranchuk. "Are implanted electronic devices hackable?" *Trends in cardiovascular medicine* 29, no. 8 (2019): 476-480.

77. Pradeesh, E. L., V. Vadivel Vivek, M. Bhuvaneshwari, T. Thilakavarshini, V. Guruprasad, and A. Sri Vaishnavi. "Investigation on iot based smart e-inhaler integrated with mobile application." *Materials Today: Proceedings* 66 (2022): 1082-1087.

78. Suhail, Ibna, and Samaya Pillai. "IoT enabled applications for Healthcare decisions." In *2022 International Conference on Decision Aid Sciences and Applications (DASA)*, pp. 47-54. IEEE, 2022.

79. Hadzovic, Suada, Sasa Mrdovic, and Milutin Radonjic. "Identification of IoT actors." *Sensors* 21, no. 6 (2021): 2093, p. 2.

80. Kotha, Harika Devi, and V. Mnssvkr Gupta. "IoT application: a survey." *Int. J. Eng. Technol* 7, no. 2.7 (2018): 891-896, p. 892.

81. Fremantle, P. "A reference architecture for the internet of things,‖ vol. 0." (2015): 21.

82. Hadzovic, Suada, Sasa Mrdovic, and Milutin Radonjic. "Identification of IoT actors." *Sensors* 21, no. 6 (2021): 2093, p. 2.

83. Schladofsky, Werner, Jelena Mitic, Alfred Paul Megner, Claudia Simonato, Luca Gioppo, Dimitris Leonardos, and Arne Bröring. "Business models for interoperable IoT ecosystems." In *Interoperability and Open-Source Solutions for the Internet of Things: Second International Workshop, InterOSS-IoT 2016, Held in Conjunction with IoT 2016, Stuttgart, Germany, November 7, 2016, Invited Papers 2*, pp. 91-106. Springer International Publishing, 2017.

84. Schmid, Stefan, Arne Bröring, Denis Kramer, Sebastian Käbisch, Achille Zappa, Martin Lorenz, Yong Wang, Andreas Rausch, and Luca Gioppo. "An architecture for interoperable IoT ecosystems." In *Interoperability and Open-Source Solutions for the Internet of Things: Second International Workshop, InterOSS-IoT 2016, Held in Conjunction with IoT 2016, Stuttgart, Germany, November 7, 2016, Invited Papers 2*, pp. 39-55. Springer International Publishing, 2017.

85. King, Andrew A., and Michael J. Lenox. "Industry self-regulation without sanctions: The chemical industry's responsible care program." *Academy of management journal* 43, no. 4 (2000): 698-716.

86. Yu, Bin, Jarod Wright, Surya Nepal, Liming Zhu, Joseph Liu, and Rajiv Ranjan. "Iotchain: Establishing trust in the internet of things ecosystem using blockchain." *IEEE Cloud Computing* 5, no. 4 (2018): 12-23.

87. Sametinger, Johannes, Jerzy Rozenblit, Roman Lysecky, and Peter Ott. "Security challenges for medical devices." *Communications of the ACM* 58, no. 4 (2015): 74-82.

88. Vitunskaite, Morta, Ying He, Thomas Brandstetter, and Helge Janicke. "Smart cities and cyber security: Are we there yet? A comparative study on the role of standards, third party risk management and security ownership." *Computers & Security* 83 (2019): 313-331.

89. Djenna, Amir, Saad Harous, and Djamel Eddine Saidouni. "Internet of things meet internet of threats: New concern cyber security issues of critical cyber infrastructure." *Applied Sciences* 11, no. 10 (2021): 4580.

90. Malgieri, Gianclaudio, and Jędrzej Niklas. "Vulnerable data subjects." Computer Law & Security Review 37 (2020): 105415.

91. Waddington, Lisa. "Exploring vulnerability in EU Law: An analysis of ‘vulnerability’in EU criminal law and consumer protection law." *European Law Review* 45, no. 6 (2020): 779-801.

92. Bugeja, Joseph, Désirée Jönsson, and Andreas Jacobsson. "An investigation of vulnerabilities in smart connected cameras." In *2018 IEEE international conference on pervasive computing and communications workshops (PerCom workshops),* pp. 537-542. IEEE, 2018.

93. Livingstone, Sonia, and Amanda Third. "Children and young people’s rights in the digital age: An emerging agenda." *New media & society* 19, no. 5 (2017): 657-670.

