A thesis submitted in fulfilment of the requirements of the Master of Laws: Advanced Studies Program in Law and Digital Technology degree, Leiden Law School.

Innovate, comply or die?

An analysis of the GDPR's impact on data-driven innovation in the healthcare industry and considerations for future policy response.

27.000 words

Author:

Hadassah Gavriella Drukarch

s1968793

Supervisor:

Prof.dr. V.A.J. Frissen

Second reader:

M.V. Kruizinga

LEIDEN UNIVERSITY

Leiden, The Netherlands

July 2023

Date: 10 July, 2023

Location: Amsterdam, The Netherlands

Declaration Statement

I further hereby certify that this is an original work, that this thesis does not contain any materials from other sources unless these sources have been clearly identified in footnotes, and any and all quotations have been properly marked as such and full attribution made to the author(‘s) thereof.

I further authorise Leiden University, the Faculty of Law, the LL.M. Adv. Programme in Law and Digital Technologies, its Programme Board and Director, and/or any authorised agents of the Institution, and persons named here in and above, to place my thesis in a library or other repository including but not limited to associated websites, for the use of the visitors to or personnel of said library or other repository. Access shall include but not be limited to hard copy or electronic media.

Name

Hadassah Gavriella Drukarch

Student Number

s1968793

Signature

HDukarch

Table of contents

Executive summary

Data is reshaping the way we produce, consume, and live. In this regard, the EC has noted that "[B]enefits will be felt in every single aspect of our lives, ranging from more conscious energy consumption and product, material and food traceability, to healthier lives and better health-care" (EC, 2020b). In light of the latter, the combined use of (Big) health data and technologies to make sense of such data has opened unprecedented opportunities to improve the outcomes of contemporary medicine across all involved stakeholders. It has led organizations and businesses across the healthcare industry to capitalize on the widening spectrum of healthcare-related data to improve patient care, manage the health system, understand and manage population and public health, and facilitate health research.

However, while the healthcare domain has been recognized as one of the most promising fields for the application of Big data, DDI in the healthcare domain is not without challenges. To address the complex dynamics, risks, and opportunities involved in the processing of personal data, and with an eye on resolving existing tensions between DDI and the protection of consumer privacy, the EU adopted the GDPR in 2016. This framework provides a unified and modern governance structure that protects fundamental rights in the digital age, including the right to data protection and the freedom to conduct business. It tackles the healthcare industry's need for increased data while ensuring privacy safeguards in the face of economic and social challenges.

To this end, the GDPR comprises a balancing test – it aims to guarantee the right to data protection while simultaneously strengthening and converging the economies within the EU internal market, thus fostering economic growth and innovation. However, it cannot be ignored that this balancing activity brings about a complex trade-off between these two objectives, where the lack of sufficient and effective data protection rules and enforcement may harm consumers' rights and trust – on the one hand –, and where too stringent protection regimes will unduly restrict commercial activities, increase administrative burdens for economic operators and ultimately stifle innovation. In this sense, DDI in the healthcare space might be highly contingent upon data protection regulation.

This thesis analyzes and discusses the impact of the GDPR on DDI in the healthcare industry, and then – on the basis of this assessment and analysis – aims to put forward empirically grounded considerations for future policy response considering ongoing developments in light of the European Data Strategy.

The key research question of this thesis is <u>"How does the GDPR impact data-driven innovation in the healthcare industry, and what considerations does this prompt for future policy response in light of the ongoing development of the European Data Strategy?"</u>

To answer this question, the first half of this thesis defines DDI in healthcare and its drivers (chapter 2), thereby emphasizing the potential opportunities and risks of (Big) data. It then explores the impact of data protection regulation on DDI, specifically in the healthcare industry (chapter 3). This thesis finds that although data protection regulation may spur social and market innovation, it also has the potential to hamper the development and functioning of certain DDBMs and technologies, contrary to what policymakers may have intended. As data protection regulation thus inevitably impacts the direction of innovation and economic growth, a balance is necessary between the economic and societal value created by the use of personal data for innovative ends and the need to safeguard individuals' privacy in such cases.

The second half of this thesis provides an analysis of the account for data processing activities in the healthcare industry under the framework of the GDPR (chapter 4), thereby highlighting concerns regarding the lack of definitional clarity around the concept of *(Big) health data* under the GDPR, the framework's extensive scope and strict obligations for all relevant market players, and the

considerable ambiguity of the GDPR's further provisions pertaining to the processing of health data for clinical and research purposes. The impact of the GDPR on DDI in healthcare is then assessed using a two-stage research approach: desktop research in the form of a review of the literature and legislation, and qualitative research on the basis of semi-structured interviews (chapter 5). This thesis finds that the GDPR has impacted the DDI landscape in healthcare across four key focus points, namely:

- Awareness, trust, and level playing in the context of the GDPR;
- Ambiguity in the definitional demarcation and scoping under the GDPR;
- Workability of substantive provisions under the GDPR; and
- Fragmentation in the legal framing of (Big) health data processing.

The final part of this thesis punts these findings into perspective by offering a preliminary discussion of policy considerations directed toward the EC, national regulators, and European and national DPAs in light of ongoing regulatory efforts at the EU level in relation to DDI in the healthcare domain, in particular the EHDS and the AIA (chapter 6). As such, this thesis puts forward five policy considerations namely:

- Streamline the patchwork of DDI-related regulations and oversight bodies in healthcare;
- Facilitate a level playing field for compliance through a maturity-based approach;
- Overcome regulatory ambiguity through legal design and concrete guidance;
- Account for national interests in the move toward a European health ecosystem; and
- Clarify the balancing of public and private interests in data sharing for healthcare purposes.

Regulating DDI in the healthcare sector is crucial in today's fast-paced environment with complex data ecosystems and increasingly sophisticated digital technologies. Though recent EU-level regulatory initiatives reflect the importance of managing these factors, effective regulation requires considering all interests at stake, with trust being a key aspect in this regard. To fully benefit from DDI in healthcare, future regulations must strike a balance that considers all interests and promotes trust through a human-centered, responsible, practical, and context- and case-dependent approach.

Main findings

While data has come to be considered the new oil of the digital age, its use for innovation purposes has raised much concern in relation to the protection of individuals' right to privacy and data protection. In the healthcare domain, the opportunities and challenges of data exploitation for innovation purposes are even further exacerbated, as data may offer the key to life-saving treatments while also requiring the processing of often highly sensitive patient information to reach such achievements in the first place.

Through the adoption of the GDPR, the EU aimed to address this challenging environment by offering individuals a mechanism for control over their personal data, providing trust in the digital economy, and harmonizing data protection throughout the EU to facilitate an EU single market in which data can flow freely across borders. As such, the GDPR aims to strike a balance between data protection and economic growth and innovation within the EU.

However:

(a) Despite being recognized as a comprehensive and forward-looking legislation designed to tackle data protection challenges in the digital era, there are doubts about the extent to which the GDPR has achieved its dual objective in the healthcare sector.
(b) While the GDPR comprises an extensive framework covering both substantive and procedural provisions for data processing activities in the healthcare context, concerns have been raised as to its lacking definition for 'Big health data', its wide-ranging scope, and its stringent yet oftentimes ambiguous obligations for market players.
(c) In practice, the GDPR has impacted DDI in healthcare across four key focus points, both procedural and substantive in nature, including the lack of awareness, trust, and a level playing field, ambiguity in defining and scoping health data, the workability of its substantive provisions, and the fragmented legal framing of (Big) health data processing within the EU.

Further:

(a) Recognizing the significance of DDI and its potential for success in the data-agile economy, the EC formulated a strategy to foster the EU data economy. Building upon the Data Act and Data Governance Act, the healthcare industry has more recently been introduced to the proposal for the EHDS. Moreover, though not directly incorporated into the EU Data Strategy, another regulatory framework relevant to the healthcare sector is the proposal for the AIA.
(b) As the introduction of these new regulatory frameworks is likely to complicate further the regulatory framing of the DDI scene in healthcare, it is important for regulators and policymakers to consider streamlining and harmonizing existing and upcoming regulations and oversight bodies in healthcare, establish fair compliance standards based on organizational maturity, provide clear guidance to address regulatory ambiguity, consider national interests in the development of a European health ecosystem, and achieve a balanced approach to data sharing for healthcare purposes in light of public and private interests.
(c) To ensure the realization of the economic and societal benefits of DDI in healthcare, upcoming regulatory efforts must strike a balance that considers all interests involved and balance the trust of individuals and organizations alike in a human-centered, responsible, practical, and context- and case-dependant manner.

1. Introduction

This chapter provides an introduction to the topic of this thesis, which focuses on the impact of the European General Data Protection Regulation (GDPR) on data-driven innovation (DDI) in the healthcare industry. It first introduces the challenges faced by regulators in finding an adequate balance between protecting individuals' informational privacy and benefitting from the economic and societal advantages of DDI. It also defines the scope of the research as well as the research question and objectives central to the thesis. Moreover, this chapter elucidates the methodology used for the current research, presents the sub-questions to be answered, and describes the structure of the thesis.

1.1. Setting the stage

'It is difficult to imagine the power that you're going to have when so many different sorts of data are available.'[1]

Since the inception of the Internet in the 1960s and the introduction of the World Wide Web in the late 1980s, digital technologies and services have transformed our society and daily lives. The rapid digitization of society and the swift progression toward a digital economy is fueled by the mass-scale gathering and deployment of personal data and the exploitation of Big data with the aim of generating value (Hartmann et al., 2016). While precise numbers on data collection, generation, and storage are unavailable, back in 2013 9.57 zettabytes[2] of data were estimated to have been processed by enterprise servers across the globe (Deloitte, 2013). Moreover, at the level of the EU, in particular, the volume of data produced also continues to grow, from 33 zettabytes generated in 2018 to an estimated 175 zettabytes by 2025 (EC, 2022b).

Acknowledging the potential of data for economic growth and societal prosperity, organizations have capitalized on data-driven business models (DDBMs). In the EU alone, the data economy was valued at EUR 300 billion in 2016, and it was estimated to increase by almost 250% – to EUR 739 billion – in 2020 (Deloitte, 2013). While the benefits abound, however, the processing of personal data for innovation purposes may be at odds with existing privacy expectations, bringing about complex challenges for individuals, groups, and societies as a whole, as has been confirmed by earlier studies (Warc, 2013; Kim et al., 2020). In light of these concerns, governments worldwide have recognized the need to address the economic and societal challenges associated with large-scale data processing activities. Among these challenges and risks, the Organisation for Economic Co-operation and Development (OECD) has included the following: barriers to the free flow of data; market concentration and competition barriers; and privacy violation and discrimination (OECD, 2015). At the EU level, regulatory instruments, including the GDPR, aim to tackle these challenges. The GDPR – adopted in 2016 and entered into force in 2018 – seeks to provide individuals with control over their personal data, provide trust in the digital economy, and harmonize data protection throughout the EU pursuant to the Digital Single Market strategy.[3] To this end, it aims to strike a balance between data protection, economic growth, and innovation in the EU internal market.[4]

[1] This statement was made by Tim Berners Lee in 2007. Sir Tim Berners-Lee (June 8, 1955, London, England) is a British computer scientist who is generally credited as the inventor of the World Wide Web, the leading information retrieval service of the Internet.

[2] A zettabyte is equivalent to a trillion gigabytes.

[3] The Digital Single Markets Strategy aims to ensure improved access to online goods and services across the EU for consumers and businesses. This is done, for instance, by removing barriers to cross-border e-commerce and access to online content while also increasing consumer protection. *See* https://ec.europa.eu/eurostat/cache/infographs/ict/bloc-4.html#:~:text=The%20Digital%20Single%20Market%20strategy%20seeks%20to%20ensure%20better%20access,content%20while%20increasing%20consumer%20protection. Accessed on 31 March 2022.

[4] *See* recital 2 of the GDPR.

Nevertheless, it should not be left without mention that balancing the objectives of data protection and innovation presents a complex trade-off. While many organizations have experienced rapid growth through data exploitation, their future development might be highly contingent upon data protection regulation (Martin et al., 2019). However, so far, limited research exists on the effects of data protection laws, such as the GDPR, on DDI, particularly in the context of the EU data economy, and further efforts toward building a single market for data. Previous studies suggest that privacy regulations can both stimulate and constrain innovation (Martin et al., 2019), with stringent regulations potentially damaging economic market structures (Deloitte, 2013; Campbell et al., 2015) while at the same time offering a means to restore trust in the digital economy (Economist, 2018) and drive organizations to capitalize on efficiencies, thereby fostering new products and markets.[5]

In June 2020, the EC published an evaluation report on the GDPR (EC, 2020a). While acknowledging the positive impact of the GDPR on the EU technological innovation landscape, the report also highlights how it has not fully succeeded at harmonizing data protection policy regimes across the EU, leading to challenges for cross-border business and innovation. Moreover, the report points to the tendency of Data Protection Authorities (DPAs) and the European Data Protection Board (EDPB) to put forward an overly restrictive interpretation of the GDPR, in some instances going against the letter and spirit of the framework's text and relevant case law (Digital Europe, 2020). Consequently, DDI in Europe is considered risky, and investments are oftentimes hampered. As Goldfarb and Tucker (2012) highlight in this regard, "Privacy concerns are thus no longer limited to government surveillance and public figures' private lives. The empirical literature shows that privacy regulation may affect the extent and direction of data-based innovation. (...) We therefore argue that digitization has made privacy policy a part of innovation policy" (Goldfarb & Tucker, 2012).

Despite ongoing debates on data protection regulation's appropriate level of strictness, there is limited scholarly research on the impact of such regulation on the DDI landscape in general and in specific industries, as well as the policy response this ought to prompt (Morlok et al., 2018). This knowledge gap extends to the EU context, where there has been little systematic examination of the interaction between EU regulation, including the GDPR, and DDI (Christensen et al., 2013; Pelkmans & Renda, 2014; London Economics, 2017).

1.2. Research scope and objectives

Earlier research has highlighted that the impact of regulation on innovation varies depending on the specific characteristics of the regulation and the industries involved (Pelkmans & Renda, 2014; Blind, 2016; Martin et al., 2019). DDI is now a crucial aspect across various sectors, including healthcare, which has recently undergone significant digital transformation. The combined use of personal data – including health data – or Big data and data analytics technologies (BDA) have come to offer unprecedented opportunities to improve the outcomes of contemporary medicine and has led organizations across the healthcare industry to recognize that DDI is fundamentally necessary to improve patient care, manage the health system, understand and manage population and public health, and facilitate health research (OECD, 2015; Harvard Business Review Analytics Services, 2019).

Despite recognizing the importance of increased access to personal data for healthcare improvement, however, DDI in the healthcare domain is not without challenges. Concerns around data security, privacy, governance, and compliance broaden the gap between the perceived importance of managing health data and the current level of maturity in organizations to do so (Harvard Business Review Analytics Services, 2019). In addition to traditional patient data, healthcare providers now seek access to a wider range of data, including social determinants of health like education, income,

[5] The practice of capitalization on overlooked efficiencies is often referred to as the *Porter Hypothesis. See* Porter & van der Linde (1995), Enzmann & Schneider (2005), and Blind (2012).

and housing, to gain valuable insights (Harvard Business Review Analytics Services, 2019). Although data processing activities by organizations across all industries require careful consideration of privacy risks, the collection and processing of sensitive medical and other information for advancing medicine present unique challenges in balancing individuals' privacy and the need for DDI in healthcare. Bearing this all in mind, this thesis analyzes the impact of the GDPR on DDI in the healthcare industry and provides empirically grounded considerations for future policy response, taking into account ongoing developments in light of the European Data Strategy.[6] By focusing on the industry-specific impact of the GDPR on DDI, this thesis contributes to the existing literature on the economics of privacy and regulation, offering insights for policy discussions.

1.3. Research questions

The primary research question this thesis focuses on is as follows:

RQ(main)	*How does the GDPR impact data-driven innovation in the healthcare industry, and what considerations does this prompt for future policy response in light of the ongoing development of the European Data Strategy?*

In answering this question, the following sub-questions will be analyzed:

RQ(sub) 1:	*What does data-driven innovation entail and how does this translate to the healthcare industry?*
RQ(sub) 2:	*How does (data protection) regulation affect data-driven innovation more generally and in the healthcare industry specifically?*
RQ(sub) 3:	*To what extent does the GDPR address data processing activities in the healthcare industry?*
RQ(sub) 4:	*How does the GDPR impact data-driven innovation in the healthcare industry?*
RQ(sub) 5:	*What considerations does this prompt for future policy response in light of ongoing regulatory efforts at the EU level?*

1.4. Methodology

The thesis relies on a two-stage research approach consisting of:

I. Desktop research in the form of a review of the literature and legislation; and
II. Qualitative research on the basis of semi-structured interviews.

The desktop research consists of a review of the existing literature and legislation, in particular, the GDPR and – where relevant – other EU legislative instruments and proposals (e.g. the recent legislation and legislative proposals by the EC in light of the European Data Strategy and the European approach to Artificial Intelligence (AI)). Furthermore, this thesis examines commentaries by the European institutions on the GDPR which assist in answering the above research question and subquestions. Finally, the literature reviewed for the purposes of this thesis pertains to the economics

[6] The European data strategy aims to make the EU a leader in a data-driven society and enable innovative processes, products, and services through the creation of a single market for data. The main (proposed) legislative frameworks that form part of this strategy and will, where relevant, be examined in this thesis are the Data Governance Act and the Data Act. *See* https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_en. Accessed on 9 August 2022.

of privacy and regulation, including sources published as part of academic legal research, general media, press releases, public communications, (government and industry) reports, briefings, and conferences. All literature and legislation have been sourced from publicly accessible sources on the Internet, and from online academic repositories; as well as books and articles available at the Leiden University Library and privately held. In this regard, a variety of search strings were used (for instance, “privacy and innovation”, “Data-driven innovation and regulation”, “GDPR impact on innovation”, “GDPR effect on healthcare innovation”, and “ data-driven innovation in healthcare and GDPR”).

The qualitative research is conducted through semi-structured interviews with 5-10 experts from two different stakeholder groups selected on the basis of their expertise and experience in the field of data-driven healthcare innovation in a position responsible for various aspects surrounding digitization, thereby ensuring a high level of quality of the research results. A more elaborative overview of this methodology is provided in chapter 5 of this thesis.

1.5. Structure of the thesis

This thesis is structured as follows:

Chapter 2 answers the first sub-question of the thesis. It defines DDI and its application in healthcare, followed by an explanation of its working and the ecosystem it is made up of. Moreover, this chapter highlights some of the concerns that have been raised in light of recent and continuing developments around (Big) data.

Chapter 3 answers the second sub-question. It seeks to bring into view how data protection regulation affects DDI in the healthcare domain by defining the practice of regulation and exploring the DDI-enabling and constraining effects of data protection regulation as a form of social regulation.

Chapter 4 provides an answer to the third sub-question. It analyzes the account for (Big) health data processing under the GDPR, thereby offering a definitional clarification in relation to (Big) health data and presenting the GDPR’s approach toward data processing activities in healthcare.

Chapter 5 of this thesis aims to answer the fourth sub-question through an exploration of the practical impact of the GDPR on DDI in healthcare. To this end, it presents the findings following a literature review and stakeholder interviews, discussing their perspectives on GDPR-related challenges and opportunities.

Chapter 6 answers the final sub-question by offering a preliminary discussion of the necessary considerations for future policy response considering the ongoing developments in light of the European Data Strategy.

