Stanford – Vienna
Transatlantic Technology Law Forum

A joint initiative of
Stanford Law School and the University of Vienna School of Law

European Union Law Working Papers

No. 88

The Interplay Between the European Health Data Space Act and the GDPR: Secondary Use of Health Data and Its Protection

Ivana Máthéová

2024

European Union Law Working Papers

Editors: Siegfried Fina and Roland Vogl

About the European Union Law Working Papers

The European Union Law Working Paper Series presents research on the law and policy of the European Union. The objective of the European Union Law Working Paper Series is to share "works in progress". The authors of the papers are solely responsible for the content of their contributions and may use the citation standards of their home country. The working papers can be found at http://ttlf.stanford.edu.

The European Union Law Working Paper Series is a joint initiative of Stanford Law School and the University of Vienna School of Law's LLM Program in European and International Business Law.

If you should have any questions regarding the European Union Law Working Paper Series, please contact Professor Dr. Siegfried Fina, Jean Monnet Professor of European Union Law, or Dr. Roland Vogl, Executive Director of the Stanford Program in Law, Science and Technology, at:

Stanford-Vienna Transatlantic Technology Law Forum
http://ttlf.stanford.edu

Stanford Law School
Crown Quadrangle
559 Nathan Abbott Way
Stanford, CA 94305-8610

University of Vienna School of Law
Department of Business Law
Schottenbastei 10-16
1010 Vienna, Austria

About the Author

Ivana Máthéová earned her Bachelor of Laws (LL.B.) in International and European Law from The Hague University of Applied Sciences in 2022 and furthered her studies with a Master of Laws (LL.M.) in European and International Business Law at the University of Vienna, Austria. During her academic journey, Ivana undertook a minor in Compliance and completed an internship at the Permanent Representation of Slovakia to the EU, in the department of digitalization.

With practical experience in corporate law and data protection gained at a law firm in Slovakia, Ivana currently serves as a legal trainee at *noyb.eu*, focusing on strategic litigation to strengthen privacy rights.

General Note about the Content

The opinions expressed in this student paper are those of the author and not necessarily those of the Transatlantic Technology Law Forum, or any of TTLF's partner institutions, or the other sponsors of this research project.

Acknowledgments

I extend my sincere appreciation to Dr. Lukas Feiler, SSCP, CIPP/E, my thesis supervisor, for his invaluable guidance and for entrusting me with the opportunity to conduct this research. Additionally, I am profoundly grateful to my family for their unwavering support, encouragement, and belief in my academic pursuits. Lastly, I extend my thanks to everyone else who supported me throughout this research journey. Your collective support has been an essential cornerstone in the completion of this thesis.

Suggested Citation

This European Union Law Working Paper should be cited as:
Ivana Máthéová, The Interplay Between the European Health Data Space Act and the GDPR: Secondary Use of Health Data and Its Protection, Stanford-Vienna European Union Law Working Paper No. 88, http://ttlf.stanford.edu.

Copyright

Abstract

In the wake of the post-pandemic era, the reuse of existing data for scientific research has emerged as a critical policy focus. This thesis delves into the European Commission's 2022 proposal, aimed at establishing a sector-specific regulation governing the secondary use of health data within the European Union and its interplay with the General Data Protection Regulation (‘GDPR’). This ambitious initiative seeks to harness the potential of novel technologies while streamlining administrative processes. However, the pursuit of efficiency often implicates compromises in privacy and fosters power imbalances and therefore does not result in an alignment with the GDPR. This research underscores the importance of aligning the proposed regulations with the GDPR's principles and safeguards, particularly concerning the handling of sensitive personal health data. The GDPR mandates stringent rules to protect health data due to the profound economic, psychological, and societal harms that unauthorized access or sharing may pose. By illuminating these ethical quandaries, this thesis aims to advocate for a balanced approach that upholds both efficiency and privacy while leveraging emerging technologies for scientific progress within the EU.