94. Blume, Peter. "The data subject." *Eur. Data Prot. L. Rev.* 1 (2015): 258.

95. Quelle, Claudia. "Enhancing compliance under the general data protection regulation: the risky upshot of the accountability-and risk-based approach." *European Journal of Risk Regulation* 9, no. 3 (2018): 502-526.

96. Van der Hof, S. "Children and data protection from the perspective of children's rights-Some difficult dilemmas under the General Data Protection Regulation." *Thorbecke-colleges* (2018).

97. Georgiou, Dimitra, and Costas Lambrinoudakis. "Compatibility of a security policy for a cloud-based healthcare system with the EU general data protection regulation (GDPR)." *Information* 11, no. 12 (2020): 586.

98. Convention for the protection of individuals with regard to automatic processing of personal data [1981] ETS No. 108 (CM/Inf(2018)15-final).

99. Mulder, Trix, and Melania Tudorica. "Privacy policies, cross-border health data and the GDPR." *Information & Communications Technology Law* 28, no. 3 (2019): 261-274.

100.Tupasela, Aaro, Juanita Devis Clavijo, Marjut Salokannel, and Christoph Fink. "Older people and the smart city: Developing inclusive practices to protect and serve a vulnerable population." *Internet policy review* 12, no. 1 (2023): 1-21

101. Article Data Protection Working Party. "Opinion 8/2014 on the on Recent Developments on the Internet of Things." *European Commission* (2014).

102. Lindstad, Sarita, and Kaspar Rosager Ludvigsen. "When is the processing of data from medical implants lawful? The legal grounds for processing health-related personal data from ICT implantable medical devices for treatment purposes under EU data protection law." (2022): 1-36.

103. Enslow, Philip Harrison. "What is a" distributed" data processing system?." *Computer* 11, no. 1 (1978): 13-21.

104. Koops, Bert-Jaap. "The trouble with European data protection law." *International data privacy law* 4, no. 4 (2014): 250-261.

105. Heo, Sehyeon, Sungpil Woo, Janggwan Im, and Daeyoung Kim. "IoT-MAP: IoT mashup application platform for the flexible IoT ecosystem." In *2015 5th International Conference on the Internet of Things (IOT)*, pp. 163-170. IEEE, 2015.

106. Hadzovic, Suada, Sasa Mrdovic, and Milutin Radonjic. "Identification of IoT actors." *Sensors* 21, no. 6 (2021): 2093.

107. Mazhelis, Oleksiy, Eetu Luoma, and Henna Warma. "Defining an internet-of-things ecosystem." In *Conference on Internet of Things and Smart Spaces*, pp. 1-14. Berlin, Heidelberg: Springer Berlin Heidelberg, 2012.

108. Bell, Jessica, Stergios Aidinlis, Hannah Smith, Miranda Mourby, Heather Gowans, Susan E. Wallace, and Jane Kaye. "Balancing data subjects' rights and public interest research." *Eur. Data Prot. L. Rev.* 5 (2019): 43.

109. Milkaite, Ingrida, and Eva Lievens. "Child-friendly transparency of data processing in the EU: from legal requirements to platform policies." *Journal of Children and Media* 14, no. 1 (2020): 5-2.

110. Mulder, Trix, and Melania Tudorica. "Privacy policies, cross-border health data and the GDPR." *Information & Communications Technology Law* 28, no. 3 (2019): 261-274.

111. Alharbi, Rawan, and Haya Almagwashi. "The Privacy requirments for wearable IoT devices in healthcare domain." In *2019 7th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW)*, pp. 18-25. IEEE, 2019.

112. Wang, Yichuan, LeeAnn Kung, and Terry Anthony Byrd. "Big data analytics: Understanding its capabilities and potential benefits for healthcare organizations." *Technological forecasting and social change* 126 (2018): 3-13.

113. Breuer, Jonas, Rob Heyman, and Rosamunde van Brakel. "Data protection as privilege—Factors to increase meaning of GDPR in vulnerable groups." *Frontiers in Sustainable Cities* 4 (2022): 977623.

114. Piasecki, Stanislaw, and Jiahong Chen. "Complying with the GDPR when vulnerable people use smart devices." *International Data Privacy Law* 12, no. 2 (2022): 113-131.

115. Custers, Bart, Francien Dechesne, Alan M. Sears, Tommaso Tani, and Simone Van der Hof. "A comparison of data protection legislation and policies across the EU." *Computer Law & Security Review* 34, no. 2 (2018): 234-243.