The thesis then concludes by answering the main research question – How does the GDPR impact data-driven innovation in the healthcare industry, and what policy response should this prompt in light of the ongoing development of the European Data Strategy?

2. Data-driven innovation in healthcare: definitions, workings, and implications

This chapter provides an overview of DDI and its implications in the healthcare industry. It addresses the question of what DDI is and translates this to the healthcare sector. As such, this chapter answers subquestion (i) of the thesis, namely: What does data-driven innovation entail and how does this translate to the healthcare industry? Section 2.1. defines DDI, its objectives, and its application in healthcare. It also discusses traditional innovation processes and the potential of (Big) data in driving innovation. This is followed by an examination of the concerns associated with (Big) data, particularly in the healthcare context, in section 2.2.

2.1. Defining data-driven innovation and its application in healthcare

Innovation is crucial for economic growth and prosperity, and has the potential to impact the day-to-day lives of individuals globally (Kusiak, 2009). To benefit from innovation-driven efforts, organizations must recognize that innovation is not merely an outcome but also a process and a mindset (Kahn, 2018). While the importance of all three of these elements of innovation is to be acknowledged, this thesis specifically focuses on innovation as an outcome, particularly product or service innovation, as the use of (Big) data aims to improve and develop new products, processes, methods, and markets.

Innovation occurs after market acceptance and can be categorized as market innovation or social innovation (Stewart, 1981). While market innovation benefits organizations financially through product or process improvements that result in market sales, social innovation creates broader benefits for society. While this thesis does not delve into a detailed analysis of these types of innovation, it recognizes their importance because regulation affects them differently, as explained in chapter 3.2. of this thesis.

Many theories have been developed that shed light on the characteristics that influence consumer acceptance of innovations, among which the so-called Innovation Diffusion Theory (IDT) by Rogers (1995). Roger's IDT offers insights into the factors that influence consumer acceptance and adoption rates of innovations and identifies five variables that affect adoption rates, as shown in Table 2.1.

Innovation Diffusion Theory	
Attribute	*Explanation*
Relative advantage	The degree to which an innovation is perceived as being better than the idea it supersedes.
Complexity	The degree to which an innovation is perceived as relatively difficult to understand and use.
Observability	The degree to which the results of an innovation are visible to others.
Compatibility	The degree to which an innovation is perceived as consistent with the existing values, past experiences, and needs of potential adopters.
Trialability	The degree to which an innovation may be experimented with on a limited basis.

Table 2.1. Innovation Diffusion Theory (Rogers, 1995).

Although it goes beyond the scope of this thesis to further elaborate on the IDT, it is important to note that while the IDT has been effective in explaining the factors influencing the adoption of traditional innovations, it falls short when the nature of innovation changes, as in the case of DDI. More recent research has focused on acceptance determinants for information technologies, particularly regarding perceived security and privacy violations (Dillon & Morris, 1996; Venkatesh et al., 2003; Alabdulkarim et al., 2012). Where consumers do not merely benefit from innovation but also become strongly intertwined in the innovation process itself, acceptance thus does not solely depend on whether their needs and value expectations are met in an economic sense, but also on trust and alignment with core values and rights. This also applies to the DDI landscape in the healthcare domain, where successful innovations rely on usability and desirability, as well as trust and concerns related to the handling of personal data (Jirotka et al., 2005; Kelly & Young, 2017; Allain, 2022).

While innovation has traditionally been consumer-driven, perspectives from domain experts, legacy materials, and product life-cycle data should be considered too (Kusiak, 2009). In this sense, it is clear that knowledge serves as the foundation for innovation (Kusiak, 2009), and it is precisely in the context of the dynamics of knowledge-based organizations that the value of data has become evident (Choo, 1996). In the healthcare domain too, the potential of data has been recognized, offering significant opportunities for health management by providing quantitative foundations for pharmaceutical trials, medical studies, public health programs, pandemic response, and overall measurement of individual health (Condry & Quan, 2021). Shifting away from episodic interventions to focusing on prevention and effective management of chronic conditions, the opportunities of data have been embraced as a determining force for the successful adaptation of the healthcare domain to this new reality, with healthcare technology investments disproportionately focussing on — among other things — data analytics, including data mining, in order to make improved clinical and other health-related decisions (Raghupathi, 2016; Singhal et al., 2020).

Data, as defined by Stone and Wang (2014), enables informed decision-making, replacing reliance on instinct alone. It can be categorized into various groups, including Big data, which has emerged as a new production factor akin to hard assets and human capital (Cavanillas et al., 2016). Big data is characterized by high volume, velocity, variety, variability, and veracity, necessitating new processing methods for improved decision-making, insight discovery, and process optimization (Laney, 2001; Garlasu, 2013; Chen et al., 2014; Gandomi & Haider, 2015; Hashem et al., 2015; Rodríguez-Mazahua et al., 2015; Cavanillas et al., 2016; Yaqoob et al., 2016). The combination of these characteristics empowers organizations to automate processes, experiment with, and drive the creation of, new products and business models at an unprecedented speed (OECD, 2015). The ability of organizations to extract value from very large volumes and sorts of data by enabling high-velocity capture, discovery, and/or analysis, has led to the widespread adoption of a data-driven approach to innovation, known as DDI, which should be understood as "the value from using any kind of data to innovate" (Stone & Wang, 2014). Bearing this in mind, nowadays the term *Big data,* as such, is frequently used by major players across various industries globally to describe very large and diverse data sets including structured, semi-structured, and unstructured data with different attributes, in different sizes and from widely differing sources collected by organizations and mined to enable them to gain richer and deeper insights and an overall competitive advantage (Sagiroglu & Sinanc, 2013). In the 21st century, Big data has thus emerged as a driving force for innovation, enabling organizations to measure and improve their decision-making, efficiency, and performance (Manyika, 2011; McAfee et al., 2012; Hemerly, 2013). Recognizing the importance of Big data for survival and competitiveness, many organizations are now building their core business around its utilization (OECD, 2015; Cavanillas et al., 2016).

As the costs of healthcare continue to increase globally and exceed the ability of governments to provide compensation, Big data, and advanced data analytics tools have continued to gain unprecedented importance, more accurately determining linkages between risk factors and diseases and enabling substantial efficiencies (Raghupathi and Raghupathi, 2014). Historically, the healthcare industry has processed large amounts of data as a result of record-keeping, compliance efforts in relation to regulatory requirements, and patient care (Raghupathi, 2016). Beyond their volume, these large amounts of data — also referred to as "Big health data" — include a wide diversity of data types and varying speeds at which they must be managed (Olaronke and Oluwaseun, 2016; Raghupathi, 2016). In the healthcare domain, Big data thus refers to large and complex electronic health data (*see* figure 2.1) that are challenging to process, distribute and analyze using traditional methods (Raghupathi, 2016; Olaronke and Oluwaseun, 2016; Alexandru et al., 2016; Abouelmehdi et al., 2018). In the data-driven environment, organizations often lack the necessary resources and expertise to manage such large and diverse datasets alone. As a result, they engage with various internal and external actors to navigate this complexity successfully. Moore (1996) defined this collaborative network of organizations and individuals as a business ecosystem, where value creation is enabled through resource exchange and collaboration (Moore, 1996; Adner, 2006; Kim et al., 2010). In the healthcare industry, this ecosystem comprises a diverse range of stakeholders, such as hospitals, clinics, insurance companies, and other health-related organizations, working together to deliver high-quality, affordable healthcare to patients (Wu et al., 2019). This collaborative effort has offered the healthcare industry unprecedented opportunity and potential to support a wide range of medical and healthcare functions, including clinical decision support, disease surveillance, and population health management (Raghupathi and Raghupathi, 2014). In other words, the (continuously increasing) availability of Big data in healthcare and the deployment of BDA have allowed for the discovery of associations, patterns, and trends within the inherent complexity of this data, and to come to actionable insights for smarter decision-making (Alexandru et al., 2016; Raghupathi and Raghupathi, 2014).

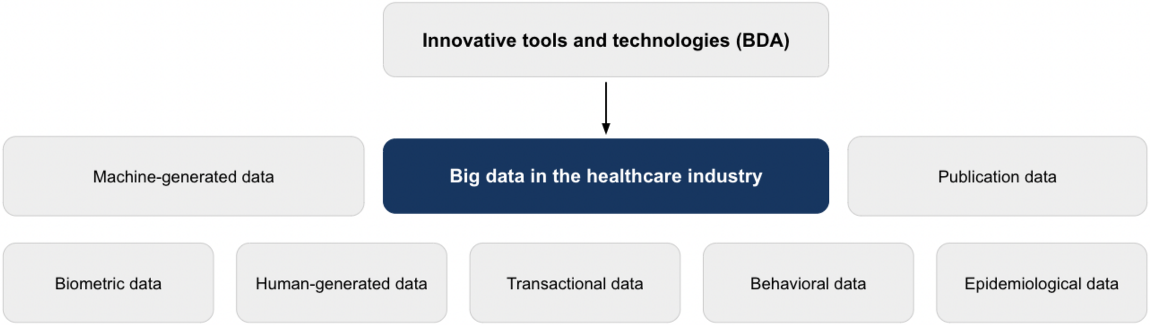

Figure 2.1. Conceptualizing Big data in healthcare (adapted from Olaronke and Oluwaseun, 2016).

2.2. Concerns surrounding (Big) data

In the digital economy, data has become the driving force behind economic growth and innovation. The application of Big data technologies has particularly sparked excitement in various fields, including healthcare, where there is a wealth of data to be stored, processed, and analyzed (Buhl et al., 2013). This availability of Big data and the emergence of business analytics ecosystems present new opportunities for innovating traditional business models (Ferreira et al., 2021), including in healthcare. However, along with the positive transformations, the increasing role of Big data also brings significant challenges and consequences to society.

Big data often capture personal information of individuals, which is increasingly harvested, aggregated, and analyzed by both private and public sectors to gain valuable insights (Bunnik et al., 2016). This enables organizations to gather more information about individuals, understand their behavior, and use these insights for personalized interactions (Sætra, 2019). This process of mining personal data for economic gain through personalization and behavioral modification has more popularly been termed *surveillance capitalism* (Zuboff, 2019). Defined by Zuboff (2019) as "a new economic order that claims human experience as free raw material for hidden commercial practices of extraction, prediction, and sales", the exploitation of Big data has become a cause for serious concerns surrounding — among other things — the misuse of personal information, breaches of privacy and data protection, profiling of individuals and discrimination (Wigan & Clarke, 2013; Markus, 2015; Zuboff, 2015; Clarke, 2016; Van Dijck et al., 2016; Martin, 2020). Tying this to the healthcare industry, integrating diverse health data into Big data presents challenges related to security and privacy issues (Alexandru et al., 2016; Olaronke and Oluwaseun, 2016). These and other unintended, and potentially negative consequences of Big data at various levels (individual, organizational, and societal) have been brought into perspective by Asadi Someh et al. (2016) as depicted in table 2.2. below.

Big data: individual, organizational, and societal concerns	
Level of concern	*Concerns*
Individual issues	Data Ownership Data Control Awareness Trust Privacy Self-Determination Fear
Organizational issues	Competitive Pressure Data Quality Data Sourcing Data Sharing/Disclosure Algorithmic Decision Making Presentation Ethical Capability Ethical Culture Ethical Governance Ethical Performance Reputation
Societal issues	Power Dependence Social awareness Surveillance Principles and Guidelines Authority Climate

Table 2.2. Individual, organizational, and societal concerns resulting from Big data analytics (adapted from Asadi Someh et al., 2016).

It follows from this that organizations relying on Big data, especially in healthcare, face a paradoxical tension between the positive and negative consequences of their disruptive business models. To succeed in DDI, healthcare organizations must address these challenges and establish a well-defined strategy, including clear privacy and data protection strategies compliant with existing laws and regulations (Zillner et al., 2016).

3. The effects of (data protection) regulation on data-driven innovation

This chapter explores the impact of (data protection) regulation on DDI and applies these findings analogously to the healthcare domain. As such, this chapter answers subquestion (ii) of the thesis, namely: How does (data protection) regulation affect data-driven innovation? Section 3.1. defines regulation, its societal role, and modalities, emphasizing social regulation in line with the topic and scope of this thesis. This is followed by an examination of the effects of social regulation on DDI, highlighting enabling and constraining factors, with a focus on data protection regulation in section 3.2.

3.1. Defining regulation, its drivers, and objectives

Regulation has gained significant attention across various disciplines due to increased global activities and the involvement of international organizations (Baldwin et al., 2011). However, a universally accepted definition of regulation is still lacking, leading to a wide range of interpretations and concepts (Baldwin et al., 1998). Generally, regulation is seen as a form of coercive rule-setting that encompasses governmental and non-governmental actions to supervise market activity and the behavior of economic actors (OECD, 1997; Baldwin et al., 2011).

In light of the topic of this thesis — which focuses on the GDPR as a source of regulation —, the scope of this research is limited to *regulation* understood as a specific set of commands.[7] Within this form, there are distinct phases: agenda-setting, legislation, compliance, and enforcement. Although the agenda-setting phase and legislation phase each impact the innovation cycle in their own way, this thesis focuses exclusively on the compliance phase of regulation. In this phase of regulation, targeted stakeholders are expected to have put in place the necessary mechanisms to comply with the given set of rules, and the extent to which compliance burdens result from such regulation may alter the overall expected benefit from the innovative activity (Pelkmans & Renda, 2014).

Regulators intervene through regulation for various reasons, and it is important to differentiate between their motives and the technical justifications they rely on. While regulators may have different motives, those acting in the public interest typically base their interventions on technical justifications. One common justification is the market failure rationale, which supports regulatory intervention when an unregulated market fails to align with public interests (Baldwin et al., 2011). Bearing this rationale in mind, scholars and practitioners generally recognize and distinguish between three types of regulation, all of which have effects on innovation (OECD, 1997). These are:

- **Economic regulation**, which aims to enhance market efficiency by overseeing and guiding market competition;
- **Administrative regulation** which concerns general government management of public and private sector operations; and
- **Social regulation** which imposes requirements on organizations to protect the welfare, well-being, and rights of society in various domains, including health, safety, the environment, and social cohesion (OECD, 1997).

This thesis focuses on social regulation, which aims to maintain a balanced relationship between economic progress and societal well-being. This is achieved by internalizing societal costs (externalities) resulting from the pursuance of economic interests and by making compliance

[7] The GDPR qualifies as a regulation under EU law. Under article 288 of the Treaty on the Functioning of the European Union (TFEU), the EU institutions shall adopt regulations, directives, decisions, recommendations, and opinions to exercise the Union's competencies. This article further stipulates that EU regulations shall have general application, shall be binding in their entirety, and shall be directly applicable in all EU Member States. In this sense, the GDPR qualifies as a binding set of rules established in accordance with EU law, which ought to be applied in accordance with its material and territorial scope, and the compliance with which is overseen by dedicated national supervisory authorities.

mandatory for relevant actors (Litan, 2021). While typical examples of social regulation include environmental and consumer protection, privacy and data protection have also come to be grouped under this classification (Martin et al., 2019).

Privacy is a recognized human right, though its meaning has been ambiguous and diverse (Hoofnagle et al., 2019; Westin, 1968). To more clearly conceptualize privacy, Koops et al. (2016) established a comprehensive typology of privacy covering eight separate dimensions that are protection-worthy, even under conditions of increased digitization (*see* figure 3.1). However, informational privacy, which is closely linked to all other dimensions, has gained prominence in the EU's efforts to enhance protection in the digital age (Hoofnagle et al., 2019; Westin, 1968).

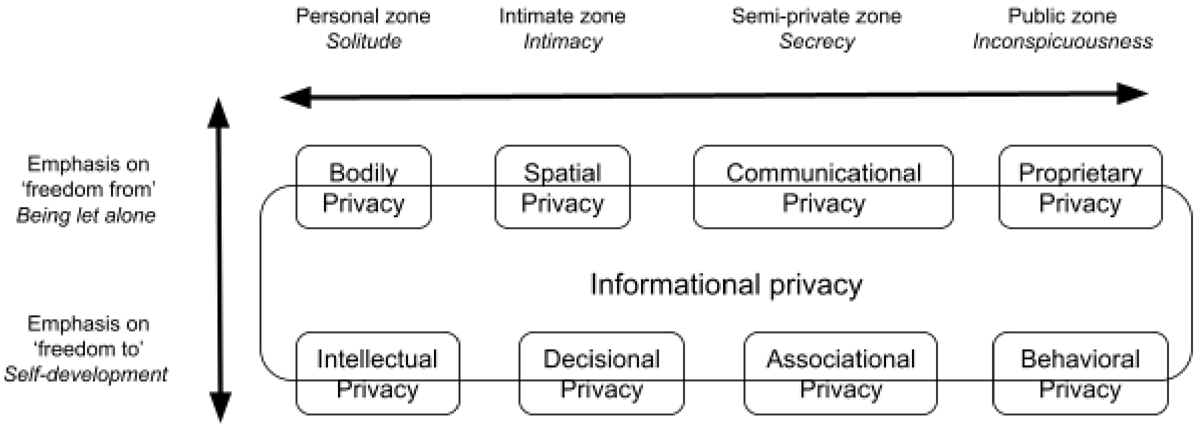

Figure 3.1. Different dimensions of privacy (Koops et al., 2016).

While the rights to privacy data protection are closely related, they are legally distinct (Gellert & Gutwirth, 2013; CoE, ECtHR, EDPS, EUAFR, 2018). In Europe, the right to privacy emerged in international human rights law before the information society came about. To address the processing of personal data through new technologies, new rules were necessary, leading to the rise of the concepts of "informational privacy" and the "right to informational self-determination".[8] In the EU, the development of these rules began in the 1970s and resulted in the inclusion of the right to data protection in the EU Charter of Fundamental Rights (EUCFR) and the adoption of the GDPR. These developments highlight the recognition of data protection as a distinct value and separate right that is not subsumed by the right to privacy.

As such, data protection law aims to safeguard individuals' data by regulating its legitimate processing. It protects against unauthorized access, criminal activities, and unlawful handling of personal data. This is achieved by mandating IT security and extensive process controls, and by putting in place (severe) penalties for non-compliance (Martin et al., 2019). In this sense, data protection regulation qualifies as a form of social regulation. However, complying with these regulations can have significant economic implications for organizations (Hoofnagle et al., 2019). Consequently, economic progress and social protection are interconnected, the effects of which — in particular concerning data protection regulation — on DDI will be discussed in the next section of this thesis.

[8] *See* Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland [GC], 2017, § 137, which states as follows: *"The protection of personal data is of fundamental importance to a person's enjoyment of his or her right to respect for private and family life, as guaranteed by Article 8 of the Convention. The domestic law must afford appropriate safeguards to prevent any such use of personal data as may be inconsistent with the guarantees of this Article (...). Article 8 of the Convention thus provides for the right to a form of informational self-determination, allowing individuals to rely on their right to privacy as regards data which, albeit neutral, are collected, processed, and disseminated collectively and in such a form or manner that their Article 8 rights may be engaged."*

3.2. The effects of data protection regulation on DDI in the healthcare industry

Data protection law, as a form of social regulation, has had a significant impact on the enforcement environment and market structure, influencing incentives for and against DDI. Discussions on the effects of regulation, including data protection regulation, on DDI are divided, with some seeing it as enabling desirable behavior and others viewing it as imposing burdens on economic and social activity (Baldwin, 2011). Research on the effects of data protection regulation on startup innovation reveals a variety of mixed effects driven by specific regulatory stipulations and their interaction with particular business models (Martin et al., 2019). In this sense, the impact of data protection regulation on DDI varies and should be assessed on a case-by-case basis, considering the balance between innovation-inducing and innovation-constraining factors (Pelkmans & Renda, 2014). Despite the increasing attention to data security, privacy protection, and data-driven strategies, systematic empirical research on the privacy-innovation conundrum remains limited (Saura et al., 2021). Focussing on existing literature on the relationship between innovation and regulation more broadly, however, may offer valuable insights from which to depart in this regard.