Key words

European Health Data Space, General Data Protection Regulation, health data, sensitive data, secondary use of data, data processing, privacy protection

TABLE OF CONTENTS

Abbreviations

CBHC	the Cross Border Health Care Directive
COVID-19	the severe acute respiratory syndrome coronavirus 2 or SARS-CoV-2
DG	the Directorates-General
DGA	the Data Governance Act
EDPB	the European Data Protection Board
EDPS	the European Data Protection Supervisor
EHDS	the European Health Data Space
EHR-S	the Electronic Health Record Systems
EY	the Ernst & Young Global Limited
GDPR	the General Data Protection Regulation
EU	the European Union
NGO	the non-governmental organization
TFEU	the Treaty on the Functioning of the European Union
TEHDAS	the Towards the European Health Data Space

1. INTRODUCTION

On 3 May 2022, the European Commission published a proposal for the European Health Data Space Act (hereinafter referred as 'EHDS'; 'Proposal').[1] Its aim is to promote safe cross-border exchange and control of patients' data as well as support research on treatments, medicines, medical devices, and outcomes.[2] Such should be achieved through development of electronic health record systems (hereinafter referred as 'EHR-S') for *primary use* to deliver healthcare for individuals from whose data were collected and for *secondary use* to improve research, innovation and policy making.[3] To make the EHDS successful, the data processing of such sensitive nature will, therefore, require robust legal basis in line with the European Union (hereinafter referred as 'EU') data protection law.[4]

At this moment, the proposal mentions merely general references to the General Data Protection Regulation (hereinafter referred as 'GDPR' or 'the Regulation')[5] which may not suffice as it creates wide rights and obligations with regard to the access, use and sharing of special categories of data – health data. This increases the risk of misinterpreting provisions related to data protection, thus, leading to lowering the level of GDPR data protection currently enjoyed in the EU.

---

[1] European Parliament, European health data space (*Europarl.europa.eu,* 6 December 2023) < https://www.europarl.europa.eu/thinktank/sk/document/EPRS_ATA(2023)754642> accessed 10 December 2023

[2] ibid

[3] ibid

[4] European Data Protection Board, European Data Protection Supervisor, 'EDPB-EDPS Joint Opinion 03/2022 on the Proposal for a Regulation on the European Health Data Space' (2022) < https://edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-032022-proposal_en> accessed 10 December 2023, para 12

[5] Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L 199/1

There are many aspects of the Proposal which go against generally acceptable rules of the GDPR. First and foremost, to make processing of health data legitimate under the GDPR, the EHDS makes use of the exception offered by Article 9(2)(g), (i) and (j) GDPR[6]. Meeting the requirements for the use of this legal basis can be achieved by providing suitable and specific safeguards to protect data subjects' legitimate interests. However, given the fact that the law makers propose to create access to restricted health data to all health professionals[7], restricting the right to information[8], allowing processing for secondary use of data derived from potentially dangerous wellness applications[9] and other rather controversial provisions raise serious doubts about the Proposal's compatibility with the GDPR.

The main issues foreseen so far are related to the secondary use of clinical data in Chapter IV of the Proposal. The concept of secondary use does not appear in the GDPR. In fact, it is explicitly prohibited by the principle of purpose limitation as per Article 5(1)(b) GDPR which is restricting further processing of collected data.[10] The Proposal opens a possibility for further processing of data for potentially any form of innovation activities contributing to public health or social security. However, the Proposal does not create criteria consistent with Article 9 GDPR which should serve as a basis for health data access bodies which assess and decide on data applications to issue data permits for processing.[11] As much as the authors of the Proposal aim to generate considerable benefits for the public good through the introduction of this concept, the focus should be put on the maintenance of balance with horizontal principle adopted under Article 16 of the

[6] ibid art 9(2)(g), (i), (j)
[7] European Commission, 'Proposal for a Regulation of the European Parliament and of the Council on the European Health Data Space', COM (2022) 197 final, art 4(1)
[8] ibid, art 38(2)
[9] ibid, art 1(3)(a)
[10] GDPR (n 5) art 5(1)(b)
[11] Joint Opinion EDPB-EDPS (n 4) para 92

Treaty on the Functioning of the European Union (hereinafter referred to as 'TFEU')– '*everyone has the right to the protection of personal data concerning them'.*[12] Indeed, healthcare systems need to react to the developments of digital economy also accelerated by the recent COVID-19 pandemic. Nevertheless, the interplay between the EHDS and the GDPR will be an important aspect to consider in order to ensure the safe and responsible use of health data in the EU.