116. Abiteboul, Serge, and Julia Stoyanovich. "Transparency, fairness, data protection, neutrality: Data management challenges in the face of new regulation." *Journal of Data and Information Quality (JDIQ)* 11, no. 3 (2019): 1-9.

117. Buitelaar, J. C. "Child’s best interest and informational self-determination: what the GDPR can learn from children’s rights." *International Data Privacy Law* 8, no. 4 (2018): 293-308, p.5.

118. Wachter, Sandra. "The GDPR and the Internet of Things: a three-step transparency model." *Law, Innovation and Technology* 10, no. 2 (2018): 266-294, p.9.

119. Clifford, Damian, and Jef Ausloos. "Data protection and the role of fairness." *Yearbook of European Law* 37 (2018): 130-187, p. 8.

120. Barati, Masoud, Omer Rana, Ioan Petri, and George Theodorakopoulos. "GDPR compliance verification in Internet of Things." *IEEE access* 8 (2020): 119697-119709.

121. Seyyar, M. Bas, and Zeno JMH Geradts. "Privacy impact assessment in large-scale digital forensic investigations." *Forensic Science International: Digital Investigation* 33 (2020): 200906.

122. Li, Wei, Yuanbo Chai, Fazlullah Khan, Syed Rooh Ullah Jan, Sahil Verma, Varun G. Menon, fnm Kavita, and Xingwang Li. "A comprehensive survey on machine learning-based big data analytics for IoT-enabled smart healthcare system." *Mobile networks and applications* 26 (2021): 234-252.

123. Ko, JeongGil, Chenyang Lu, Mani B. Srivastava, John A. Stankovic, Andreas Terzis, and Matt Welsh. "Wireless sensor networks for healthcare." *Proceedings of the IEEE* 98, no. 11 (2010): 1947-1960.

124. Mittelstadt, Brent. "Designing the health-related internet of things: ethical principles and guidelines." *Information* 8, no. 3 (2017): 77.

125. Kelly, Jessica M., Robert E. Strecker, and Matt T. Bianchi. "Recent developments in home sleep-monitoring devices." *International Scholarly Research Notices* 2012 (2012).

126. Wickramasinghe, Nilmini, and Freimut Bodendorf, eds. *Delivering superior health and wellness management with IoT and analytics*. Springer Nature, 2019.

127. Orlosky, Jason, Onyeka Ezenwoye, Heather Yates, and Gina Besenyi. "A look at the security and privacy of Fitbit as a health activity tracker." In *Proceedings of the 2019 ACM Southeast Conference*, pp. 241-244. 2019.

128. Dini Kounoudes, Alexia, Georgia M. Kapitsaki, and Ioannis Katakis. "Enhancing user awareness on inferences obtained from fitness trackers data." *User Modeling and User-Adapted Interaction* (2023): 1-48.

129. Hon, W. Kuan, Christopher Millard, and Ian Walden. "Negotiating cloud contracts: Looking at clouds from both sides now." *Stan. Tech. L. Rev.* 16 (2012): 79.

130. Pingo, Zablon, and Bhuva Narayan. "Users' responses to privacy issues with the connected information ecologies created by fitness trackers." In *Maturity and Innovation in Digital Libraries: 20th International Conference on Asia-Pacific Digital Libraries, ICADL 2018, Hamilton, New Zealand, November 19-22, 2018, Proceedings 20*, pp. 240-255. Springer International Publishing, 2018.

131. Fereidooni, Hossein, Tommaso Frassetto, Markus Miettinen, Ahmad-Reza Sadeghi, and Mauro Conti. "Fitness trackers: fit for health but unfit for security and privacy." In *2017 IEEE/ACM International Conference on Connected Health: Applications, Systems and Engineering Technologies (CHASE),* pp. 19-24. IEEE, 2017.

132. Torre, Ilaria, Odnan Ref Sanchez, Frosina Koceva, and Giovanni Adorni. "Supporting users to take informed decisions on privacy settings of personal devices." *Personal and Ubiquitous Computing* 22 (2018): 345-364.

133. Leenes, Ronald, and Aaron Martin. "Technology and regulation 2021." (2022).

134. Zivkovic, Carna, Yajuan Guan, and Christoph Grimm. "IoT Platforms, Use Cases, Privacy, and Business Models." (2021).

135. Paola, Iamiceli, Cafaggi Fabrizio, and CHIARA SILVIA Angiolini. "Casebook Effective Data Protection and Fundamental Rights." (2022).