3.2.1. Social regulatory impact on innovation

The relationship between regulation and innovation is complex, multidimensional, ambiguous, and dynamic, with effects observable throughout the innovation cycle (Pelkmans & Renda, 2014). Innovation is driven by the willingness, opportunity, and capability of organizations' management to partake in this activity, all of which can be influenced by regulation in two competing ways (Ashford, 2000; Pelkmans & Renda, 2014; Stewart, 2010). Firstly, compliance burdens can divert resources away from innovation, and secondly, organizations may adapt or circumvent regulations to align with their innovative pursuits (Stewart, 2010).

More specifically, Stewart (2010) identifies three dimensions of innovation affected by regulatory interventions: flexibility (i.e. the number of possible routes for implementation that organizations may have available for compliance), stringency (i.e. the extent to which new regulations require compliance innovation or impose compliance burdens on a firm, industry or market), and information (i.e. the extent to which regulation provides information and transparency in the market). Moreover, he highlights the impact of regulatory uncertainty before the enactment of regulations as a factor that may have mixed effects on innovation (Stewart, 2010). The findings following hid extensive cross-industry literature review on the impact of regulation on innovation in the US broadly suggest that the impact of regulation on innovation depends on whether compliance innovation is required. While regulation without compliance innovation can stimulate circumventive practices but hinder overall innovation, regulation that requires compliance innovation has a more nuanced impact, with social regulation increasing social innovation but decreasing market innovation. In the end, the actual impact on innovation remains ambiguous, dependent on factors such as administrative and compliance burdens, timing, flexibility, and uncertainty (Pelkmans & Renda, 2014). In line with the findings by Ashford et al. (2000), stringency has the biggest impact on technological innovation and, therefore, deserves further attention in light of this thesis.

Stringency refers to the degree of behavioral or technological changes required for compliance with regulation. In this sense, social regulation may cause organizations to divert resources from other business activities toward compliance, potentially hindering unrealized innovations (Blind, 2012). As such, higher stringency increases compliance costs and may negatively impact innovative capacity (Renda et al., 2013). However, social regulation has also been recognized to stimulate innovation, a phenomenon known as the Porter Hypothesis (Ashford, 1976; Porter & Van der Linde, 1995). Focussing on environmental policy debates, the Porter Hypothesis holds that well-designed regulation can create a 'win-win' situation, fostering both social and market innovation, as long as the distance between such stringent regulation and the status quo is not excessive, and the outcome is specified in a technology-neutral and non-prescriptive way so as to allow experimentation in the compliance responses (Pelkmans & Renda, 2014). Social regulation may thus guide regulatees to innovate, leading to new technologies, products, and markets, and uncovering overlooked efficiencies to create so-called “regulation-exploiting” innovations (Porter & Van der Linde, 1995; Ambec et al., 2020). Moreover, compliance with these regulations may increase consumer acceptance and trust, since they can now rely on some minimum level of protection (Martin et al., 2019), facilitating the successful introduction and diffusion of innovation (Blind, 2012; Martin et al., 2019).

3.2.2. Mapping the data protection-innovation conundrum

The impact of regulation on innovation depends on specific regulations, industries, market characteristics, and timeframes during which the regulation has been applicable (Martin et al., 2019; Blind et al., 2017; Blind, 2016; Goldfarb & Tucker, 2012). This thesis specifically examines the influence of data protection regulation, particularly the GDPR, on DDI. While empirical evidence on this topic is limited, some general conclusions can be inferred from governmental, industry, and academic studies.

As is the case with social regulation more broadly, the perceived effects of data protection regulation on the innovative capacity of organizations are heterogeneous (Goldfarb & Tucker, 2012). On the one hand, it is argued that stringent data protection regulation hampers valuable innovation by increasing costs for organizations utilizing personal data and limiting potential benefits for consumers (Thierer & Hagemann, 2015). More specifically, previous research highlights that compliance costs disproportionately affect start-ups and small operators in the data-driven sector (Campbell et al., 2015). These higher costs may deter smaller organizations from investing in DDI, limiting their ability to introduce valuable products and services. Consequently, larger organizations may dominate markets, depriving consumers of potentially beneficial innovations.

On the flip side, and in line with the Porter Hypothesis, it has been argued that data protection regulation — rigid and encompassing in nature — can act as a driver for innovation. While acknowledging that data protection regulation may limit specific forms of data processing across a wide variety of industries, there is a growing recognition that balancing economic growth and societal implications is crucial in this regard (Van Lieshout, 2018; Van Lieshout & Emmert, 2018). Departing from the notion that privacy is a business asset, the RESPECT4U framework promotes privacy principles that view privacy as a catalyst for innovation, providing organizations with structured approaches to meet data protection requirements — in particular under the GDPR — in a systematic and structured manner (Van Lieshout, 2018).

In other studies, researchers acknowledge a shifting perspective on privacy and innovation, emphasizing the importance of consumer trust for data-driven businesses (Bachlechner et al., 2019; Bleier et al., 2020). In this sense, organizations increasingly adopt privacy-protecting tools and services to comply with regulations and build trust. This proactive approach not only enhances consumer trust but also fosters the development of PETs like anonymization and encryption, driving innovation (Bachlechner et al., 2020; Bleier et al., 2020). Consequently, privacy policies may stimulate regulation-exploiting innovation, depending on organizational capabilities and resources, ease of implementation, enforcement levels, and market demand (Martin et al., 2019).

In addition to this innovation-driven response to data protection regulation, the literature presents various conceptual frameworks of (data protection) regulation’s effects on organizations’’ innovation choices as depicted in table 3.1. below (Stewart, 2010; Fosch-Villaronga & Heldeweg, 2018; Martin et al., 2019).

Organizations’ innovative choices in relation to (data protection) regulation	
Organizations’ choice of action	*Description*
Product abandonment	The organization abandons the development as a consequence of prohibitive and definite regulatory restrictions and focuses on developments that face fewer regulatory restrictions.
Compliance innovation	The organization modifies its plans and innovates to ensure compliance while maintaining the core architecture and value proposition, such as implementing privacy-by-design principles.
Regulation-exploiting innovation	The organization leverages the regulation as an opportunity to develop innovative solutions that address the challenges it presents.
Deliberative innovation	The organization proceeds with the development while engaging in negotiations with regulators to revise the existing regulation for compliance without altering the intended design.
Strategic non-compliance	The organization intentionally violates relevant regulations and continues the development, risking potential penalties for non-compliance.
Circumventive innovation	The organization exploits regulatory loopholes to continue the development without being constrained by the regulation.

Table 3.1. Conceptual framework of (data protection) regulation’s effects on innovation choices.

Finally, Cohen (2013) argues that data protection regulation is essential for fostering innovation, as it provides the necessary checks and balances for market behavior and encourages critical reflection. She holds that innovation should not be seen as the absence of regulatory constraints and that without the necessary checks in place to steer variable market behavior, cultural and technical innovation cannot be achieved. According to this line of reasoning, the red-tape perspective on the relationship between privacy and innovation is incorrect because it fails to take into account the nature of innovation or the dynamic function of privacy (Frischmann, 2012). The impact of stringency on innovation thus depends on modulation rather than regulation itself. In this sense, data protection regulation is particularly crucial for driving innovation in the domain of Big data (Cohen, 2013), which is vital for maintaining a dynamic and just society, even if it does not necessarily align with commercial imperatives.

Bearing all of the above in mind, data protection regulation may thus spur social and market innovation, but it also has the potential to hamper the development and functioning of certain DDBMs and technologies, contrary to what policymakers may have intended. Data protection regulation inevitably impacts the direction of innovation and economic growth, and this interlinkage necessarily demands a balancing of economic value and privacy. Further research is needed to understand the specific effects of regulation in different industries and contexts (Goldfarb & Tucker, 2012; Martin et al., 2019). Bearing this in mind, the following chapters focus on the impact of the GDPR on DDI in the healthcare industry.

4. The GDPR's account for data processing activities in the healthcare industry

This chapter examines the account for data processing activities in the healthcare industry under the GDPR. As such, this chapter answers subquestion (iii) of the thesis, namely: To what extent does the GDPR address data processing activities in the healthcare industry? Section 4.1. provides an overview of the EU data protection roadmap and the transition from the 1995 Data Protection Directive to the GDPR. Section 4.2. then lays the basis for legal analysis by providing a definitional clarification in relation to (Big) health data under the GDPR. Finally, section 4.3. presents the GDPR's approach toward data processing activities in healthcare, explaining the GDPR's objectives, scope, and approach more broadly, followed by an assessment of its approach toward regulating (Big) health data processing more specifically.

4.1. A new EU data protection framework: from challenges to objectives

In January 2012, the EC proposed a new regulation on the protection of personal data to replace the 1995 Data Protection Directive (DPD). Reflecting existing data protection principles laid down in national laws of Member States and in Convention 108 by the Council of Europe, the DPD aimed to safeguard individuals' privacy rights while facilitating the free flow of personal data between EU Member States. Prior to the proposal, the EC conducted a review of the DPD in 2009, including public consultation and studies, to assess its adequacy in the digital age and to outline the approach for revision. Although the findings confirmed that the core principles of the framework are still valid and that its technology-neutral approach should be preserved, several issues were identified (EC, 2010), namely:

- A lack of clarity and specification for applying data protection principles to new technologies, requiring further clarification and awareness for data controllers.
- Insufficient harmonization between Member States' data protection legislation, leading to the need for more legal certainty and a level playing field.
- An unsatisfactory scheme for international data transfers, necessitating streamlining to simplify and facilitate such transfers.
- Weak institutional arrangement for effective enforcement, calling for a stronger role of DPAs, increased transparency, and clarification of tasks and powers.
- Absence of an overarching instrument covering data processing in all EU sectors and policies, emphasizing the need for an integrated and consistent approach to personal data protection.

Through the adoption of the GDPR, the EU addressed these issues, namely by developing "a comprehensive and coherent approach guaranteeing that the fundamental right to data protection for individuals is fully respected within the EU and beyond", in particular, in the light of "the challenges resulting from globalization and new technologies" (EC, 2010). In this sense, the objective was to create a modernized and consistent EU data protection framework, protecting fundamental rights and facilitating business in the digital age (CoE, ECtHR, EDPS, EUAFR, 2018). More specifically, with the new data protection framework, the EC pursued five key objectives: strengthening individuals' rights, enhancing the internal market, revising data protection rules in the judicial domain, clarifying the global dimension of data protection, and strengthening enforcement mechanisms.

4.2. Definitional clarification: (Big) health data under the GDPR

Health data are at the core of the Big data revolution (Tzanou, 2020). The observation of our physical state and performance through technologies is deeply embedded in our everyday lives, generating unprecedented amounts of data for continuous learning and improvement. Big health data analytics offers numerous benefits, such as improved healthcare quality, disease prevention, cost reduction, increased patient empowerment, and efficient healthcare services (Tzanou, 2020). As noted in chapter 2.1., Big health data analytics has offered the healthcare industry unprecedented opportunity and potential to support a wide range of medical and healthcare functions through the discovery of associations, patterns, and trends within the inherent complexity of the large quantities of data available, and to come to actionable insights for smarter decision making, facilitate medical research and encourage the development of innovative business models in the healthcare domain (Raghupathi and Raghupathi, 2014; EDPS, 2015; Alexandru et al., 2016; Tzanou, 2020). To grasp the impact of the GDPR on the processing of such data in the healthcare domain for innovation purposes, we additionally ought to understand how the GDPR approaches the definitional challenge of defining the concepts of 'health data' and 'Big health data'. With the adoption and entry into force of the GDPR, the EC first defined 'data concerning health' in the context of data processing activities and the consequent requirements under data protection law. In line with article 4(15) of the GDPR:

> *"data concerning health' means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status."*

Recital 35 of the GDPR expands upon this definition of health data by further explaining that personal data concerning health includes information about an individual's past, current, or future physical or mental health status.This encompasses data collected during registration for, or the provision of, health care services, unique identifiers for health purposes, test results from body parts or biological samples, and information about diseases, disabilities, disease risk, medical history, treatments, or physiological or biomedical state of the data subject obtained from healthcare professionals, hospitals, medical devices, or a medical device or an in vitro diagnostic test.

Furthermore, the GDPR defines 'genetic data'. In article 4(13) of the GDPR it is noted that:

> *"genetic data means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question."*

While acknowledging the broad definition of 'health data' under the GDPR, it is important to note the challenges it presents (Tzanou, 2020). Although a further elaboration on the definitional complexities surrounding (Big) health data under the GDPR goes beyond the scope of this chapter, it is important to stress that the implications of these definitional uncertainties can not be ignored when assessing the impact of the GDPR on DDI in the healthcare industry, nor can such an analysis be conducted without any definition in place in this regard. Bearing this in mind, for the purpose of this thesis *Big health data* is understood in line with the definition provided by Tzanou (2020), namely "an umbrella concept that covers broadly data generated from a variety of different sources and from which information about a person's health can be inferred".

4.3. The GDPR's approach toward data processing activities in healthcare

4.3.1. The GDPR: objectives, scope, and approach

The GDPR constitutes the core of EU data protection law, gaining global influence as a leading framework for personal data protection (De Ville and Gunst, 2021; Rustad and Koenig, 2019). Divided into eleven chapters[9] and accompanied by 173 (non-binding) recitals, it lays down rules for data

[9] These chapters broadly address data protection principles, data subject rights, obligations for controllers and processors, rules regarding Data Protection Authorities ('DPA'), procedures regarding cooperation and consistency, and provisions on remedies, liability, penalties, and rules relating to specific processing situations.

subjects' protection and the free movement of data within the EU.[10] Though largely preserving the core principles and rights laid down in the DPD, the GDPR brings improvements, clarifications, and new principles, rights, and obligations for data controllers, enhancing procedural aspects of data protection, including in the healthcare context.

Zooming in on its subject matter and objectives, the GDPR builds upon the DPD by recognizing the right to data protection as a fundamental right within the EU. It also extends the territorial scope of the EU data protection framework, covering the processing of personal data by controllers or processors, regardless of their location, if they are involved in activities related to EU establishments or offer goods/services to individuals in the EU or monitor their behavior.[11] In this sense, although the GDPR only protects data subjects within the EU, its practical impact is felt by organizations globally (Li et al., 2019).

The GDPR is a principles-based regulation that sets out six key principles for processing personal data: lawfulness, fairness and transparency, purpose limitation, data minimization, accuracy, storage limitation, and integrity and confidentiality.[12] It emphasizes accountability, ensuring that data controllers are responsible for and able to demonstrate compliance with these principles (Digital Europe, 2020). Article 5(2) explicitly introduces the principle of accountability, while Article 6(1) outlines the grounds for lawful processing, including consent, execution of a contract with the data subject, compliance with the law, protection of vital interests, the performance of a task carried out in the public interest or in the exercise of official authority, and legitimate interests.

As an omnibus regulation (Marelli et al., 2020; Tzanou, 2020), the GDPR primarily focuses on the relationship between data subjects[13] and data controllers[14] and enhances the rights of data subjects established in the DPD. These rights include the right to information[15], the right of access[16], the right to rectification[17], the right to erasure[18], the right to restriction of processing[19], the right to data portability[20], the right to object to certain types of processing[21], and the right not to be subjected to automated individual decision-making, including profiling[22]. Moreover, the GDPR enhances the responsibilities of data controllers by requiring them to implement and demonstrate compliance with technical and organizational measures.[23] Additionally, they may need to appoint a Data Protection Officer (DPO)[24] and report personal data breaches to the relevant DPA within seventy-two hours of discovering the breach, and the communication thereof to the data subject where there is likely to be a "high risk" to their rights and freedoms.[25]. Fueled by a risk-based approach, the GDPR furthermore obliges data controllers to conduct a Data Protection Impact Assessment (DPIA) “where a type of processing, in particular, using new technologies and taking into account the nature, scope, context, and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural

[10] *See* article 1(1) of the GDPR, article 2(1) of the GDPR, and article 3 of the GDPR.
[11] *See* article 3 of the GDPR.
[12] *See* article 5(1) of the GDPR.
[13] According to article 4(1) of the GDPR, a data subject is an identified or identifiable natural person. Under the GDPR, an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier.
[14] According to article 4(7) of the GDPR, a controller is a natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.
[15] *See* articles 13 and 14 of the GDPR.
[16] *See* article 15 of the GDPR.
[17] *See* article 16 of the GDPR.
[18] *See* article 17 of the GDPR.
[19] *See* article 18 of the GDPR.
[20] *See* article 20 of the GDPR.
[21] *See* article 21 of the GDPR.
[22] *See* article 22 of the GDPR.
[23] *See* article 24(1) of the GDPR.
[24] *See* article 37 of the GDPR.
[25] *See* articles 33-34 of the GDPR.

persons".[26] Additionally, it introduces the principles of 'data protection by design and by default'[27], emphasizing the need for effective safeguards and minimal data processing throughout the product or service lifecycle.

Finally, the GDPR expands upon the DPD by introducing principles for transferring personal data to third countries or international organizations[28], including appropriate safeguards, binding corporate rules, and international agreements.[29] Alongside these provisions, it also establishes conditions for imposing administrative fines and empowers national DPAs to enforce GDPR compliance.[30] In this sense, DPAs have various options for addressing non-compliance, such as issuing warnings, reprimands, temporary or permanent bans on processing, and imposing fines up to €20 million or 4% of a business's total annual worldwide turnover in the case of an infringement of the data protection rules.[31]

4.3.2. The GDPR's approach toward regulating (Big) health data processing

Beyond the definitional demarcation of *(Big) health data* discussed in chapter 4.2. above, the GDPR contains a number of further provisions pertaining to health data and health, as will be discussed in more depth in the paragraphs below.