2. EUROPEAN HEALTH DATA SPACE

2.2. Objectives of the EHDS

The Proposal for the EHDS represents a pivotal initiative within the EU, reflecting the ongoing transformation of healthcare in the digital age. The EHDS envisions to address challenges related to electronic health data access by creating a framework for secure and interoperable exchange of health data across the EU.[13] Adopting the EHDS will among other things enable patients to easily control their health data and researchers, innovators, and policy makers to have access to such data.[14] To understand the significance of this Proposal, it is essential to delve into the background of its development and the motivations driving it.

The EU exerts a diligent effort into building a strong European Health Union, in which the Member States work together in preparation and response to health crisis, disease management, covering preparation, treatment and aftercare and prevention of shortage of medical supplies.[15] Today, the fragmented nature of health data across the EU Member States which adapt uneven standards in interoperability and legal frameworks poses various challenges. Although the provisions of the

---

[12] Consolidated version of the Treaty on the Functioning of the European Union [2012] OJ C326/47 (TFEU) art 16
[13] EHDS (n 7) Explanatory Memorandum, p 1
[14] ibid
[15] Cyber Risk GmbH, 'The European Health Data Space (EHDS)' (*European-helath-data-space.com,* 2022) <https://www.european-health-data-space.com/> accessed 10 December 2023

GDPR guarantee rights of natural persons over their health data, the same certainty, in terms of the GDPR interpretation is not provided to individuals or entities who want to access and use the data for secondary purpose. The researchers, healthcare professionals or innovators in question face these challenges due to inconsistent interpretation of the Regulation in various Member States.[16] This becomes an issue especially in cross-border research collaborations and healthcare services. Therefore, organizations that operate in multiple Member States may find it challenging to comply with those different interpretations which often results in increased administrative burden and compliance costs.[17]

The lack of common framework for the management of health data appeared to pose a key barrier to COVID-19 scientific research.[18] The COVID-19 pandemic has, as a result, fuelled the debate on the need for cross-border cooperation and has shown the importance of use and re-use of electronic health data.[19] It comes as no surprise, that the secondary use of health data became the central concern and that the EHDS now serves as the response to these challenges.

The Joint Action Towards the European Health Data Space (hereinafter referred as 'TEHDAS') is a health programme launched under the EU Action in the Field of Health with a vision to explore opportunities for data governance models.[20] One of TEHDAS working packages named 'Sharing Data for Health' aims to develop concepts for exchanging health data for secondary purpose and

[16] EHDS (n 7) Explanatory Memorandum, p 1
[17] EHDS (n 7) Explanatory Memorandum, p 17
[18] ibid
[19] McLennan S, Celi LA, Buyx A, 'COVID-19: Putting the General Data Protection Regulation to the Test' [2020] JMIR Public Health Surveill 6
[20] Towards the European Health Data Space, 'Joint Action Towards the European Health Data Space – TEHDAS' (2022) < https://tehdas.eu/> accessed 10 December 2023

provide recommendations to Member States on national legislations which would enable cross-border data sharing.[21]

The results of the health programme's research ascertained barriers to such sharing under the GDPR.[22] In light of these findings, the research was coupled with the real-life experience to provide evidence on the impact of these results to data users. TEHDAS discovered that not only the EU countries fail to evenly interpret the GDPR provisions in relation to secondary use of health data, but the Member States also lack a common interpretation of what is or is not considered the secondary use of data.[23] To be more specific, the concept of secondary use lacks legal basis across all Member States, and a distinct demarcation between primary and secondary use is notably absent in the national legislations.[24]

TEHDAS is not the only programme highlighting this very issue. It has been also identified by the DG Health and Food Safety study[25] that impact of the unclear and inconsistent application of this terminology poses considerable challenges during the consent acquisition process. This ambiguity can result in difficulties in interpreting the scope of individuals' consent, making it challenging to discern the specific elements to which individuals have given their consent. Moreover, such

[21] Towards the European Health Data Space, 'Packages' (2022) < https://tehdas.eu/packages/> accessed 10 December 2023
[22] Towards the European Health Data Space, 'Member states' readiness to benefit from the EHDS regulation varies' (2023) <https://tehdas.eu/results/member-states-readiness-to-benefit-from-the-ehds-regulation-varies/> accessed 10 December 2023
[23] ibid
[24] Towards the European Health Data Space, 'TEHDAS study: Member states to harmonize national legislation to enable the secondary use of health data (2023) <https://tehdas.eu/results/tehdas-study-member-states-to-harmonise-national-legislation-to-enable-the-secondary-use-of-health-data/> accessed 10 December 2023
[25] European Commission (DG Health and Food Safety), 'Assessment of the EU Member States' rules on health data in the light of GDPR' (2021) p 14

uncertainties can present obstacles for ethical review boards in their efforts to decide whether valid consent has indeed been granted.

2.3. Outline of the Proposal

The EHDS Proposal comprises 76 articles, delineating its comprehensive framework.[26] The proposal is structured around two distinct pillars, each addressing critical aspects of health data management within the EU. The first pillar spans Articles 1 to 32 and predominantly focuses on primary health data-related concerns. It encompasses pivotal aspects such as the design and implementation of electronic health registers, ensuring interoperability of EHR-S across EU Member States, and the formulation of regulations governing wellness applications. While this pillar introduces intriguing elements, notably the self-regulatory powers for developers of wellness applications, the primary focus of this paper centres on the second pillar.

Spanning Articles 32 to 58, the second pillar marks a significant milestone by establishing the foundational framework for the secondary use of health data within the EU. This paper will warrant scrutiny through a systematic analysis of its provisions, shedding light on several critical points. Specifically, the challenges in obtaining the consent for the secondary use data processing, access to and potential misuse of sensitive health data and other privacy issues stemming from rather controversial provisions of the Proposal.

2.4.Building European Health Union – legal basis

Historically, the EU has provided competence to individual Member States to determine their own

[26] EHDS (n 7)

health policies, therefore, they retain a national control over the health-related aspects and collaborate only in clear cross-border dimension cases.[27] As the COVID-19 pandemic has fuelled the debate on the need to improve the resilience of the EU's health systems, new series of legislation is being translated into a policy frame called 'European Health Union'. The EHDS is a building central block of this initiative and a milestone in EU's digital transformation.[28]

The EHDS Proposal draws its legal foundation from two pivotal articles, namely Articles 16 and 114 of the Treaty on the Functioning of the European Union (TFEU).[29] The primary aim of Article 114 TFEU is to streamline the functioning of the internal market by aligning national regulations.[30] According to the explanatory memorandum, the choice of Article 114 TFEU as the appropriate legal basis is based on the fact that the majority of provisions within the Proposal seek to enhance the operation of the internal market and facilitate the free movement of goods and services.[31] This stems from the fact that some Member States have taken regulatory actions to regulate EHR-S, while others have not, therefore, leading to divergent rules and practices across the EU.[32] Consequently, this legislative fragmentation potentially imposes compliance burden on companies which operate under different regulatory regimes.

Whilst Article 114 TFEU approximates the national rules and is suitable for actions related to public health protection[33], the other, inseparably linked legal basis for this Proposal is Article 16

---

[27] Tugce Schmitt and others, 'What does it take to create a European Health Data Space? International commitments and national realities' (2023) Vol 179 Zeitschrift für Evidenz, Fortbildung und Qualität im Gesundheitswesen 1, 3

[28] European Commission, European Health Union: Protecting our health together' <https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/promoting-our-european-way-life/european-health-union_en> accessed 10 December 2023

[29] Consolidated version of the Treaty on the Functioning of the European Union [2012] OJ C326/47 (TFEU) art 16, 114

[30] TFEU (n 29) art 114

[31] EHDS (n 7) Explanatory Memorandum, p 6

[32] ibid

[33] TFEU (n 29) art 114

TFEU to effectively safeguard the electronic health data protection.[34] The Article 16 TFEU establishes the right of individuals to the protection of their personal data concerning them and for this reason, it also serves as a legal basis for the GDPR and reinforces its objectives by emphasizing the importance of personal data protection as a fundamental right.[35]

The protection of the electronic health data is intricately linked to the EHDS as it strives to establish a comprehensive framework which enables responsible and secure data sharing.[36] According to the GDPR, health data is recognized as a "special category of data" which encompasses any information about an individual's health status, revealing details about their past, present, or potential future conditions.[37]

The GDPR is a comprehensive piece of legislation. It, thus, outlines applicable rules to the handling of sensitive health information for scientific research purposes under a special derogatory regime as per Article 6 and 9 GDPR.[38]

To conclude, the EU's aim to create a European Health Union by adopting the EHDS as its building block finds its legal basis in the Article 16 and 114 of the TFEU to harmonise the internal market and guarantee the protection of the personal data involved as well as the GDPR provisions regulating the processing of such sensitive data.