Special categories of personal data and exemptions to health data processing

Article 9(1) of the GDPR prohibits the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation. As such, health data enjoys enhanced protection as a 'special category of personal data' under the GDPR. However, there are several exceptions to this prohibition, some of which relate specifically to the processing of health data. Interestingly, though, article 9(4) of the GDPR allows Member States to maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data, or data concerning health.[32]

Though conditioned by very high substantive and procedural requirements and subject to a certain level of discretion by Member States, where the data subject has given her 'explicit consent', the processing is in principle allowed.[33] In addition, the processing of health data is allowed when this is necessary to protect the vital interests of the data subject or another person unable or legally incapable of giving consent.[34] The prohibition on the processing of health data is also lifted if the data subject has made the data manifestly public, although the qualification of health data from mobile health apps in this regard remains debated (Tzanou, 2020). Moreover, the GDPR allows for the processing of health data where this is considered to be necessary for reasons of substantial public interest, where this is based on Union or Member State law and which is proportionate to the aim pursued, respects the essence of the right to data protection and provides for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject, though it remains

[26] *See* article 35(3)(a) of the GDPR.
[27] *See* article 25 of the GDPR.
[28] *See* article 44 of the GDPR.
[29] *See* articles 45-48 of the GDPR.
[30] *See* article 51 of the GDPR.
[31] *See* article 83 of the GDPR.
[32] In this sense, the GDPR exhibits characteristics of a directive, in the sense that in parts, member states are given powers and obligations to set further rules. In the Netherlands, for instance, that space was filled in, among other things, by the Uitvoeringswet Algemene Verordening Gegevensbescherming (UAVG).
[33] *See* article 9(2)(a) of the GDPR.
[34] *See* article 9(2)(c) of the GDPR.

unclear under the provisions of the GDPR what should be understood as 'substantial public interest' in any case.[35]

The GDPR also permits the processing of health data for specific purposes, including preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services".[36] This, however, requires the processing to be conducted by professionals bound by professional secrecy or by other individuals with a legal obligation to maintain secrecy.[37] In addition, the GDPR allows the processing of health data if this is necessary for archiving purposes, scientific research, historical research, or statistical purposes under Article 89(1). In this sense, scientific research purposes should also include studies conducted in the public interest in the area of public health, and special regard must be taken for the additional measures that must be taken in the interest of the data subject in accordance with the general rules of the GDPR.[38] With regard to the public health exemption, the term 'public health' should be understood as:

> *"(...) all elements related to health, namely health status, including morbidity and disability, the determinants having an effect on that health status, health care needs, resources allocated to health care, the provision of, and universal access to, health care as well as health care expenditure and financing, and the causes of mortality."*[39]

Finally, the GDPR permits the processing of health data for public health reasons, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular, professional secrecy.[40] Where this exemption applies, processing of health data may take place without the consent of the data subject although safeguards should be put in place to ensure that health data processed for reasons of public interest do not end up being processed for other purposes by third parties such as employers or insurance and banking companies.[41] Moreover, the processing of health data for public health purposes may involve restrictions to data protection principles, data subject rights, and the rules governing international transfers of personal data.[42] Lastly, the GDPR notes that there may be instances in which the processing of health data "may serve both important grounds of public interest and the vital interests of the data subject as for instance when processing is necessary for humanitarian purposes, including for monitoring epidemics and their spread or in situations of humanitarian emergencies, in particular in situations of natural and man-made disasters", such as was the case during the fight against the COVID-19 pandemic.[43]

Data Protection Impact Assessment and automated decision-making in relation to health data

The GDPR mandates a DPIA for processing activities that pose a high risk to individuals' rights and freedoms.[44] This includes cases involving the systematic and extensive evaluation of personal aspects relating to a data subject based on automated processing, including profiling – also in relation to a natural person's health –, and on which decisions are based that produce legal effects concerning

[35] *See* article 9(2)(g) of the GDPR.
[36] *See* article 9(2)(h) of the GDPR.
[37] *See* article 9(3) of the GDPR.
[38] *See* recital 159 of the GDPR.
[39] *See* article 3(c) of Regulation (EC) No 1338/2008 of the European Parliament and of the Council of 16 December 2008 on Community statistics on public health and health and safety at work (OJ L 354, 31.12.2008, p. 70).
[40] *See* articles 9(2)(i) and 35 of the GDPR.
[41] *See* recital 54 of the GDPR.
[42] *See* articles 23, 17(3)(c) , 45(3), 46, 29(1)(d), and 49(1)(f) of the GDPR. Also, see recitals 65 and 112 of the GDPR.
[43] *See* recital 46 of the GDPR.
[44] *See* article 35 of the GDPR.

the natural person or similarly significantly affect the natural person;[45] or in the case of processing on a large scale of special categories of personal data, among which health-related data.[46] As such, DPIAs are generally required for processing health data, unless the processing concerns personal data from patients or clients by an individual physician or other health care professional.[47]

Finally, the GDPR prohibits automated decision-making including profiling, that has legal or similarly significant effects on individuals.[48] In this sense, article 22(2)(c) of the GDPR adds to this that there are exceptions to this prohibition in cases where the data subject has given explicit consent for the processing. This exception, however, does in principle not apply where the automated decision-making is based on special categories of personal data, such as health data.[49] As noted above, where a data subject is subjected to fully automated decision-making processes, including profiling, that specifically analyzes or predict aspects regarding their health, the controller is obliged to conduct a DPIA.[50]

Data subject rights and controller obligations specific to health data

Data subjects have a right to access their personal data, including health-related data – i.e. the data in their medical records containing information such as diagnoses, examination results, assessments by treating physicians and any treatment or interventions provided.[51] In addition, the GDPR grants data subjects the right to erasure, known as the right to be forgotten, allowing individuals to have their personal data erased, although limitations to this right may apply in cases of public interest in the area of public health.[52]

Moreover, the GDPR introduces the obligation for data controllers to nominate a DPO under certain circumstances[53], for instance, if the core activities of the controller or the processor consist of processing health data on a large scale.[54] Finally, regarding the obligation of controllers in relation to health data, the GDPR obliges controllers to keep records of processing activities[55] and where the controller or processor is not established in the EU, it must designate in writing a representative in the Union if they process health data on a large scale.[56]

To conclude, the GDPR has come into force during a critical period of digital transformation, presenting both risks and opportunities. While it is considered to be comprehensive and forward-looking, its impact on data architectures and emerging technologies is expected to be significant. The growth of digital health and the use of (Big) health data highlight the complex challenges in balancing privacy concerns and technological advancements. This has led to conflicting interests between protecting individuals' rights and enabling innovation. The following chapter expands upon this state of affairs by analyzing the impact of the GDPR on DDI in the healthcare industry through a study of the literature and complemented by interviews with industry stakeholders.

[45] Article 35(3)(a) of the GDPR.
[46] *See* article 35(3)(b) of the GDPR.
[47] *See* recital 91 of the GDPR.
[48] *See* article 22(1) of the GDPR.
[49] *See* article 9(4) of the GDPR.
[50] *See* article 35(3)(a) of the GDPR.
[51] *See* recital 63 of the GDPR.
[52] *See* article 17(3)(c) of the GDPR.
[53] *See* article 37 of the GDPR.
[54] *See* article 37(1)(c) of the GDPR.
[55] *See* article 30(5) of the GDPR.
[56] *See* article 27(2)(a) of the GDPR.

5. The impact of the GDPR on data-driven innovation in the healthcare industry

This chapter examines the impact of the GDPR on DDI in the healthcare industry, addressing subquestion (iv) of the thesis, namely: How does the GDPR impact data-driven innovation in the healthcare industry? Section 5.1. outlines the qualitative research methodology, including literature review and interviews, and discusses ethical considerations in light of the interviews conducted. This is followed by a presentation and discussion of the findings from the literature review and stakeholder interviews in section 5.2., highlighting the positive and negative factors related to the GDPR's impact on DDI in healthcare.

5.1. Methodology of the thesis

This thesis relied on a two-stage research approach consisting of 1) desktop research, which includes a literature and legislation review; and 2) qualitative research, specifically, semi-structured interviews. Both stages contributed to the findings presented in section 5.2. of this thesis. The qualitative research design aimed to provide in-depth insights and achieve data saturation. It involved conducting semi-structured interviews with 5-10 experts from two stakeholder groups, as outlined in Table 5.1.

Group	Stakeholder group	ID	Role description
1	Business management	11	Founder & managing director healthtech ecosystem
		12	CEO at a healthcare/healthtech company
		13	Liaison at a medical innovation center
2	Advisory	21	Senior privacy and information management expert at a global healthcare company
		22	Strategic-legal advisor in the field of health and medical law and innovation
		23	DPO at a medical center
		24	DPO at a healthcare/healthtech company
		25	DPO at a medical center
		26	Strategic-legal advisor in the field of health and medical law and innovation

Table 5.1. Stakeholder groups and participants' overview.

As a point of departure, the qualitative research included a minimum of three participants from each expert group to ensure the diversity and quality of the research outcomes (Malterud et al., 2016). Participants were contacted directly or through the interviewer's network starting from January 2023. Selection criteria were based on expertise and experience in the field of data-driven healthcare innovation in a position responsible for various aspects surrounding digitization. The sample size was evaluated throughout the research process, considering the principle of 'information power' to determine adequacy (Malterud et al., 2016).

Participants were interviewed for approximately one hour using the Zoom video conferencing platform (official Leiden University account). The interviews, conducted from March to May 2023, were recorded and analyzed. They were conducted in either Dutch or English, with a predefined set of open-ended questions focusing on challenges and opportunities from the participants' perspective. This format ultimately allowed for further exploration of participants' subjective perceptions and experiences in relation to the subject matter (Saldana, 2011), including explanations and opinions. Finally, comprehension questions and paraphrasing techniques were used to ensure clear understanding. For a more detailed overview of the interview outline and questions presented to the interviewees, see Annex 3.

In light of the data collection phase, the interview data were analyzed, resulting in the identification of several themes and comparisons between expert groups. A review of the literature was combined with the analysis of interview results to generate GDPR-related findings that impact DDI in the healthcare industry. These findings, presented in the following subsection, include both positive and negative factors.

5.2. Results of the thesis research

In the wake of the digitization of society and the emergence of critical technologies, personal data has become the fuel that drives commercial activity in the digital environment. At the same time, however, the large-scale exploitation of this resource by organizations for innovation purposes has raised serious privacy concerns. Conflicting interests arise from the need for effective data protection rules to safeguard consumer rights and trust while avoiding excessive restrictions on commercial activities and stifling innovation (Marelli et al., 2020; London Economics, 2019). Balancing these interests is crucial to enable the expansion of DDI in healthcare and the associated societal benefits.

At the core of the EU's data governance regime is the objective to balance the protection of individuals' data with the promotion of a fair and thriving digital market that offers the potential for growth and innovation (Albrecht, 2016). Though it follows from this that the GDPR ultimately aims to balance distinct fundamental values and interests, whether it has managed to strike a fair balance in this respect is a question that is yet to be answered. This section examines the impact of the GDPR on DDI in healthcare, considering its implications as we have reached the fifth anniversary of its implementation.

5.2.1. Awareness, trust, and level playing in the context of the GDPR

The GDPR has had a significant impact on the handling of personal data within the EU and far beyond its territorial borders and continues to have a significant impact on the digital technologies and data architectures that currently collect, store and manage personal data (Li et al., 2019). Although the GDPR celebrates its fifth anniversary at the time of writing, however, many organizations are still not familiar with its compliance policies (Biswal and Kulkarni, 2022).

Prior to the enforcement of the GDPR, there was a general lack of awareness and understanding among organizations regarding the new legislation and its requirements, although the reason for this is not well explained nor understood (Addis and Kutar. 2018; Sirur et al., 2018). Efforts to inform organizations about the upcoming changes were insufficient, resulting in low levels of implementation, except for organizations within the regulated market that were already more advanced in taking efforts toward data protection (Addis and Kutar. 2018). Moreover, a study conducted in Portuguese health clinics found that while there was awareness of the GDPR's obligations, only a small percentage of organizations had effectively adopted the required measures (Lopes et al., 2020). Interestingly, in this regard, interviewee 22, a strategic-legal advisor in the field of health and medical law and innovation, noted that this narrow approach to data protection was due to a lack of understanding of the legislative framework and the necessary steps for maximizing the benefits of digital care. Bearing this in mind, he emphasized that data protection should be integrated into an overarching strategy and policy, with a focus on baseline protection of data subjects.

Compliance with the GDPR varies depending on the complexity of the organization's business activity, its maturity, the volume and variety of personal data used, the adequacy and flexibility of its information systems, and the availability and willingness of its stakeholders (Lopes et al., 2020). In this regard, interviewees 11, founder & managing director of a healthtech ecosystem, 12, CEO at a healthcare/healthtech company, 21, senior privacy and information management expert at a global healthcare company, 23, DPO at a medical center, and 24, DPO at a healthcare/healthtech company have highlighted how the GDPR is not necessarily perceived as a constraining framework but rather another hoop to jump through in order to ensure a responsible journey toward innovation through data, the perceived burden of which may be different depending on the maturity of the organization and the context in which it operates. Larger organizations and those operating in regulated markets, including the healthcare industry, have generally been more informed and knowledgeable about the GDPR's impact due to regulatory efforts and available resources (Sirur et al., 2018). Smaller organizations, on the other hand, have faced challenges in understanding and complying with the GDPR, requiring significant effort and investment (Adams and Webley, 2001; Ettredge et al., 2011; Petts, 2017; Sirur et al., 2018). These increased costs of compliance are eventually passed on to consumers, thereby inevitably disadvantaging smaller organizations that cannot easily meet these costs. This applies to organizations within the EU, but also extends beyond the EU borders, affecting organizations in the US and China as well, ultimately reflecting the economic impact of the GDPR’s Brussels effect (Li et al., 2019). As such, the fairness of the GDPR's treatment of organizations' compliance abilities has been questioned, creating an uneven playing field for compliance.

This uneven level playing field has become particularly apparent in the healthcare industry with its diverse range of actors operating in different contexts and with varying levels of maturity (Hulsen, 2021). Compliance efforts vary, with larger organizations and data protection forerunners relying less on state support and seeking industrial guidance and private advisory assistance instead (Sirur et al., 2018; Hulsen, 2021). For instance, to ensure compliance with the GDPR, Philips adopted its own guidance instruments – the Philips Data Principles and the Philips AI Principles –, which focus on topics such as security, privacy, benefits to consumers' well-being, oversight, robustness, fairness, and transparency. Smaller organizations, on the other hand, have benefited from state support and guidance from national DPAs, such as the more recently published EDPB guide to assist smaller organizations in achieving GDPR compliance. More specifically, this guide aims to raise awareness among smaller organizations about the GDPR and to provide them with practical information about GDPR compliance in an accessible and easily understandable format (EDPB, 2023). Private advisory assistance has been helpful for smaller organizations, although fraudulent offers have posed serious challenges due to their lack of critical knowledge in the data protection domain (Sirur et al., 2018). Finally, and perhaps most unfortunately, academic research has not been widely utilized by both larger and smaller organizations in their compliance efforts, mainly due to its esoteric nature and lack of practicality (Sirur et al., 2018).

At the same time, it has been noted that stringent enforcement of the GDPR has the potential to substantially impact digital innovation in Europe. Overly strict enforcement may lead to suboptimal approaches and hinder digital innovation without necessarily improving trust among data subjects (Chivot, 2019; Marelli et al., 2020). In the healthcare domain, the restrictive outcomes of the GDPR for organizations have been balanced against the positive effect of compliance for the facilitation of trust in innovation. In this sense, trust is also considered to be a crucial concept in the context of DDI in healthcare, as confirmed by evidence of the GDPR's impact on individuals' willingness to share health data, which indicates that the GDPR has a positive effect by virtue of its focus precisely on user-centricity (Karampela et al., 2019; Asan et al., 2020; Iacob and Simonelli, 2020; Bentzen et al., 2021). This has also been emphasized by interviewee 22, who noted that building a relationship of trust through the GDPR can be a means to foster digital innovation in healthcare, depending on the approach taken. In this sense, data protection is not a barrier to digital care but rather a necessary condition for the responsible and future-proof use of (complex) digital care. To achieve the facilitative role of the GDPR, however, a shift in perspective from hurdles to opportunities is required, primarily through management, as noted by interviewee 23. Moreover, interviewees 23 and 25, DPO at a medical center, confirm this finding, noting the impotence of openness about data processing, communication, and transparency for building trust between data subjects and healthcare providers or research institutes.

In this regard, Lopes et al. (2020) have noted that patients' trust toward healthcare innovation is in part dependent upon consideration of 4 key dimensions, namely: the data architectures used when processing their personal data, the management of their data, and security measures implemented to mitigate potential risks, the realization of their consent and data protection rights, and the putting into place of adequate governance and oversight mechanisms to oversee data processing activities. Bearing this in mind, organizations must shape their conduct to respect consumer privacy, enhance trust in digital services, and promote the growth and competitiveness of EU industries (Reding, 2012; Zarsky, 2015). In this sense, interviewee 25, noted that trust is both an external and internal matter, requiring communication and collaboration within organizations. At the same time, however, interviewees 13, liaison at a medical innovation center, and 23 stressed that finding the right balance between trust, individual patient interests, and data sharing for the greater good is challenging. In this sense, although they have noted the increased interest of private and public organizations in the medical domain to collaborate in relation to data use, they also acknowledge that this is not always possible nor has an adequate balance in this regard been found. Ultimately, robust frameworks based on trust are needed to increase access to and sharing of health data (Digital Europe, 2021). In this regard, it cannot be ignored that the GDPR provides the foundation of trust for a thriving health data ecosystem (Iacob and Simonelli, 2020) and in this sense, trust has become a key asset for data-driven businesses and organizations and an incentive for potential investors (Reding, 2012).

5.2.2. Ambiguity in the definitional demarcation and scoping under the GDPR

The GDPR was adopted as an omnibus rather than sectoral regulation (Marelli and Testa, 2018; Marelli et al., 2020). As such, it aims to provide a flexible framework that prioritizes governance and accountability. However, this comprehensive approach has led to some definitional ambiguity and difficulties in understanding the regulation. Organizations lacking legal expertise noted that although it is a readable and understandable document, the semantics and meaning behind the words of the GDPR are challenging to decipher. This finding has also been confirmed by interviewees 11 and 12, who noted that the lack of clarity and accessibility in language hinders its operationalization. Moreover, interviewee 21 remarked that inconsistencies in terminology further complicate compliance and alignment in data protection. In this regard, according to interviewee 12, the use of overly legalistic or vague descriptions and definitions in the GDPR is not workable in practice and necessitates the involvement of legal experts to understand its practical applicability.

The GDPR's definitional ambiguity is particularly evident in specific contexts like healthcare, as discussed in chapter 4.2. regarding the definition of *(Big) health data*. According to Tzanou (2020), the concept of 'health data' lacks clear demarcation, and the rise of BDA has further complicated the scene. With individuals generating over one million gigabytes of health-related data over their lifetime, in particular, through mHealth devices (Rouvroy, 2016), the scope of health data under the GDPR needs to be expanded to include sources that may directly or indirectly reveal information about an individual's current or future health status (Tzanou, 2020) or social determinants of health. The Big data environment and the dynamic nature of data thus exacerbate these definitional complexities, with the applicable definitional boundaries differing from time to time and across different contexts.

The inferential and predictive nature of data analytics in healthcare challenges key definitions in the GDPR's data governance framework, such as sensitive personal data and identifiable versus anonymous data (Marelli et al., 2020). The concept of sensitive personal data has evolved legally and factually, with new categories emerging as a result of the continuously increasing computing power, availability of Big data, and interconnectivity which are not captured within the GDPR's framework and thus questions the extent to which the GDPR's definitional demarcation of the concept is sufficiently future-proof (Quinn and Malgieri, 2021). In this regard, interviewee 26, who is a strategic-legal advisor in the field of health and medical law and innovation, has noted the importance of clarifying the concept of anonymization, especially in light of secondary data usage, bearing in mind the shift within the healthcare industry to seek access to an enlarged pool of data through social determinants of health to gain insights previously deemed unimaginable. Moreover, in line with this argument, interviewee 23 highlighted that thinking differently and more flexibly about the different ways in which data sets containing personal data can be accessed in a manner that is in line with the principles of data minimization and purpose limitation, through so-called 'privacy-enhancing technologies' (PETs), may also be valuable.