2.5. Consistency with other EU provisions in the policy area

[34] TFEU (n 29) art 16
[35] TFEU (n 29) art 16(2)
[36] EHDS (n 7) Explanatory Memorandum, p 2
[37] GDPR (n 5) Recital 35
[38] GDPR (n 5) art 6, art 9

Apart from the GDPR, the Proposal will become part of a much broader legal framework established by the EU contributing to the formation of the European Health Union. It concerns legislations such as Data Governance Act ('DGA'), Data Act, Medical Devices Regulation, the Network, and Information System Directive and Cross Border Health Care Directive ('CBHC Directive').[39] Although the cross-border exchange of electronic health data is to a certain extend covered by the CBHC Directive, the rights on the use of electronic health data are limited.[40] In 2011, the legislation established merely a voluntary body of experts working to promote EU-wide interoperability of electronic health data. However, its provisions are voluntary in nature and thus significantly limiting the access and control over natural person's electronic health data.[41] This is why the more robust and binding framework is needed to meet the expectations presented during the proposal phase of the CBHC, however, were not effective in practice. The EHDS should address this shortcoming.

The Proposal also marks the initial effort to establish a unified framework within the EU for the secondary use of health data. It can be perceived as a specialized structure governing data management within the broader context outlined by the DGA. There is a considerable overlap between the provisions of both frameworks, exemplified by instances such as making information available through the DGA's single information points aligning with the Proposal's introduction of

[39] Regulation 2022/868 of the European Parliament and of the Council on European Data Governance (Data Governance Act) [2022] OJ L 152/1; European Commission, 'Proposal 2022/0047 (COD) for a Regulation of the European Parliament and of the Council on harmonized rules on fair access to and use of data (Data Act)' COM(2022) 68 final; Regulation (EU) 2017/745 of the European Parliament and of the Council on medical devices (Medical Devices Regulation) [2017] OJ L 117/1; Directive (EU) 2016/1148 of the European Parliament and of the Council concerning measures for a high common level of security of network and information systems across the Union [2016] OJ L 194/1; Directive 2011/24/EU of the European Parliament and of the Council of 9 March 2011 on the application of patients' rights in cross-border healthcare [2011] OJ L 88/45

[40] EHDS (n 7) Explanatory Memorandum, p 3

[41] EHDS (n 7) Explanatory Memorandum, p 8

national datasets for electronic health data.[42] Additionally, the Proposal integrates the notion of data altruism in healthcare, making explicit references to corresponding provisions within the DGA[43]. However, a significant distinction lies in the fact that while the DGA presents a general framework for the secondary use of public sector data, the Proposal establishes a legal right specifically for such utilization in the realm of electronic health data. Moreover, whereas the Data Act confines public sector access to private entity-held data strictly to cases of public emergencies, the Proposal extends this scope to enable public sector entities to acquire necessary information for fulfilling their law-assigned duties, constituting a slight advancement of the draft regulation.[44] As a result, the EHDS builds on the existing legal framework concerning the sharing and utilization of data. However, the proposed mechanism for processing health data goes beyond the already established norms, making data widely accessible and thus is considered a bold move by the EU Commission in its attempt to regulate the sensitive health data secondary use.[45]

2.6.Planned Governance

In response to the evolving landscape of healthcare and the urgent need for streamlined access to electronic health data across Europe, the Proposal heralds a pivotal transformation in data governance mechanisms. At its core lies the inception of health data access bodies, robust entities entrusted with unparalleled powers and responsibilities pivotal to the EHDS.

---

[42] EHDS (n 7) art 37 (1) (q); art 37 (1) (i)
[43] EHDS (n 7) art 40; Recital 45
[44] EHDS (n 7) art 48
[45] Alex Rajagopalan, 'Shooting For The Stars: The Bold European Health Data Space (EHDS) Proposed By The EU Commission' (*Informationgovernanceservices*, 13 May 2022) <https://www.informationgovernanceservices.com/shooting-for-the-stars-the-bold-european-health-data-space-ehds-proposed-by-the-eu-commission/> accessed 10 December 2023

The pioneering concept – the health data access bodies – will orchestrate the aggregation, management, and controlled access to electronic health data for secondary use.[46] These bodies, fostered within each Member State, stand as independent entities, yet subjected to financial monitoring and judicial review to ensure transparency and accountability.[47] These bodies, fuelled by financial support from Member States, operate with a partially self-sustainable model.[48] Revenue streams are diversified through fees levied on data applications and usage, ensuring sustainable operations while offsetting costs.[49]

2.6.1. Transparent Collaboration and Governance Structure

Encouraging collaboration stands at the heart of the EHDS ethos. Health data access bodies are explicitly encouraged to engage and collaborate with supervisory authorities, ensuring compliance, ethical practices, and aligning with stakeholders' perspectives.[50] Notably, stakeholders encompass patient organizations, healthcare professionals, and researchers, fostering a comprehensive approach to data governance.[51] The composition of these bodies remains open-ended, devoid of explicit limitations on participation or stipulations mandating civil service status. However, stringent conflict of interest guidelines will govern the conduct of staff members, ensuring unbiased decision-making. Article 36 (3) EHDS reinforces the autonomy of health data access bodies, emphasizing their independence from external influence in decision-making processes.[52]

---

[46] EHDS (n 7) art 37
[47] Petros Terzis, 'Compromises and Asymmetries in the European Health Data Space' [2022] Eur J Health Law 345, 349
[48] ibid
[49] EHDS (n 7) art 42
[50] ibid art 36 (1)
[51] ibid
[52] ibid art 36 (6)

2.6.2. Centralization, Mediation and Access Control

The pivotal role of health data access bodies extends beyond mere aggregation. They serve as the central nexus, consolidating information gathered from a myriad of public and private databases and applications.[53] Armed with this aggregated knowledge, these bodies meticulously moderate and mediate access to health data, strictly adhering to the EHDS framework.[54]

Crucially, Recital 55 EHDS underlines the importance of a secure processing environment, envisaging a technical infrastructure that mitigates privacy risks.[55] This setup acts as a shield, preventing direct transmission of electronic health data to data users which enables secure processing. Emphasizing and prioritizing such secure transfer and processing of health data, stringent provisions govern the safe exchange of data to and from the databases managed by health data access bodies.[56] These protocols underscore the commitment to data security, integrity, and confidentiality throughout the data lifecycle.

2.6.3. Role of the Health Data Access Bodies

To sum up this structured framework, the role of these access bodies embodies a multifaceted nature, entailing an array of obligations and responsibilities. These responsibilities encompass the following pivotal tasks.

To begin with, health data access bodies hold the authority to adjudicate on health data applications, an essential gateway through which entities seeking access must pass.[57] Their

[53] Compromises and Asymmetries in the European Health Data Space (n 47) 350
[54] EHDS (n 7) art 38
[55] EHDS (n 7) recital 55
[56] ibid art 50
[57] ibid art 37

decisions bear the weight of ensuring compliance with regulations, safeguarding privacy, and aligning with the overarching objectives of the EHDS. Ensuring the confidentiality of intellectual property rights remains integral and forms an important part of its role. Health data access bodies bear the onus of safeguarding these rights while managing the infrastructure that serves as the repository for health data, a fortress against breaches and unauthorized access. They undertake the task of making pertinent information related to their databases accessible to the public.[58]

Additionally, they hold the mandate to supervise both data holders (e.g. health-care professionals, hospitals, or insurers) and users, monitoring adherence to protocols, security measures, and ethical standards.[59]

2.6.4. Managing data for secondary purpose - procedure

In the pursuit of enabling a comprehensive and regulated utilization of health data for secondary purposes within Member States, a structured process has been established. According to many scholars, it is important that this procedure ensures compliance, transparency, and responsible handling of sensitive health-related information.[60] Entities operating within the healthcare sector, holding data falling within the 15 categories of health data as outlined in Article 33 EHDS, are mandated to disclose details about such data to the designated health data access body of a Member State.[61]

[58] ibid art 37 (1) (q)
[59] ibid art 37
[60] Giorgia Bincoletto, 'Scientific Research Processing Health Data in the European Union: Data Protection Regime vs. Open Data' (2023) 11 J Open Access L 1, 2
[61] EHDS (n 7) art 33