Because it is becoming less intuitively obvious what should be considered to qualify as sensitive personal data under the GDPR, this may ultimately lead to either overly restrictive or overly extensive interpretations of the concept, causing either the deterrence of certain processing activities that may be beneficial from an economic, scientific, or social point of view out of fear for legal repercussions or the devaluation of the concept of 'sensitive personal data' and its becoming of a "tick box" exercise (Quinn and Malgieri, 2021; Marelli et al., 2020; Zarsky, 2016). Consequently, Quinn and Malgieri (2021) emphasize the need for precautionary measures to mitigate such risks and propose a hybrid approach to the concept. In view of the heightened possibility for data integration and linkage, any data points – even those not necessarily considered to be of a sensitive nature –, could reveal sensitive information or lead to intimate assumptions (Prainsack and Buyx, 2017), though the categorization of such data as sensitive under Article 9 of the GDPR is unclear and open to challenges (Malgieri and Comandé, 2017).

Another definitional confusion can be found in the GDPR's scoping of processing activities for the purpose of conducting scientific research. In this regard, recital 159 of the GDPR notes the following:

> *"(...) the processing of personal data for scientific research purposes should be interpreted in a broad manner including for example technological development and demonstration, fundamental research, applied research and privately funded research. (...) Scientific research purposes should also include studies conducted in the public interest in the area of public health. (...) If the result of scientific research in particular in the health context gives reason for further measures in the interest of the data subject, the general rules of this Regulation should apply in view of those measures."*[57]

In this regard, the EDPS published its Preliminary Opinion on data protection and scientific research in 2020, highlighting the increasingly complex interface between research organizations and the wider research ecosystem, with research no longer being limited to the academic realm alone. The intertwining of academia and the commercial sector presents itself in various ways, including funding, the attraction of talent, and public-private collaborations. As such, scientific research is broadly defined under the GDPR regime and extends beyond academia to include research steered and executed by not-for-profit organizations, government institutions, and commercial companies (Kindt et al., 2021).

Though it is commonly assumed that scientific knowledge is a public good to be encouraged and supported and that it is to be used to the benefit of society, the lack of a clear scoping of scientific research in relation to the increasingly present entanglement between public and private parties and interests raises concerns about potentially irresponsible risks when performing an activity considered to be research. In this regard, the EDPB Guidelines 05/2020 on consent under Regulation 2016/679 consider that "the notion may not be stretched beyond its common meaning" and the EDPB therefore

[57] *See* recital 159 of the GDPR.

"understands that 'scientific research' in this context means a research project set up in accordance with relevant sector-related methodological and ethical standards, in conformity with good practice".[58] As such, the EDPB notes that the special data protection regime for scientific research should be applied where personal data are processed, where relevant sectoral standards of methodology and ethics apply, and where the research is carried out to realize growth in society's collective knowledge and wellbeing, rather than merely serving private interests. In this sense, the accountability principle under article 5(2) of the GDPR plays a crucial role in assessing and responsibly managing risks inherent in their research projects.

As the advent of Big data is causing the boundary between academic and private research to become increasingly more blurry, and the distinction between research conducted for the benefit of society and research that mainly serves private interests is becoming less clear, it is necessary to clarify the definition and scope of the concept of scientific research under the GDPR. In practice, the EDPS suggests improving dialogue between DPAs and ethical review boards to establish a better and more aligned understanding of the activities that qualify as genuine research, establishing EU codes of conduct for scientific research, aligning EU research programs with data protection standards, and discussing the legal basis for public-private collaborations in order to ensure effective accountability in the highly complex ecosystem of (Big) health data (EDPS, 2020).

Considering the future landscape of abundant data, advanced technologies, and increased collaborations between private and public entities, Wachter (2019) emphasizes the need to redefine the remit of data protection law. In this sense, she stresses that outdated categorizations of data as personal or non-personal and sensitive or non-sensitive are insufficient, as they only reflect the data's nature at the time of collection and fail to account for subsequent processing. Moreover, the binary approach in the GDPR exacerbates this issue, as the black/white scoping in relation to the protection of health data is difficult to maintain and static definitional demarcations can no longer be maintained, especially in the age of Big data and mHealth, and may cause the GDPR's protective framework to fall short in achieving its ultimate objectives (Tzanou, 2020). In this sense, interviewee 21 stressed that the discussion surrounding definitional ambiguity is not necessarily about interpretation but more so about the risks that cooperating parties are willing to take, bearing in mind their interest to ensure access to care and trust in their operation and handling of personal data.

5.2.3. Workability of substantive provisions under the GDPR

As discussed in chapter 3 of this thesis, the governance framework central to the GDPR has been largely informed by the so-called "informational self-determination" or "notice-and-consent" approach (Nissenbaum, 2011; Cate and Mayer-Schönberger, 2013; Mantelero, 2014), which revolves around the idea that personal data cannot be disconnected from its source – the data subject – and that data subjects should therefore be endowed with adequate means to exercise their autonomy, ownership, and control over processing activities concerning their personal data (Marelli et al., 2020; Ziegler et al., 2019). However, the effectiveness of this model in protecting data subjects' autonomy, ownership, and control has been challenged in the era of Big data, AI, and advanced technologies (Hulsen, 2021; Mantelero, 2014; Cate and Mayer-Schönberger, 2013; Kuner, 2012; Nissenbaum, 2011). This is especially relevant in the healthcare domain, where issues arise with regard to commercial research by genetic testing companies (Marelli et al., 2020; Hayden, 2012; Ducharme, 2018) and the development of mHealth technologies that remain scattered and underregulated (Tangari et al., 2021; Iwaya et al., 2020; Mulder, 2019; Plachkinova et al., 2015).

Recent advancements in healthcare technology, particularly in Big health data, BDA, and the focus of DDBMs in healthcare on re-purposing and cross-linking different flows of personal data (Van Dijck et al., 2016), challenge key principles of the GDPR such as purpose limitation, data minimization, and

[58] *See* paragraph 153 of the EDPB Guidelines 05/2020 on consent under Regulation 2016/679.

storage limitation. The principle of purpose limitation requires personal data to be collected for specified, explicit and legitimate purposes and may in principle not be further processed in a manner that is incompatible with those purposes.[59] In this regard, Kuner et al. (2021) have noted that Big data poses significant challenges in complying with data governance frameworks, thereby stressing that there is still little evidence that data protection is keeping up with the pace of change in the digital space. While the principle of purpose limitation is geared toward data subjects and their ability to exercise autonomy and control over their personal data, thereby ultimately serving to prevent the uncontrolled processing of personal data (Hildebrandt, 2015) and thus promoting trust in data environments, adhering to this principle in the healthcare context may prove to be difficult. This holds especially true for healthcare research as researchers working with big genetic data may find that it is impossible to adhere to this principle without reducing the value of a particular research experiment nor may it be clear to the researcher what compliance may entail in the first place. As a result, establishing clear boundaries for the purposes of personal data processing in healthcare research may be unfeasible, despite the GDPR's provisions for accommodating scientific research (Quinn and Quinn, 2018).

Similarly, the GDPR prescribes a data minimization principle, which is closely connected to the principle of purpose limitation and requires the processing of personal data to be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed.[60] However, this principles may conflict with Big data-driven scientific research, which relies on processing large volumes of data to uncover meaningful insights (Marelli, 2020; Quinn and Quinn, 2018). As a result, abiding by the data minimization principle in this context may go against the very nature of such research. Similarly, the storage limitation principle – which encompasses the notion that personal data should not be stored for longer than is strictly necessary and should thus be deleted once the purpose for processing no longer applies[61] – may prove to be incompatible in the age of Big (health) data, as research often extends beyond initial purposes and requires data to be available for future studies. Although the GDPR introduces an exemption to this principle of limitation in cases where personal data is processed for scientific research purposes, this does not provide sufficient guardrails to researchers to abide by this principle in practice, especially considering how the GDPR allows for the introduction of nation-specific provisions with regard to the processing of genetic, health and biometric data.[62] This is mainly due to the fact that research may continue for longer than initially expected as a result of new discoveries that extend beyond the initial scope of and purposes for processing activities, and also as a result of good practice in scientific research, which requires the making available of datasets to subsequent researchers for scientific research purposes (Quinn and Quinn, 2018).

Beyond these key principles set out in the GDPR, a fourth principle is challenged by DDI practices in the healthcare space, namely the principle of transparency.[63] According to recital 39 of the GDPR, any processing of personal data should be transparent in the sense that “it should be transparent to natural persons that personal data concerning them are collected, used, consulted or otherwise processed and to what extent the personal data are or will be processed”. The principle of transparency furthermore requires “that any information and communication relating to the processing of those personal data be easily accessible and easy to understand, and that clear and plain language be used”.[64] However, in the healthcare sector, achieving transparency in practice can be challenging due to structural opacity present at various levels of health research and care (Marelli et al., 2020). In this regard, Nissenbaum (2011) has noted that compliance with the transparency principle may result in a "transparency paradox" where practical implementation conflicts with theoretical transparency.

[59] *See* article 5(1)(b) of the GDPR.
[60] *See* article 5(1)(c) of the GDPR.
[61] *See* article 5(1)(e) of the GDPR.
[62] *See* article 6(4) of the GDPR.
[63] *See* article 5(1)(a) of the GDPR.
[64] *See* chapter III section I of the GDPR.

This becomes particularly problematic in situations where choice appears to be constrained – for instance, where long and complex privacy notices are presented, thereby ultimately forcing data subjects to either submit to passive consent or abandon the use of the desired service (Cate and Mayer-Schönberger, 2013).

The rules for consent are laid down in article 4(11) of the GDPR and refer to:

> *"(...) [A]ny freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her".*

In the context of processing special categories of personal data, such as health data, explicit consent of the data subject in line with article 9(2) of the GDPR is often considered the preferred legal basis (Mostert et al., 2016), and consequently consent is often considered to be the default ground for processing in the context of scientific research (Quinn, 2021). However, especially in the context of secondary use of health data, the narrow interpretation of explicit consent creates particular barriers, while the adoption of a new approach toward the processing of personal data for research purposes was one of the most controversial topics in the course of drafting the GDPR (Shabani and Borry, 2018). The EDPB Guidelines on consent highlight that consent is only considered to be appropriate as a lawful basis where the data subject is offered control and a genuine choice with regard to accepting or declining the terms offered without detriment. More specifically, recital 33 of the GDPR acknowledges how it may often be impossible to fully identify the purpose of personal data processing for scientific research purposes at the time of data collection, and therefore extends the scope of consent by data subjects to certain areas of scientific research when in keeping with recognized ethical standards for scientific research. As noted above, this may prove particularly relevant in the context of scientific research in the healthcare domain where compliance with the principles of purpose limitation, data minimization, and storage limitation is becoming increasingly challenging. Moreover, repetitive requests for consent may be undesirable from an ethical point of view, incompatibility may arise where data is used for other research purposes than the purpose set out originally, the concept of explicit consent has not been defined separately in the GDPR, and fragmentation of its understanding may exist as a result of different interpretations to the concept of consent by Member States (Kist, 2022). Though seemingly allowing for a broader interpretation of the concept of consent, however, the EDPB stresses that the phrase 'broad consent' has neither been included in the recitals nor in the GDPR itself, ultimately indicating that the scope of consent may not be stretched too far beyond reason. Building forth upon this discussion, interviewee 26 reiterated that the workability of consent varies in the health sector, and its manifestation should be context-dependent. Even more so, interviewee 23 remarked that considering the diversity of national legislation on consent, broad consent should be considered valid under the GDPR regime, especially in light of evolving data use for healthcare and advancements in technology.

In this regard, several studies have explored alternative legal bases for the secondary use of personal data for health research under the GDPR (Kist, 2022; Quinn, 2021; Quinn and Quinn, 2018). These include reasons of public or legitimate interest, the scientific research exemption, and personal data that has been manifestly made public. These options highlight the flexibility provided by the GDPR for research activities and demonstrate the balance between data protection and the public and societal interest in data sharing (Kist, 2022). However, this approach varies across Member States, leading to a fragmented landscape that hinders pan-European and international data sharing, contradicting the GDPR's goal of harmonization (Kist, 2022; Shabani and Borry, 2018). Moreover, this state of affairs raises questions as to the extent to which various types of actors enjoy a level playing field regarding their ability to conduct research with (potentially sensitive) personal data (Quinn, 2021).

5.2.4. Fragmentation in the legal framing of (Big) health data processing

The GDPR was a stepping stone in strengthening individuals' right to data protection while promoting commerce in data within the EU. However, two years after its implementation, the European Commission recognized that harmonization across Member States is still incomplete, posing challenges to cross-border business and innovation (EC, 2020a). In this sense, interviewee 21 acknowledged the increased harmonization and focus on privacy brought about by the GDPR but noted minimal practical impact in the context of DDI in healthcare. Bearing this all in mind, there are several factors that have to be considered in this regard.

First, in order to ensure an effective and consistent application of the EU data protection framework, the GDPR introduced the 'One-Stop Shop' mechanism to facilitate cross-border data processing. While the OSS mechanism unmistakably reflects the unification and simplification that was envisaged by the GDPR (Balboni et al., 2014), its practical implementation has fallen short of expectations due to a more restrictive interpretation by the Court of Justice of the European Union (CJEU)[65] and the inability to prevent forum shopping (Thyve, 2016; Schreiber, 2019). This complicates matters for businesses and organizations wishing to innovate through data, particularly in complex ecosystems like the healthcare industry that rely on (Big) data.

Second, there is a noted tendency among DPAs and the EDPB to interpret the legal framework of the GDPR overly restrictively, in some instances going against the letter and spirit of the GDPR text or relevant case law (Digital Europe, 2020). Although DPAs have developed tools to help businesses comply with the GDPR, and the EDPB has offered guidance on the interpretation of the GDPR's provisions, there are still varying interpretations of the GDPR by supervisory authorities across the EU. This lack of harmonization raises uncertainty in terms of the scope and applicability of the framework, and may consequently impact the profitability of businesses and organizations and their desired ‘level playing field’. Interviewee 25 confirms this finding, stating that the GDPR seeks a healthy balance between data protection and the free flow of personal data, but the rule-based interpretation of the framework both within organizations themselves and by European and national supervisory authorities is limiting to the innovation landscape. In this sense, interviewees 22 and 25 not that it is important for regulatory and supervisory authorities, as well as advisory privacy functions, to adopt a positive and risk-based approach to the GDPR, considering the necessary protections against the mere commercial exploitation of personal data while also facilitating crucial treatments and research.

Moreover, despite the GDPR's efforts toward harmonization, national legislators still have the ability to introduce specific laws or provisions that deviate from the GDPR, ultimately leading to fragmentation and preventing the unified application of the GDPR across the EU (Digital Europe, 2020). This scene is further complicated in the healthcare industry, where there is a patchwork of legal and regulatory frameworks governing the handling of personal data and the use of digital technologies, for instance with regard to the processing of genetic data, biometric data, or data concerning health. In a similar sense, interviewee 25 noted that the patchwork of existing and upcoming supervisory authorities in the healthcare domain has also contributed to this process of complication. In the health data and innovation environment, we are faced with European and national data protection supervisory authorities, national healthcare authorities, and upcoming supervisory bodies, such as the algorithm sub-authorities and the European Health Data Access Bodies. In this regard, interviewee 25 emphasized that the lack of maturity among data protection and other upcoming supervisory authorities, compared to more established healthcare authorities, creates a disconnect and hinders their ability to understand and address the needs and challenges faced by healthcare organizations.

[65] See the case of Facebook Ireland Ltd, Facebook Inc., Facebook Belgium BVBA v. Gegevensbeschermingsautoriteit (Case C-645/19).

This development is interesting from both a national and sectoral point of view; the fragmentation of the legal landscape arises from Member States implementing stricter rules that deviate from the GDPR, which leads to different approaches to the processing of health data and creates challenges in accessing such data locally and across borders, particularly for health-related scientific research as elaborated on in more depth in chapter 5.2.3. At the same time, the GDPR has not adequately addressed sector-specific concerns, resulting in an unclear application of its provisions. While the GDPR and complementing legal frameworks within Member States have already been in place for half a decade, sector-specific legislation fit for the data age is still thus still lagging behind.

A 2021 Parliament letter by rapporteur Van Gent highlights the complexities faced in the healthcare domain regarding the practical implementation of the GDPR in the Netherlands, two years after its entry into force. The letter reveals that researchers encounter difficulties when applying the rules laid down in the GDPR, hindering valuable research and innovation. The patchwork of legislation in the healthcare sector, including the GDPR and national laws, creates ambiguity in data-sharing activities. In this sense, interviewee 25 emphasized that it is the patchwork of legislation, rather than the GDPR or the proposal on the European Health Data Space (EHDS), that hampers meaningful innovation in healthcare. The letter also emphasizes the need to clarify the landscape of applicable legal frameworks and to update national legislation, such as the Dutch Medical Treatment Contracts Act (WGBO). In this regard, interviewee 22 explained that the GDPR in itself does not form a hurdle to DDI in the healthcare industry as it merely forms a general data governance framework. Rather, he noted that it is the more specific and oftentimes decades-old legislation tailored to the healthcare sector that complicates the balancing of data usage for various purposes against the protection of patients' privacy. These laws are generally not updated to match the complexities of the data age in which we currently find ourselves and, consequently, the outdated and legalistic frameworks they offer the research domain and industry may hamper efforts taken toward implementing innovative practices and introducing new solutions. Additionally, interviewee 25 highlighted that national implementation laws of the GDPR, such as the Dutch implementation law, rely on outdated legislation from the 1990s for scientific research provisions. This requirement for compliance with both the GDPR and country-specific privacy regulations further complicates the compliance landscape (Przyrowski, 2018). Finally, in this regard, interviewee 23 emphasized the need for clarity in EU and national legislation, as well as adaptation of upcoming legislation like the EU Artificial Intelligence Act (AIA) and the EHDS, to ensure alignment with the GDPR. In this sense, she notes that the problem is not the GDPR, but the manner in which the GDPR is being dealt with and how national legislation in the healthcare domain is built around it and interacts with it. Without clear guidance and a balanced approach to the existing requirements, GDPR compliance may become unworkable and hinder desired outcomes.

The 2021 Parliament letter furthermore raises concerns about the Dutch DPA's relatively restrictive interpretation of the GDPR in the context of scientific research in the medical domain compared to other EU DPAs. This approach decreases legal certainty and may cause fear of administrative or reputational repercussions. As a result, expenses for legal advice rise, reducing research budgets and hindering innovation. There are discussions about the role of DPAs in providing clear expectations through education and communication regarding permitted processing activities, thereby taking into consideration existing concerns regarding the resources and capacity available to the Dutch DPA to fulfill such a role and preventing confusion around their primary role as independent regulators and enforcers of the GDPR. In this regard, interviewees 12 and 24 stressed how in their view national DPAs have an important role to play in offering clarification to organizations that process data beyond ensuring compliance, in order for an effective and efficient implementation and application of the GDPR to be achieved in practice. Additionally, interviewee 21 suggested that organizations in the healthcare industry would benefit from clear sector-specific criteria for data processing. Currently, organizations rely on their own interpretations of the GDPR, leading to varying arguments for or against certain processing activities. As this often takes place at an individual level within and between organizations, interviewee 21 sees a significant role for the EC to play in this regard, though he does not believe such a role is to be primarily given to the national DPAs as they often lack the necessary expertise and resources to do so adequately and effectively. Nevertheless, he does note in this regard that strict interpretations by national DPAs should not interfere with their ability to cooperate and think along with organizations in their compliance efforts.