The Commission retains the authority to specify the essential information elements data holders must furnish regarding datasets and their characteristics through implementing acts.[62] The catalogue compiled and published by the health data access body encompasses comprehensive information regarding the source and nature of electronic health data, alongside the terms and conditions for accessing this data. To gain access to the data, individuals or organizations, whether legal or natural persons, can then apply to the health data access body for a 'data permit' aligned with the stipulated provisions and purposes of the Proposal.[63] Upon receipt of an application, the health data access body is mandated to respond within a 30-day timeframe.[64] Failure to do so within this duration necessitates the automatic issuance of the data permit. Once granted, the health data access body orchestrates access to the data within a secure processing environment, ensuring that the data remains within the designated depository without leaving its confines.[65] Under the terms of the data permit, both the data user and the health data access body share joint control over the accessed data.[66] Typically, accessed data undergoes anonymization unless the applicant presents justifiable reasons for requiring access in a pseudonymized format. Non-cooperation or lack of good faith with the health data access bodies may result in penalties or exclusion from participation in the EHDS.[67]

Additionally, within this envisioned framework, decentralized health data access bodies will oversee broad categories of health data within Member States. All data will integrate into

[62] ibid, art 55
[63] ibid, art 37 (1) (q) (i)
[64] ibid, art 37 (1) (q) (ii)
[65] Giorgia Bincoletto, 'Scientific Research Processing Health Data in the European Union: Data Protection Regime vs. Open Data' (2023) 11 J Open Access L 1, 15
[66] ibid, art 51
[67] ibid, art 44 (3); art 45 (2) (d); art 45 (4); art 45 (5)

HealthData@EU, a cross-border infrastructure for secondary health data usage.[68] The development of this infrastructure and interactions among stakeholders will be overseen by the newly established European Health Data Space Board, tasked with coordinating standards for interoperability among health databases across Member States.[69]

All in all, the proposed framework for managing health data for secondary purposes within Member States appears to offer a balanced approach, aiming to enable access while upholding data protection under GDPR obligations. By emphasizing transparency, controlled access, and clear guidelines, it strives to ensure the safe and practical utilization of health data for research and services. However, its effectiveness will rely heavily on meticulous implementation and ongoing adherence to GDPR principles to strike a harmonious balance between data accessibility and privacy protection which will be discussed in the following chapter.

3. SECONDARY HEALTH DATA PROCESSING IN THE GDPR FRAMEWORK

3.2. Sensitive data – data concerning health

As previously pointed out, the regulatory framework for the processing of personal data, including sensitive data is laid down in the GDPR. The purpose of this regulation is not only to "*lay down rules relating to the protection of natural persons with regard to the processing of personal data"* but also "*rules relating to free movement of such data."*[70] Both aims, protecting the rights of individuals and facilitating the free flow of data, are its cornerstones. In the realm of the EHDS Proposal, the term "electronic health data" holds paramount importance. It refers to personal and

[68] ibid, art 52
[69] ibid, art 64
[70] GDPR (n 5) art 1 (1)

non-personal electronic health data[71] which are, according to Article 4(15) GDPR directly linked to the physical or mental health of an individual.[72]

The GDPR views this information as highly sensitive and it merits higher protection due to its potential to significantly impact individuals adversely.[73] This includes information about medical treatments received, health conditions, or any data revealing insights into a person's health status.[74] The European Court of Justice (ECJ) has emphasized the need for a broad interpretation of "data concerning health" in accordance with the GDPR and its Recital 53.[75] This broad scope encompasses various sources from which health data can originate.

Firstly, there are records maintained by healthcare providers, encompassing medical histories, test results, and treatment outcomes. Additionally, health data can arise from cross-referencing information; for example, combining various data sets to reveal an individual's health status or potential health risks, such as inferring a higher risk of heart-related issues from consistently high blood pressure readings.[76] Furthermore, individuals may voluntarily provide health-related information through self-reported surveys or questionnaires, detailing symptoms or health-related experiences.[77] Also, contextual information, like recent travel to regions affected by diseases such

[71] ibid, art 2 (2)
[72] GDPR (n 5) art 4 (15)
[73] ibid
[74] ibid
[75] Case C-101/01 *Lindqvist* [2003] ECR I – 12992, para 50
[76] EDPB, 'Guidelines 03/2020 on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak' (2020) <https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202003_healthdatascientificresearchcovid19_en.pdf> accessed 10 December 2023, p 5
[77] ibid

as COVID-19, when assessed by a medical professional, contributes to diagnosing or understanding health implications.[78]