To conclude, an assessment of the impact of the GDPR on DDI in the healthcare industry requires specific consideration of a variety of factors, including awareness, trust, and the existence of a level playing in the context of the GDPR, ambiguity in the definitional demarcation and scoping under the GDPR, the workability of substantive provisions under the GDPR, and fragmentation in the legal framing of (Big) health data and the processing thereof. In this regard, it must be emphasized that inadequate data protection rules, insufficient clarity as to the scope and meaning of existing concepts and rules, and lacking enforcement can harm consumers' rights and trust, while overly strict protection regimes may hinder commercial activities, increase administrative burdens, and ultimately stifle innovation through data at an individual and societal level. Addressing identified issues in the GDPR in relation to the above-required balancing act in the healthcare context is particularly relevant in light of current EU initiatives aimed at harnessing the potential of data in Europe; in particular, ongoing developments pertaining to the EHDS and the AIA. What policy response should be prompted to ensure that the GDPR optimally balances the protection of privacy and the facilitation of DDI in the healthcare industry in light of these developments will be discussed in the next chapter of this thesis.

6. Discussion and considerations for policy response

This chapter offers a preliminary discussion of the policy considerations prompted by the identified impact of the GDPR on DDI in the healthcare industry. Bearing the results of chapter 5 in mind, this chapter answers subquestion (v) of the thesis, namely: What considerations does this prompt for future policy response in light of ongoing regulatory efforts at the EU level? Section 6.1. introduces the renewed EU approach to harnessing the potential of data in healthcare, thereby focussing on the proposal for a regulation on the EHDS and the AIA. Section 6.2. then examines the shift from fragmentation to alignment by presenting policy considerations for future policy response. Finally, section 6.3. presents the limitations of this thesis and discusses avenues for future research.

6.1. A renewed EU approach to harnessing the potential of data in healthcare

Putting the importance of innovation through data at the center of its policymaking activities and acknowledging its potential to be successful in the data-agile economy, at the start of 2020, the EC formulated a strategy to enable the EU data economy. In this regard, the EC (2020b) has noted that at the core of the EU's potential to grow and innovate through data lies the trust of citizens and their willingness to embrace data-driven innovations, which, in turn, relies on strict compliance with data protection rules. To fully harness the potential of data, the EU aims to establish a single European data space governed by EU law, including the GDPR. This data space should ensure compliance with EU market norms and facilitate the secure, accessible, and sustainable flow of personal and non-personal data globally.

Broadly speaking, the EU strategy for data is based on four key pillars, of which two will be discussed in more detail hereafter. First, the EU aims to establish a cross-sectoral governance framework for the access and use of data. In this regard, the EC's approach to regulation has focussed on the establishment of an enabling legislative framework for the governance of common European data spaces that allows for "lively, dynamic and vivid ecosystems to develop" and which puts in place an agile approach that facilitates experimentation with regulation, iteration, and differentiation. In practice, such legislative frameworks should clarify what data can be used in which situations, facilitate cross-border data use, and prioritize interoperability requirements and standards within and across sectors while leaving a certain level of discretion to sectoral authorities to specify requirements. In practice, two key governance pillars of the EU strategy for data are the European Data Governance Act[66] and the proposal for the European Data Act[67]. While the former strengthens the single market's governance mechanism and establishes a framework to facilitate general and sector-specific data-sharing, the latter complements the European Data Governance Act by stipulating in more detail who can create value from data and under which conditions.

In addition to the horizontal governance framework discussed above, the EC aims to promote common European data spaces in strategic sectors and domains of public interest to accelerate the development of the European data economy and to capitalize thereon to benefit society at large (EC, 2022a). As a point of departure, the EC has indicated its initial support for ten data spaces, though additional data spaces may follow in order to build a comprehensive European data space. These include common EU data spaces for industrial manufacturing, environmental sustainability, mobility, finance, energy, agriculture, public administration, labor market skills, and health (EC, 2020b). The main goal of these EU-wide common, interoperable data spaces in strategic sectors is to make available the necessary tools and infrastructure and put in place common rules, thus fostering trust, in order to overcome legal and technical barriers to data sharing.

[66] Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act).

[67] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on harmonised rules on fair access to and use of data (Data Act).

Returning to the focus of this thesis, in May 2022, the EC published its proposal on the EHDS, intended to serve as a governance framework for future health data use across the EU for the purposes of advancing the prevention, detection, and curing of diseases as well as promoting evidence-based efforts toward improving the accessibility, effectiveness, and sustainability of the healthcare systems (EC, 2022a). The publication of this proposal formed a direct response to earlier research which identified challenges that negatively impact the primary and secondary use of health data within the EU and present barriers to individuals' effective exercise of control over their personal data (Shabani, 2022). The importance of putting in place such a common ecosystem for health data was even further stressed during the COVID-19 pandemic, which highlighted the critical role of data in the fight against the virus at a global level (Hendolin, 2021; Schutte et al., 2021; Shabani, 2022). Building upon the horizontal framework set out in the European Data Governance Act and other existing EU frameworks, in particular the GDPR, the proposal on the EHDS aims to establish a harmonized internal market for health data by facilitating access, sharing, and use of health data for the purpose of providing healthcare services while ensuring that individuals maintain control over their health data, encouraging the free flow of health data through a genuine single market for digital health services and products, and facilitating secondary use of health data for research, innovation, policy-making and other regulatory activities in a privacy-preserving, secure, timely, transparent and trustful way, accompanied by appropriate institutional governance mechanisms.[68]

Though not directly incorporated into the EU Data Strategy, another regulatory framework proposed by the EU that cannot be left without mention in the context of this thesis is the proposal for the AIA. As part of its Digital Strategy, the EU set out to regulate AI with the aim of ensuring better conditions for the development and use of this innovative technology. This eventually led the EC to propose the first EU regulatory framework for AI in April 2021. Complementary to the GDPR, the AIA introduces harmonized rules to ensure the safe and ethical use of AI systems within the EU while upholding fundamental rights. Moreover, in light of the growing availability of health data and the clear benefits of broad access to existing health databases for research, clinical, and public health purposes, the importance of accessing data from the EHDS in relation to the training, validation, and testing of high-risk AI systems has also been emphasized in the AIA. In terms of its setup, the AIA – like the GDPR – adopts a risk-based approach to address the varying levels of potential harm posed by AI systems. As such, the AIA distinguishes between unacceptable, high, medium (limited), and low (minimal) risk AI uses, with accompanying prohibitions on development, due diligence obligations, and transparency requirements. Similar to the strategy upheld in the GDPR, the AIA introduces such an approach with the aim of striking a balance between enabling innovation and growth in low-risk areas while providing robust fundamental rights protections in relation to prohibited or high-risk AI uses.

6.2. From fragmentation to alignment: preliminary considerations for policy response

To bring the preceding analyses together, this section offers a preliminary discussion of policy considerations directed toward the EC, national regulators, and European and national DPAs in light of ongoing regulatory efforts at the EU level as described above. The analysis and discussion presented in the foregoing chapters allow for five policy considerations accordingly, as will be presented hereafter.

6.2.1. Streamline the patchwork of regulations and oversight bodies in healthcare

The healthcare industry operates within a complex regulatory landscape, consisting of a patchwork of legislative frameworks which has created challenges for organizations striving to achieve legal compliance. The overlapping and sometimes conflicting nature of these frameworks adds to this complexity, leaving organizations unsure of how these frameworks intersect and relate to one another. As new regulations for the management of health data and digitization emerge, in particular the EHDS

[68] See article 1 of the proposal for a regulation on the EHDS.

and AIA, the regulatory scene is set to become even more intricate. To address this issue, policymakers at both the EU and national levels must take decisive action to untangle this complex web of regulations and provide organizations with clear and practical guidance for compliance. By streamlining and harmonizing existing and upcoming regulatory frameworks, policymakers can alleviate the burden on healthcare organizations in both the public and private realms, thereby promoting compliance and fostering an environment that supports innovation and the responsible use of data in healthcare.

Moreover, the introduction of these new legislative frameworks will bring about the establishment of new supervisory bodies responsible for overseeing compliance in the healthcare data and digitization landscape. It is important to clarify the roles and responsibilities of these supervisory bodies to create a sustainable compliance environment. Organizations need clarity on which supervisory bodies they should engage with in specific instances and how these bodies relate to one another. By providing clear guidelines and establishing effective coordination mechanisms between national and EU-level supervisory authorities alike, policymakers can facilitate a smoother compliance process and enable organizations to navigate the evolving regulatory landscape with greater confidence and efficiency.

6.2.2. Facilitate a level playing field for compliance through a maturity-based approach

The current compliance landscape for the GDPR reveals an unequal level playing field. This disparity stems from the GDPR's failure to timely and adequately consider the varying maturity levels of organizations, including differences in expertise and resources available for compliance. Addressing this unequal playing field for compliance requires policymakers to conduct a thorough assessment of the compliance landscape, identify challenges faced by smaller and less mature organizations, and tailor compliance requirements accordingly. In this sense, practical guidance, support, and knowledge-sharing should be provided to help them meet compliance obligations effectively. With new EU legislation on health data and digitization on the horizon, the compliance scene will become even more complex. To prevent smaller and less mature organizations from shouldering disproportionate burdens and potentially stifling economically and socially valuable innovation, it is crucial to establish frameworks that facilitate a level playing field for compliance through a maturity-based approach, including exemptions, and regulatory sandboxes to promote fairness, data protection, and a thriving data-driven ecosystem that is inclusive to innovators in all stages of development and maturation. Moreover, considering the previous discussion about many organizations' lack of familiarity with the GDPR at the time of its adoption and entry into force, leading to a fragmented compliance landscape that persists today, it is crucial to ensure that future legislative frameworks concerning health data and digitization are communicated clearly, effectively, and in a timely manner to all relevant stakeholders.

6.2.3. Overcome regulatory ambiguity through legal design and concrete guidance

In order to effectively govern DDI in the healthcare sector, it is imperative to address the challenges posed by regulatory ambiguity. The assessment of the GDPR provided in this thesis reveals that one of its major pitfalls is its lack of clarity and ambiguous language, which can ultimately lead to uncertainty and confusion among healthcare organizations and individuals trying to navigate the requirements set out in this regulatory framework. As new frameworks are introduced to govern the management of health data and digitization, new terminologies, and requirements will be introduced, some of which may be complementary, while others introduce terms that already exist in other frameworks but carry different definitions and practical applications. This proliferation of terms and overlapping frameworks adds another layer of complexity to the compliance scene, making it even more challenging for stakeholders to understand and comply.

One approach to overcoming regulatory ambiguity across the patchwork of applicable legal frameworks is through legal design (Perry-Kessaris, 2019). In practice this involves a user-centered approach to creating laws, regulations, and guidelines, thereby emphasizing clear and unambiguous language, and avoiding jargon and technical terms that may cause confusion. As such, legal design could offer regulators a means to make legal compliance processes more accessible and practical. At the same time, concrete guidance is another essential component of overcoming regulatory ambiguity. Providing clear, actionable, and practical guidance resources is vital for organizations and individuals to understand their obligations and comply with the regulations effectively. These guidance materials should offer step-by-step instructions, examples, and best practices tailored to the specific context of the healthcare sector. By offering such concrete guidance, policymakers can enhance understanding and facilitate compliance, ultimately fostering innovation while protecting individuals' privacy.

6.2.4. Account for national interests in the move toward a European health ecosystem

As the EU endeavors to establish an EU ecosystem for healthcare and data sharing, exemplified by the EHDS initiative, it seeks to promote uniformity and harmonization in healthcare processes and practices across EU Member States. However, it is crucial to acknowledge that healthcare has traditionally been a national policy matter, deeply rooted in each country's institutional and regulatory culture. This became particularly apparent at the time of the COVID-19 pandemic, during which the need to consider the unique challenges and circumstances faced by each Member State was emphasized. To successfully implement new regulatory frameworks for health data and digitization, it is essential to strike a balance between EU harmonization objectives and national interests and values. EU policymakers should allow a margin of appreciation for national regulators, recognizing their role in safeguarding and accommodating national political agendas. This approach ensures that the EU's objectives are effectively achieved while respecting the diversity and context-specific considerations of Member States.

6.2.5.Clarify the balancing of public and private interests in data sharing for healthcare purposes

Ensuring the protection of personal data is crucial for fostering trust among individuals and organizations in the advancement of the digital economy and equitable access to healthcare. In light of ongoing regulatory efforts toward governing the management of health data and digitization, in particular the EHDS, the EDPB and EDPS emphasize that the success of the EHDS relies on a solid legal foundation that aligns with EU data protection law, the implementation of a robust data governance mechanism, and the implementation of effective safeguards to protect the rights and interests of individuals in full compliance with the GDPR. As such, they consider that the EHDS should serve as a means to adequately balance the interests of the individual data subjects and the shared interest of society as a whole in the sharing of health data across organizations and borders (EDPS-EDPB, 2022). More specifically, the Data Governance Act defines the concept of 'data altruism', which refers to the practice by which people and organizations make health data voluntarily available for the public interest thereby enabling new data sources for secondary purposes such as research and innovation without seeking reward. This consent-based mechanism is also clearly expressed within the EHDS framework which sets out to establish mechanisms for data altruism in the health sector. While efforts are already being made toward developing health data consent forms, clarifying the roles and responsibilities of actors in data altruism, and developing practical data altruism tools (TEHDAS, 2022), regulators should ensure GDPR compliance in relation to the practical implementation of data altruism in the health sector, in particular in relation to the required form and degree of consent. Moreover, in this regard, a clarification should be provided as to the adequate balancing of public and private interests in data sharing for healthcare purposes, so as to allow organizations possessing relevant health data to understand not only under what conditions data sharing is permitted but also under what conditions doing so is to be considered desirable from different points of reference and interests.

6.3. Limitations and future research

Drawing on the expertise of healthcare innovation professionals has contributed to developing a comprehensive understanding of the current situation and the challenges faced in data-driven healthcare innovation. In particular, it has prompted a critical examination of theoretical perspectives regarding the GDPR's influence on DDI in the healthcare domain. However, this approach is, of course, not without limitations, which vary in nature. The scope and duration of the master's thesis caused several inclusion limitations. For example, my selection of stakeholder groups includes two essential but far from all important stakeholder groups significantly involved in healthcare digitization. Consequently, future research should include a more diverse stakeholder group, in any case, a larger representation of private sector management, pharmacies, other medical professions, research institutions, academia, and patient representative organizations. Furthermore, it remains unclear whether a larger number of interview participants would have resulted in more profound findings or potentially allowed for the identification of additional contrasts. To increase the diversity and validity of the qualitative research underpinning this thesis, future research should expand upon the interviews conducted, thereby assessing the threshold for data saturation on a case-by-case basis. Finally, the limited scope and duration of this thesis did not allow for an in-depth analysis of ongoing regulatory efforts surrounding data at the EU level, including the EHDS and the AIA, nor did it allow for an assessment of the GDPR's impact on DDI in the healthcare industry across EU Member States. Since the GDPR and upcoming regulations on the EHDS and AI refer to all Member States of the EU and – due to institutional and culturally climatic differences – may impact their innovation landscape differently, future research would require a more comprehensive study of these frameworks and their interaction to provide for more fitting and tailored policy considerations.

7. Conclusion

The answer to the first part of the key research question of this thesis, i.e. “How does the GDPR impact data-driven innovation in the healthcare industry?” is clear: while the GDPR is widely regarded as a comprehensive and forward-looking piece of legislation that addresses the challenges of data protection in the digital age, it remains questionable to what extent it has succeeded at realizing its two-fold objective in the healthcare context, namely: the protection of individuals' fundamental right to data protection, on the one hand, and the promotion of a fair and functioning EU digital healthcare market that fosters growth and innovation, on the other. In this regard, this thesis has brought into view four key focus points across which the GDPR has impacted the DDI scene in healthcare, namely:

- Awareness, trust, and level playing in the context of the GDPR;
- Ambiguity in the definitional demarcation and scoping under the GDPR;
- Workability of substantive provisions under the GDPR; and
- Fragmentation in the legal framing of (Big) health data processing.

Bearing these findings in mind, the answer to the second part of the key research question of this thesis, i.e. “What considerations does this prompt for future policy response in light of the ongoing development of the European Data Strategy” considers a set of five key policy considerations directed toward the EC, national regulators, and European and national DPAs in light of ongoing regulatory efforts at the EU level, in particular the proposals for the EHDS an AIA, namely:

- Streamline the patchwork of DDI-related regulations and oversight bodies in healthcare;
- Facilitate a level playing field for compliance through a maturity-based approach;
- Overcome regulatory ambiguity through legal design and concrete guidance;
- Account for national interests in the move toward a European health ecosystem; and
- Clarify the balancing of public and private interests in data sharing for healthcare purposes.

It is hard to contest that regulating DDI in healthcare is a strict necessity in an age characterized by fast-paced flows of (sensitive) personal, complicated data ecosystems, the advancement of digital technologies exploiting such data, and the dangers and serious consequences involved in not managing the interaction between these three factors timely and adequately. Effective regulation of this complicated environment, however, requires the proportionate consideration of all interests and values at stake. In particular, central to this debate is the concept of trust, which not only oversees the success of innovation as a result of consumer acceptance but also ties into the success of organizations’ compliance efforts and actions. Bearing this in mind, this thesis emphasizes that if the full economic and societal benefits of DDI in healthcare are to be realized within the EU and beyond, upcoming and future regulation of this domain will have to consider all interests involved and balance the trust of individuals and organizations alike in a human-centered, responsible, practical, and context- and case-dependant manner.

To conclude:

(a) With the advent of (Big) health data as the new oil fuelling DDI in the healthcare industry, new opportunities to increase the quality and accessibility of care across the globe have come about while simultaneously raising serious concerns in relation to the protection of individual’s right to privacy and their trust in the advancement of the digital economy and equitable access to healthcare.

(b) The GDPR aims to address this complex interaction of opportunities and challenges in the (Big) data realm by putting in place a framework that strikes a balance between data protection, economic growth, and innovation in the EU internal market.

(c) However, this balancing activity brings about a complex trade-off between these objectives, where the lack of sufficient and effective data protection rules and enforcement may harm consumers' rights and trust – on the one hand –, and where too stringent protection regimes will unduly restrict commercial activities, increase administrative burdens for economic operators and ultimately stifle innovation.

(d) An analysis of the GDPR's account for data processing activities in the healthcare industry highlights concerns regarding its lack of clarity in defining 'Big health data,' its broad scope and stringent obligations for market players, and the ambiguity surrounding the processing of health data for clinical and research purposes.

(e) An examination of the GDPR's impact on DDI in the healthcare industry confirms that the success of DDI in the healthcare space might be highly contingent upon data protection regulation. More specifically, this analysis finds four key focus points across which the GDPR has impacted the DDI scene in healthcare, both procedural and substantive in nature.

(f) To capture the evolving health data and digitization landscape, the EC has proposed new regulatory frameworks to manage this environment more adequately and effectively, including the EHDS and AIA. For the economic and societal benefits of DDI in healthcare to be realized within the EU and beyond, however, these regulatory efforts must strike a balance that considers all interests and promotes trust through a human-centered, responsible, practical, and context- and case-dependent approach.

Sources

I - Primary Sources

(A) Legislation, regulations, directives, etc.:

1) **The General Data Protection Regulation**: 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.
2) **The Proposal for the European Health Data Space:** Proposal for a Regulation of the European Parliament and of the Council on the European Health Data Space.
3) **The Proposal for the AI Act:** Proposal for a Regulation of the European parliament and of the Council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union Legislative Acts.

(B) Recommendations, guidelines, policy papers, etc.:

1) European Commission. (2010). *"Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions. A comprehensive approach on personal data protection in the European Union"*, (COM (2010) 609 final).
2) European Commission. (2020a). *"Communication from the Commission to the European Parliament and the Council. Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition - two years of application of the General Data Protection Regulation"*, (COM/2020/264 final).
3) European Commission. (2020b). *"Communication from the Commission to the European Parliament, the Council, The European Economic and social Committee and the Committee of the Regions. A European strategy for data"*, (COM/2020/66 final).
4) European Commission. (2022a). *"Commission Staff Working Document on Common European Data Spaces"*, (SWD(2022) 45 final), available at https://digital-strategy.ec.europa.eu/en/library/staff-working-document-data-spaces.
5) European Commission. (2022b). *"Data Act: Commission proposes measures for a fair and innovative data economy"*, available at https://ec.europa.eu/commission/presscorner/detail/en/ip_22_1113.
6) EDPB. (2020). *"Guidelines 05/2020 on consent under Regulation 2016/679"*, availavel at https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf.
7) EDPB. (2023). *"EDPB Launches Data Protection Guide for small business"*, available at https://edpb.europa.eu/news/news/2023/edpb-launches-data-protection-guide-small-business_en.
8) EDPB-EDPS. (2022). "*Joint Opinion 03/2022 on the Proposal for a Regulation on the European Health Data Space"*, available at https://edpb.europa.eu/system/files/2022-07/edpb_edps_jointopinion_202203_europeanhealthdataspace_en.pdf.
9) EDPS. (2015). *"Opinion 1/2015 Mobile Health: Reconciling Technological Innovation with Data Protection"*, available at https://edps.europa.eu/sites/edp/files/publication/15-05-21_mhealth_en_0.pdf.
10) EDPS. (2020). *"A preliminary opinion on data protection and scientific research*", available at https://edps.europa.eu/sites/edp/files/publication/20-01-06_opinion_research_en.pdf.
11) Tweede Kamer der Staten Generaal. (2021). *"Brief van de rapporteur Twee jaar toepassing van de AVG"*, T. van Gent (VVD), available at https://www.tweedekamer.nl/downloads/document?id=3a77e5a4-e9a6-4885-936b-ca06df416683&title=Verslag%20rapporteur%20Twee%20jaar%20toepassing%20van%20de%20AVG.pdf.

(C) White paper:

1) Pelkmans, J., & Renda, A. (2014). How can EU legislation enable and/or disable innovation. *European Commission*.
2) Renda, A., Schrefler, L., Luchetta, G., & Zavatta, R. (2013). Assessing the costs and benefits of regulation. *Brussels: European Commission*.

II - Secondary Sources

(A) Scientific research, reports, opinions, guidelines, etc.:

1) Abouelmehdi, K., Beni-Hessane, A., & Khaloufi, H. (2018). Big healthcare data: preserving security and privacy. *Journal of big data*, *5*(1), 1-18.
2) Adams, C., & Webley, P. (2001). Small business owners' attitudes on VAT compliance in the UK. *Journal of Economic Psychology*, *22*(2), 195-216.
3) Addis, M. C., & Kutar, M. (2018). The general data protection regulation (GDPR), emerging technologies and UK organisations: awareness, implementation and readiness.
4) Adner, R. (2006). Match your innovation strategy to your innovation ecosystem. *Harvard business review*, *84*(4), 98.
5) Alabdulkarim, A., Lukszo, Z., & Fens, T. W. (2012). Acceptance of Privacy-Sensitive Infrastructure Systems: A Case of Smart Metering in The Netherlands. In *Third International Engineering Systems Symposium Design and Governance in Engineering Systems*. CESUN, MIT, TU Delft.
6) Albrecht, J. (2016). Conclusion of the EU data protection reform. *Retrieved October*, *14*, 2020.
7) Alexandru, A., Alexandru, C., Coardos, D., & Tudora, E. (2016). Healthcare, big data and cloud computing. *management*, *1*(2).
8) Ambec, S., Cohen, M. A., Elgie, S., & Lanoie, P. (2013). The Porter hypothesis at 20: can environmental regulation enhance innovation and competitiveness?. *Review of environmental economics and policy*.
9) Asadi Someh, I., Breidbach, C. F., Davern, M., & Shanks, G. (2016). Ethical implications of big data analytics. *Research-in-Progress Papers*, *24*.
10) Asan, O., Bayrak, A. E., & Choudhury, A. (2020). Artificial intelligence and human trust in healthcare: focus on clinicians. *Journal of medical Internet research*, *22*(6), e15154.
11) Ashford, N. A. (1976). *Crisis in the Workplace: Occupational disease and injury: a Report to the Ford Foundation*. MIT Press.
12) Ashford, N. A. (2000). An innovation-based strategy for a sustainable environment. In *Innovation-oriented environmental regulation: theoretical approaches and empirical analysis* (pp. 67-107). Physica-Verlag HD.
13) Bachlechner, D., Van Lieshout, M., & Timan, T. (2020). Privacy as enabler of innovation. *Privacy and Identity Management. Data for Better Living: AI and Privacy: 14th IFIP WG 9.2, 9.6/11.7, 11.6/SIG 9.2. 2 International Summer School, Windisch, Switzerland, August 19–23, 2019, Revised Selected Papers 14*, 3-16.
14) Balboni, P., Pelino, E., & Scudiero, L. (2014). Rethinking the one-stop-shop mechanism: Legal certainty and legitimate expectation. *Computer law & security review*, *30*(4), 392-402.
15) Baldwin, R., Scott, C., & Hood, C. (eds) (1998). 'Introduction', in Baldwin, R., Scott, C., & Hood, C. (eds), *A Reader on Regulation, Oxford Readings in Socio-Legal Studies* (Oxford, 1998; online edn, Oxford Academic, 22 Mar. 2012), https://doi.org/10.1093/acprof:oso/9780198765295.003.0001.
16) Baldwin, R., Cave, M., & Lodge, M. (2011). *UNDERSTANDING REGULATION 2E P: Theory, Strategy, and Practice*. Oxford university press.
17) Bentzen, H. B., Castro, R., Fears, R., Griffin, G., Ter Meulen, V., & Ursin, G. (2021). Remove obstacles to sharing health data with researchers outside of the European Union. *Nature Medicine*, *27*(8), 1329-1333.

18) Bleier, A., Goldfarb, A., & Tucker, C. (2020). Consumer privacy and the future of data-based innovation and marketing. *International Journal of Research in Marketing*, *37*(3), 466-480.
19) Blind, K. (2012). The influence of regulations on innovation: A quantitative assessment for OECD countries. *Research policy*, *41*(2), 391-400.
20) Blind, K. (2016). 15. The impact of regulation on innovation. *Handbook of innovation policy impact*, *450*.
21) Blind, K., Petersen, S. S., & Riillo, C. A. (2017). The impact of standards and regulation on innovation in uncertain markets. *Research policy*, *46*(1), 249-264.
22) Buhl, H. U., Röglinger, M., Moser, F., & Heidemann, J. (2013). Big data: a fashionable topic with (out) sustainable relevance for research and practice?. *Business & Information Systems Engineering*, *5*, 65-69.
23) Bunnik, A., Cawley, A., Mulqueen, M., & Zwitter, A. (Eds.). (2016). *Big data challenges: society, security, innovation and ethics*. Springer.
24) Campbell, J., Goldfarb, A., & Tucker, C. (2015). Privacy regulation and market structure. *Journal of Economics & Management Strategy*, *24*(1), 47-73.
25) Cate, F. H., & Mayer-Schönberger, V. (2013). Notice and consent in a world of Big Data. *International Data Privacy Law*, *3*(2), 67-73.
26) Cavanillas, J. M., Curry, E., & Wahlster, W. (2016). *New horizons for a data-driven economy: a roadmap for usage and exploitation of big data in Europe*. Springer Nature.
27) Chen, M., Mao, S., & Liu, Y. (2014). Big data: A survey. *Mobile networks and applications*, *19*, 171-209.
28) Chivot, E. (2019). One year on, GDPR needs a reality check. *Financial Times*, *30*.
29) Choo, C. W. (1996). The knowing organization: How organizations use information to construct meaning, create knowledge and make decisions. *International journal of information management*, *16*(5), 329-340.
30) Christensen, L., Colciago, A., Etro, F., & Rafert, G. (2013). The impact of the data protection regulation in the EU. *Intertic Policy Paper, Intertic*.
31) Clarke, R. (2016). Big data, big risks. *Information Systems Journal*, *26*(1), 77-90.
32) Cohen, J. E. (2012). What privacy is for. *Harv. L. Rev.*, *126*, 1904.
33) Condry, M. W., & Quan, X. I. (2021). Digital health innovation, informatics opportunity, and challenges. *IEEE engineering management review*, *49*(2), 81-88.
34) Council of Europe, European Court of Human Rights, European Data Protection Supervisor, European Union Agency for Fundamental Rights, Handbook on European data protection law: 2018 edition, Publications Office of the European Union, 2019, https://data.europa.eu/doi/10.2811/343461.
35) Deloitte. (2013). Economic impact assessment of the proposed European General Data Protection Regulation.
36) Van Dijck, J., Poell, T., & De Waal, M. (2016). *De platformsamenleving: Strijd om publieke waarden in een online wereld* (p. 180). Amsterdam university press.
37) Dillon, A., & Morris, M. G. (1996). User acceptance of new information technology: theories and models.
38) Ducharme, J. (2018). A major drug company now has access to 23andMe's genetic data. Should you be concerned?. *Time Magazine*, *26*.
39) Enzmann, M., & Schneider, M. (2005). Improving customer retention in e-commerce through a secure and privacy-enhanced loyalty system. *Information Systems Frontiers*, *7*, 359-370.
40) Ettredge, M., Johnstone, K., Stone, M., & Wang, Q. (2011). The effects of firm size, corporate governance quality, and bad news on disclosure compliance. *Review of Accounting Studies*, *16*, 866-889.
41) Ferreira, C., Merendino, A., & Meadows, M. (2021). Disruption and legitimacy: big data in society. *Information Systems Frontiers*, 1-20.
42) Fosch-Villaronga, E., & Heldeweg, M. (2018). "Regulation, I presume?" said the robot–Towards an iterative regulatory process for robot governance. *Computer law & security review*, *34*(6), 1258-1277.

43) Frischmann, B. M. (2012). *Infrastructure: The social value of shared resources*. Oxford University Press.
44) Gandomi, A., & Haider, M. (2015). Beyond the hype: Big data concepts, methods, and analytics. *International journal of information management*, *35*(2), 137-144.
45) Garlasu, D., Sandulescu, V., Halcu, I., Neculoiu, G., Grigoriu, O., Marinescu, M., & Marinescu, V. (2013, January). A big data implementation based on Grid computing. In *2013 11th RoEduNet International Conference* (pp. 1-4). IEEE.
46) Gellert, R., & Gutwirth, S. (2013). The legal construction of privacy and data protection. *Computer Law & Security Review*, *29*(5), 522-530.
47) Goldfarb, A., & Tucker, C. (2012). Privacy and innovation. *Innovation policy and the economy*, *12*(1), 65-90.
48) Hartmann, P. M., Zaki, M., Feldmann, N., & Neely, A. (2016). Capturing value from big data–a taxonomy of data-driven business models used by start-up firms. *International Journal of Operations & Production Management*, *36*(10), 1382-1406.
49) Harvard Business Review Analytics Services. (2019). Leading a new era in health care. Innovation through Data-Driven Diagnostics. Research Report, available at https://diagnostics.roche.com/global/en/news-listing/2019/new-report-on-data-driven-innovation-in-healthcare-by-harvard-bu.html.
50) Hashem, I. A. T., Yaqoob, I., Anuar, N. B., Mokhtar, S., Gani, A., & Khan, S. U. (2015). The rise of “big data” on cloud computing: Review and open research issues. *Information systems*, *47*, 98-115.
51) Hayden, E. C. (2012). A broken contract. *Nature*, *486*(7403), 312-314.
52) Hemerly, J. (2013). Public policy considerations for data-driven innovation. *Computer*, *46*(6), 25-31.
53) Hendolin, M. (2022). Towards the European health data space: from diversity to a common framework. *Eurohealth*, *27*(2), 15-17.
54) Hildebrandt, M. (2015). *Smart technologies and the end (s) of law: novel entanglements of law and technology*. Edward Elgar Publishing.
55) Hoofnagle, C. J., Van Der Sloot, B., & Borgesius, F. Z. (2019). The European Union general data protection regulation: what it is and what it means. *Information & Communications Technology Law*, *28*(1), 65-98.
56) Hulsen, T., Jamuar, S. S., Moody, A. R., Karnes, J. H., Varga, O., Hedensted, S., ... & McKinney, E. F. (2019). From big data to precision medicine. *Frontiers in medicine*, *6*, 34.
57) Hulsen, T. (2021). Challenges and solutions for big data in personalized healthcare. In *Big Data in Psychiatry# x0026; Neurology* (pp. 69-94). Academic Press.
58) Iacob, N., & Simonelli, F. (2020). Towards a European health data ecosystem. *European Journal of Risk Regulation*, *11*(4), 884-893.
59) Iwaya, L. H., Ahmad, A., & Babar, M. A. (2020). Security and privacy for mHealth and uHealth systems: a systematic mapping study. *IEEE Access*, *8*, 150081-150112.
60) Jirotka, M., Procter, R., Hartswood, M., Slack, R., Simpson, A., Coopmans, C., ... & Voss, A. (2005). Collaboration and trust in healthcare innovation: The eDiaMoND case study. *Computer Supported Cooperative Work (CSCW)*, *14*, 369-398.
61) Kahn, K. B. (2018). Understanding innovation. *Business Horizons*, *61*(3), 453-460.
62) Karampela, M., Ouhbi, S., & Isomursu, M. (2019, July). Exploring users’ willingness to share their health and personal data under the prism of the new GDPR: implications in healthcare. In *2019 41st annual international conference of the IEEE engineering in medicine and biology society (EMBC)* (pp. 6509-6512). IEEE.
63) Kelly, C. J., & Young, A. J. (2017). Promoting innovation in healthcare. *Future healthcare journal*, *4*(2), 121.
64) Kim, H., Lee, J. N., & Han, J. (2010). The role of IT in business ecosystems. *Communications of the ACM*, *53*(5), 151-156.
65) Kindt, E., Fontanillo López, C. A., Bergholm, J., Czarnocki, J., Kanevskaia, O., & Herveg, J. (2021). Study on the appropriate safeguards under Article 89 (1) GDPR for the processing of personal data for scientific research.
66) Kist, I. (2022). Assessment of the Dutch Rules on Health Data in the Light of the GDPR. *European Journal of Health Law*, *30*(3), 322-344.

67) Koops, B. J., Newell, B. C., Timan, T., Skorvanek, I., Chokrevski, T., & Galic, M. (2016). A typology of privacy. *U. Pa. J. Int'l L.*, *38*, 483.

68) Kuner, C., Cate, F. H., Millard, C., & Svantesson, D. J. B. (2012). The challenge of ‘big data’for data protection. *International Data Privacy Law*, *2*(2), 47-49.

69) Kusiak, A. (2009). Innovation: A data-driven approach. *International Journal of Production Economics*, *122*(1), 440-448.

70) Laney, D. (2001). 3D data management: Controlling data volume, velocity and variety. *META group research note*, *6*(70), 1.

71) Li, H., Yu, L., & He, W. (2019). The impact of GDPR on global technology development. *Journal of Global Information Technology Management*, *22*(1), 1-6.

72) van Lieshout, M., Djafari, S., & Vermeulen, P. (2018). *Respect4U*. Den Haag: TNO.

73) van Lieshout, M., & Emmert, S. (2018). RESPECT4U–privacy as innovation opportunity. In *Privacy Technologies and Policy: 6th Annual Privacy Forum, APF 2018, Barcelona, Spain, June 13-14, 2018, Revised Selected Papers 6* (pp. 43-60). Springer International Publishing.

74) London Economics. (2017). Analysis of the potential economic impact of GDPR, available at https://londoneconomics.co.uk/wp-content/uploads/2017/10/Analysis-of-the-potential-economic-impact-of-GDPR-FINAL-October-2017.pdf.

75) Lopes, I. M., Guarda, T., & Oliveira, P. (2020). General data protection regulation in health clinics. *Journal of Medical Systems*, *44*(2), 53.

76) Malgieri, G., & Comandé, G. (2017). Sensitive-by-distance: quasi-health data in the algorithmic era. *Information & Communications Technology Law*, *26*(3), 229-249.

77) Malterud, K., Siersma, V. D., & Guassora, A. D. (2016). Sample size in qualitative interview studies: guided by information power. *Qualitative health research*, *26*(13), 1753-1760.

78) Mantelero, A. (2014). The future of consumer data protection in the EU Re-thinking the “notice and consent” paradigm in the new era of predictive analytics. *Computer Law & Security Review*, *30*(6), 643-660.

79) Manyika, J., Chui, M., Brown, B., Bughin, J., Dobbs, R., Roxburgh, C., & Hung Byers, A. (2011). *Big data: The next frontier for innovation, competition, and productivity*. McKinsey Global Institute.

80) Marelli, L., Lievevrouw, E., & Van Hoyweghen, I. (2020). Fit for purpose? The GDPR and the governance of European digital health. *Policy studies*, *41*(5), 447-467.

81) Markus, M. L. (2015). New games, new rules, new scoreboards: the potential consequences of big data. *Journal of Information Technology*, *30*, 58-59.

82) Martin, K. (2015). Ethical issues in the big data industry. *MIS Quarterly Executive*, *14*, 2.

83) Martin, N., Matt, C., Niebel, C., & Blind, K. (2019). How data protection regulation affects startup innovation. *Information systems frontiers*, *21*, 1307-1324.

84) McAfee, A., Brynjolfsson, E., Davenport, T. H., Patil, D. J., & Barton, D. (2012). Big data: the management revolution. *Harvard business review*, *90*(10), 60-68.

85) Moore, J. F. (1996). The death of competition: leadership and strategy in the age of business ecosystems. *(No Title)*.

86) Morlok, T., Matt, C., & Hess, T. (2018). Perspektiven der Privatheitsforschung in den Wirtschaftswissenschaften: Konsumentenkalkül im Neuen Kontext und Datenmärkte. *Privatheit und selbstbestimmtes Leben in der digitalen Welt: Interdisziplinäre Perspektiven auf aktuelle Herausforderungen des Datenschutzes*, 179-220.

87) Mostert, M., Bredenoord, A. L., Biesaart, M. C., & Van Delden, J. J. (2016). Big Data in medical research and EU data protection law: challenges to the consent or anonymise approach. *European Journal of Human Genetics*, *24*(7), 956-960.

88) Mulder, T. (2019). Health apps, their privacy policies and the GDPR. *European Journal of Law and Technology*.

89) Nissenbaum, H. (2011). A contextual approach to privacy online. *Daedalus*, *140*(4), 32-48.

90) OECD. (1997). *Regulatory reform and innovation*. OECD Publishing.

91) OECD. (2015). *Data-driven innovation: Big data for growth and well-being*. OECD Publishing.

92) Olaronke, I., & Oluwaseun, O. (2016, December). Big data in healthcare: Prospects, challenges and resolutions. In *2016 Future technologies conference (FTC)* (pp. 1152-1157). IEEE.

93) Perry-Kessaris, A. (2019). Legal design for practice, activism, policy, and research. *Journal of Law and Society*, *46*(2), 185-210.

94) Petts, J. (2017). Small and medium-sized enterprises and environmental compliance: Attitudes among management and non-management. In *Small and medium-sized enterprises and the environment* (pp. 49-60). Routledge.

95) Plachkinova, M., Andrés, S., & Chatterjee, S. (2015, January). A taxonomy of mHealth apps--security and privacy concerns. In *2015 48th Hawaii International Conference on System Sciences* (pp. 3187-3196). IEEE.

96) Porter, M. E., & Linde, C. V. D. (1995). Toward a new conception of the environment-competitiveness relationship. *Journal of economic perspectives*, *9*(4), 97-118.

97) Prainsack, B., & Buyx, A. (2017). *Solidarity in biomedicine and beyond* (Vol. 33). Cambridge University Press.

98) Przyrowski, C. (2018). *The GDPR and its effects on the management of private health information at different healthcare providers: A case study* (Bachelor's thesis, University of Twente).

99) Quinn, P., & Quinn, L. (2018). Big genetic data and its big data protection challenges. *Computer law & security review*, *34*(5), 1000-101.

100) Quinn, P. (2021). Research under the GDPR–a level playing field for public and private sector research?. *Life Sciences, Society and Policy*, *17*(1), 4.

101) Quinn, P., & Malgieri, G. (2021). The difficulty of defining sensitive data—The concept of sensitive data in the EU data protection framework. *German Law Journal*, *22*(8), 1583-1612.

102) Raghupathi, W., & Raghupathi, V. (2014). Big data analytics in healthcare: promise and potential. *Health information science and systems*, *2*, 1-10.

103) Raghupathi, W. (2016). Data mining in healthcare. *Healthcare Informatics: Improving Efficiency through Technology, Analytics, and Management*, 353-372.

104) Reding, V. (2012). The European data protection framework for the twenty-first century. *International Data Privacy Law*, *2*(3), 119-129.

105) Rodríguez-Mazahua, L., Rodríguez-Enríquez, C. A., Sánchez-Cervantes, J. L., Cervantes, J., García-Alcaraz, J. L., & Alor-Hernández, G. (2016). A general perspective of Big Data: applications, tools, challenges and trends. *The Journal of Supercomputing*, *72*, 3073-3113.

106) Rogers, E. (1995). Diffusion of innovations (Fourth Paperback ed.).

107) Rouvroy, A. (2016, January). Of data and men. Fundamental rights and freedoms in a world of big data. In *Report for the Council of EuropeTs Bureau of the Consultative Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data*.

108) Rustad, M. L., & Koenig, T. H. (2019). Towards a global data privacy standard. *Fla. L. Rev.*, *71*, 365.

109) Sætra, H. S. (2019). When nudge comes to shove: Liberty and nudging in the era of big data. *Technology in Society*, *59*, 101130.

110) Sagiroglu, S., & Sinanc, D. (2013, May). Big data: A review. In *2013 international conference on collaboration technologies and systems (CTS)* (pp. 42-47). IEEE.

111) Saldana, J. (2011). *Fundamentals of qualitative research*. Oxford university press.

112) Saura, J. R., Ribeiro-Soriano, D., & Palacios-Marqués, D. (2021). From user-generated data to data-driven innovation: A research agenda to understand user privacy in digital markets. *International Journal of Information Management*, *60*, 102331.

113) Schreiber, A. (2019). Feeling fine! Harmonisation and inconsistency in EU supervisory authority administrative fines. *Journal of Data Protection & Privacy*, *2*(4), 375-388.

114) Schutte, N., Bogaert, P., Saso, M., Abboud, L., & Van Oyen, H. (2021). How can population health research benefit from a European Health Data Infrastructure?. *European Journal of Public Health*, *31*.

115) Shabani, M., & Borry, P. (2018). Rules for processing genetic data for research purposes in view of the new EU General Data Protection Regulation. *European Journal of Human Genetics*, *26*(2), 149-156.

116) Shabani, M. (2022). Will the European Health Data Space change data sharing rules?. *Science*, *375*(6587), 1357-1359.

117) Singhal, S., Kayyali, B., Levin, R., & Greenberg, Z. (2020). The next wave of healthcare innovation: The evolution of ecosystems. *McKinsey & company*.

118) Sirur, S., Nurse, J. R., & Webb, H. (2018, January). Are we there yet? Understanding the challenges faced in complying with the General Data Protection Regulation (GDPR). In *Proceedings of the 2nd International Workshop on Multimedia Privacy and Security* (pp. 88-95).

119) Stewart, R. B. (1981). Regulation, innovation, and administrative law: A conceptual framework. *Calif. L. Rev.*, *69*, 1256.

120) Stewart, L. A. (2010). The impact of regulation on innovation in the United States: A cross-industry literature review. *Information technology & innovation foundation*, *6*.

121) Stone, D., & Wang, R. (2014). Deciding with data–How data-driven innovation is fuelling Australia's economic growth. *Pricewaterhouse Coopers, Melbourne*.

122) Tangari, G., Ikram, M., Ijaz, K., Kaafar, M. A., & Berkovsky, S. (2021). Mobile health and privacy: cross sectional study. *bmj*, *373*.

123) TEHDAS. (2022). Primary recommendations to foster GDPR-compliant data altruism mechanisms for the EHDS, available at https://tehdas.eu/results/tehdas-outlines-key-issues-and-considerations-on-data-altruism/#:~:text=Data%20altruism%20refers%20to%20people,and%20innovation%20without%20seeking%20reward.

124) Thierer, A., & Hagemann, R. (2015). Removing roadblocks to intelligent vehicles and driverless cars. *Wake Forest JL & Pol'y*, *5*, 339.

125) Thyve, U. F. (2016). *One-stop-shop–or not? The Regulation of competent supervisory authority in the new EU General Data Protection Regulation–does the one-stop-shop mechanism live up to its promise?* (Master's thesis).

126) Tzanou, M. (2020). The GDPR and (big) health data: Assessing the EU legislator's choices. *Health data privacy under the GDPR: Big data challenges and regulatory responses*. Routledge.

127) Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. *MIS quarterly*, 425-478.

128) De Ville, F., & Gunst, S. (2021). The Brussels Effect: How the GDPR Conquered Silicon Valley. *European Foreign Affairs Review*, *26*(3).

129) Wachter, S. (2019). Data protection in the age of big data. *Nature Electronics*, *2*(1), 6-7.

130) Westin, A. F. (1968). Privacy and Freedom, 25 Washington and Lee Law Review. 166.

131) Wigan, M. R., & Clarke, R. (2013). Big data's big unintended consequences. *Computer*, *46*(6), 46-53.

132) Wu, J., Wang, Y., Tao, L., & Peng, J. (2019). Stakeholders in the healthcare service ecosystem. *Procedia CIRP*, *83*, 375-379.

133) Yaqoob, I., Hashem, I. A. T., Gani, A., Mokhtar, S., Ahmed, E., Anuar, N. B., & Vasilakos, A. V. (2016). Big data: From beginning to future. *International Journal of Information Management*, *36*(6), 1231-1247.

134) Zarsky, T. Z. (2015). The privacy-innovation conundrum. *Lewis & Clark L. Rev.*, *19*, 115.

135) Zarsky, T. Z. (2016). Incompatible: The GDPR in the age of big data. *Seton Hall L. Rev.*, *47*, 995.

136) Ziegler, S., Evequoz, E., & Huamani, A. M. P. (2019). The impact of the European General Data Protection Regulation (GDPR) on future data business models: Toward a new paradigm and business opportunities. *Digital Business Models: Driving Transformation and Innovation*, 201-226.

137) Zillner, S., Becker, T., Munné, R., Hussain, K., Rusitschka, S., Lippell, H., ... & Ojo, A. (2016). Big data-driven innovation in industrial sectors. *New Horizons for a Data-Driven Economy: A Roadmap for Usage and Exploitation of Big Data in Europe*, 169-178.

138) Zuboff, S. (2015). Big other: surveillance capitalism and the prospects of an information civilization. *Journal of information technology*, *30*(1), 75-89.

139) Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power: Barack Obama's books of 2019*. Profile books.

(B) News articles, conferences, online sources, etc.:

1) Allain, S. (2022). *"Healthcare Innovation for All: Trust and Equity Must be a Priority"*, available at https://jnjinnovation.com/news/blog-post/healthcare-innovation-for-all-trust-and-equity-must-be-a-priority.

2) Digital Europe (2020). *"Almost two years of GDPR: celebrating and improving the application of Europe's data protection framework"*, available at https://www.digitaleurope.org/resources/almost-two-years-of-gdpr-celebrating-and-improving-the-application-of-europes-data-protection-framework/.

3) Litan, R. (2021) *"Regulation"*. Econlib, available at https://www.econlib.org/library/Enc/Regulation.html. Accessed on 30 August 2022.

4) Warc. (2013). *"Consumers show mixed views on data"*, June 27, 2013, available at https://www.warc.com/newsandopinion/news/consumers-show-mixed-views-on-data/31582.

Acknowledgments

First, I would like to express my immense gratitude to my supervisor Prof.dr. Valerie Frissen, for her support, guidance, and feedback throughout the entire thesis research and writing process. I thrive in environments that allow me to be challenged, creative, and think out of the box. This thesis is the product of my performance in such an environment, which was made possible thanks to the trust Valerie instilled in me.

Secondly, I would like to take this opportunity to thank all of the participants from different stakeholder groups in the healthcare and healthtech domains for taking part in the interviews performed as part of the qualitative research for this thesis. It is thanks to their insights and perspectives that this thesis offers a unique and valuable contribution to the field.

Thirdly, I would like to express my gratitude to Prof.dr. Eduard Fosch-Villaronga. It is thanks to his welcoming me into the world intersecting law, technology, and healthcare that I have come to be so passionate about what the future holds for this fascinating and incredibly important domain. I want to thank Eduard for encouraging me to open my eyes to the opportunities in this field of research, to step outside my comfort zone, and to be led in my choices by what I care about most.

Finally, I would like to thank my incredible parents for their unrestricted love, support, and encouragement; my brother, Dov, for being not only my brother but also one of my best friends and always putting a smile on my face thanks to his endless positivity and mischief; and my wonderful and loving partner for life, Leon, for always encouraging me to achieve my ambitions and dreams no matter how crazy they seem, for always offering a listening ear, and for being my rock day in and day out.

Hadassah Drukarch
July 10, 2023
Amsterdam, The Netherlands

Annex

Annex 1: Interview information sheet

Research project:	Innovate, comply or die? An analysis of the GDPR's impact on data-driven innovation in the healthcare industry and recommendations for future policy response at the EU level
Context:	Master Thesis – Advanced LL.M. in Law and Digital technologies
Institution(s):	Leiden University – Leiden law School
Project Leader/Interviewer:	Hadassah Drukarch
Supervision:	Prof.dr. V.A.J. Frissen (Leiden University)

Objectives of the study

The study aims to answer the following main research question: '**How does the GDPR impact data-driven innovation in the healthcare industry, and what policy response should this prompt at the EU level in light of the ongoing development of the European Data Strategy?**' As such, this thesis seeks to analyse the impact of the GDPR on DDI in the healthcare industry, and then – on the basis of this assessment and analysis – aims to put forward empirically grounded recommendations for future policy response at the EU level, taking into account ongoing developments in light of the European Data Strategy. To this end, this research comprises a literature review and interviews with different expert groups.

Participants

5-10 experts from two different stakeholder groups will be interviewed to provide as broad a picture of the DDI landscape within the healthcare industry as possible and make it comparable. The selection of participants is based on their level of expertise and experience in the field in a position responsible for various aspects surrounding digitalization, thereby ensuring a high level of quality of the research results.

Further information

The research is conducted solely for the master's thesis of Hadassah Drukarch and serves to obtain the degree 'LL.M. in Law and Digital Technologies' at Leiden University. The thesis supervisor at Leiden University is Prof.dr. V.A.J. Frissen and no external parties are involved. The results of this thesis will be presented in the form of the complete master thesis and, with the results, a publication in a scientific journal is aimed. Participants will partake in an interview lasting approximately one hour and which will take place online, via the Zoom video conferencing platform (official Leiden University account), recorded, and subsequently analysed. The interview will take place in the period from March-June 2023 and will last approximately one hour and will mainly report on challenges and potentials from the personal perspective of the participants. Participation in the interview is voluntary, and participants have the right to revoke their consent at any time and may opt out of the study or individual elements/questions without reason, and without being disadvantaged by refusal or revocation.

Important: All data will be handled in accordance with data secrecy and GDPR requirements.

The results of this thesis will be presented in the form of the complete master thesis, and will be sent to all participants as well as to relevant policymakers. The interviewer, who will carry out the scientific analysis of the interview text, is committed to data secrecy and handles the interviews in accordance with the obligations set forth in the European Union's General Data Protection Regulation (GDPR). In this regard, audio files of the interview will be stored with anonymized labels in a dedicated Google Drive folder and will be deleted once the project has ended (i.e. after grading of the master thesis), and at the latest by the 30th of September 2023. For any questions regarding this thesis, participants may reach out at any time through the contact details provided below.

Contact details

Hadassah Drukarch | h.g.drukarch@umail.leidenuniv.nl.

Annex 2: Interview consent form

Research project:	Innovate, comply or die? An analysis of the GDPR’s impact on data-driven innovation in the healthcare industry and recommendations for future policy response at the EU level
Context:	Master Thesis – Advanced LL.M. in Law and Digital technologies
Institution(s):	Leiden University – Leiden law School
Project Leader/Interviewer:	Hadassah Drukarch
Supervision:	Prof.dr. V.A.J. Frissen (Leiden University)
Interview date:	______________________
Interview ID:	______________________

The interview participant (hereafter: ‘I’) hereby agrees to participate in an interview as part of the above-mentioned research project. For this purpose, I have been informed about the aim and the process of the research project, have received, and read the interview information sheet, and agree to the recording of the interview under these conditions.

Purpose and handling of the interview
Recording of the interview is required, and the interview will be conducted and recorded online, via the Zoom video conferencing platform (official Leiden University account). The interview will subsequently be analysed. Finally, the scientific analysis of the interview text is carried out by the interviewer. The findings following from qualitative analysis of all conducted interviews across various expert groups and participants will serve as a basis for focussed insights and subsequent recommendations for action.

Commitment to privacy and data protection
The interviewer is committed to data secrecy and handles the interviews in accordance with the obligations set forth in the European Union's General Data Protection Regulation (GDPR). In this regard, audio files of the interview will be stored with anonymized labels on a dedicated Google Drive folder and will be deleted once the project has ended (i.e. after grading of the master thesis), and at the latest by the 30th of September 2023.

Consent
My participation in the interview and my consent to the use of the data as described above are voluntary. I agree that individual sentences from the recordings that are anonymized may be used as material for scientific and educational purposes. Moreover, I have been informed and agree that publication in a scientific journal will be aimed at with the results of the thesis. Finally, I have the right to revoke my consent at any time and may opt out of the study or individual elements/questions without reason, and without being disadvantaged by refusal or revocation.

Under the conditions set forth above, I agree to participate in the interview and consent to it being recorded and analysed.

______________________	______________________
Place, date, signature of interview participant	Place, date, signature of the interviewer

Contact details
Hadassah Drukarch | h.g.drukarch@umail.leidenuniv.nl.

Annex 3: Interview outline

General information regarding the thesis project	
Research project:	Innovate, comply or die? An analysis of the GDPR's impact on DDI in the healthcare industry and recommendations for future policy response at the EU level
Context:	Master Thesis – Advanced LL.M. in Law and Digital technologies
Institution(s):	Leiden University – Leiden law School
Project Leader/Interviewer:	Hadassah Drukarch
Supervision:	Prof.dr. V.A.J. Frissen (Leiden University)
Interview date:	---
Interview ID:	---
Interview outline	
BLOCK 1	
1. Welcome and thanks for participation in the interview.	
2. Round of (personal) introductions.	
3. Presentation of the privacy terms and room for questions regarding the interview information sheet and consent form.	
4. Introduction of the technical framework used to conduct the interview (audio recording) and practical information regarding the interview process.	
5. Introduction of the research topic and objective(s) and a description of the formal framework of the thesis.	
BLOCK 2	
6. Start audio recording.	
BLOCK 3	
7. Introduction 3rd block of the interview – impact of the GDPR on DDI in the healthcare industry.	
8. How has the theoretical framework of the GDPR impacted the DDI landscape in the healthcare industry? **8.1.** To what extent has the theoretical framework of the GDPR hampered DDI in the healthcare industry? **8.2.** To what extent has the theoretical framework offered room to and created new opportunities for DDI in the healthcare industry?	• Anticipate statements throughout the interview; • Assess understanding through paraphrasing to ensure everything was understood correctly; • Critical follow-up (where necessary/relevant). • Introduce a change of perspective (where necessary/relevant).
9. How has the interpretation and enforcement of the GDPR impacted the DDI landscape in the healthcare industry? – focus on EU competent authorities, DPA's and courts.	• Anticipate statements throughout the interview; • Assess understanding through paraphrasing to ensure everything was understood correctly;

	● Critical follow-up (where necessary/relevant). ● Introduce a change of perspective (where necessary/relevant).
BLOCK 4	
10. Introduction 4th block of the interview – necessary EU policy response in light of the European Data Strategy.	
11. What are the challenges and opportunities associated with the development of the European Data Strategy for DDI in the healthcare industry? **11.1.** How are ongoing regulatory developments in light of the European Data Strategy perceived from the perspective of DDI in the healthcare industry? Focus on: Data Governance Act, EHDS, Data Act. **11.2.** How are these developments expected to practically align with the GDPR and impact upon the DDI landscape in healthcare?	● Anticipate statements throughout the interview; ● Assess understanding through paraphrasing to ensure everything was understood correctly; ● Critical follow-up (where necessary/relevant). ● Introduce a change of perspective (where necessary/relevant).
12. What policy response should be prompted at the EU level in light of the ongoing development of the European Data Strategy? **12.1.** To what extent should the GDPR make more room for the further facilitation of DDI, with a specific eye on data-driven healthcare innovation? **12.2.** What policy response is necessary to move forward with an eye on the responsible facilitation of DDI in the healthcare industry?	● Anticipate statements throughout the interview; ● Assess understanding through paraphrasing to ensure everything was understood correctly; ● Critical follow-up (where necessary/relevant). ● Introduce a change of perspective (where necessary/relevant).
13. What other steps are necessary to ensure the effective, efficient and responsible progression of DDI in the healthcare industry? **13.1.** At the industry level? **13.2.** At the organisational level?	● Anticipate statements throughout the interview; ● Assess understanding through paraphrasing to ensure everything was understood correctly; ● Critical follow-up (where necessary/relevant). ● Introduce a change of perspective (where necessary/relevant).
BLOCK 5	
14. Summary of the interview and outlook.	
15. Conclusion and wrap-up of the interview and discussion.	