The primacy of individual rights and freedoms over the common interest in making data available for research is notorious. As a result, the GDPR prohibits the processing of special categories of data, including health data and genetic data among others as per Article 9(1) GDPR.[79] However, the Regulation lays down exception to such processing in paragraph 2 of Article 9 GDPR by setting up series of circumstances that, if present, allow the data controller to circumvent the prohibition.[80] These include, for example, consent[81] to process sensitive data; the need to use the data to protect the vital interests of the data subjects[82], for reasons of essential public interest[83]. In relation to this paper, the most relevant exception to the processing of health data is the situation when processing is required '*for reasons of public interest in the field of public health, such as protection against serious cross-border threats to health, or to ensure high stands of quality and safety of healthcare and of medicinal products or medical devices'*[84] or '*for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, in accordance with Article 89(1) GDPR.*[85] Some of the situations outlined as exceptions to processing of sensitive data, namely Article 9(2)(g),(i), or (j) GDPR may take place only if they have a legal foundation in EU or

[78] ibid
[79] GDPR (n 5) art 9 (1)
[80] GDPR (n 5) art 9 (2)
[81] GDPR (n 5) art 9 (2) (a)
[82] GDPR (n 5) art 9 (2) (c)
[83] GDPR (n 5) art 9 (2) (g)
[84] GDPR (n 5) art 9 (2) (i)
[85] GDPR (n 5) art 9 (2) (j)

Member State law[86]. As will be reiterated in later subchapter, this has led to notorious drawbacks in the use of health data in research.

In addition, even if such obstacle could be successfully overcome, the processing of the data would still be unlawful if any of the grounds of legitimacy set out in Article 6 GDPR were not met. This concerns legal grounds such as consent, necessity for the performance of a contract, protection of the vital interests of the data subject or of another natural person, compliance with a legal obligation applicable to the controller, performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, or the satisfaction of legitimate interests pursued by the controller or by a third party.[87]

While the GDPR doesn't explicitly define "processing for the purpose of scientific research," Recital 159 sheds light on its broader interpretation.[88] This includes various research domains such as technological development, fundamental and applied research, and privately funded studies, aligning with the EU's objective of establishing a European Research Area under Article 179 (1) TFEU.[89] However, it is crucial to note that the former Article 29 Working Party cautioned against stretching the term "scientific research" beyond its intended meaning. In this context, "scientific research" refers to projects complying with sector-specific ethical and methodological standards,

[86] GDPR (n 5) art 9 (2)
[87] GDPR (n 5) art 6
[88] GDPR (n 5) recital 159
[89] ibid

conforming to good practice.[90] Such studies conducted in the public interest play a vital role within the broader context of health data utilization and protection.

To sum up, the EHDS Proposal aims to harmonize data access, exchange, and utilization in the healthcare sector while ensuring robust safeguards for sensitive health-related information. By understanding the breadth of "data concerning health" and the nuances of processing it for scientific purposes, the proposal seeks to strike a balance between innovation, research advancement, and individual data protection within the healthcare landscape. However, it appears to pose as a problem that there is no clear definition of the term scientific research and the secondary data processing. The EU Commission tries to resolve this problem in its Proposal, but many are uncertain of its legitimacy. The following will elaborate on the issue further.

3.2.1. Concerns related to health data processing

Scholars, health and digital rights organizations, along with workers and trade unions, have urged members of the EU Parliament to prioritize patients' rights and control over their private health information within the EHDS.[91] While they appreciate the EHDS's goal of establishing interoperable and advanced digital health systems across the EU, historical precedents in regulating data-intensive domains reveal a common trend: the pursuit of efficiency often involves compromising privacy and negotiating power dynamics.[92] From workplace surveillance to national border controls and from identity verification to loyalty programs, systems analysing

[90] Article 29 Working Party, 'Guidelines on consent under Regulation 2016/679' (2018) <file:///Users/Ivka/Downloads/20180416_article_29_wp_guidelines_on_consent_publish_09A6854F-F638-8898-7A0543CE0857250F_51030%20(1).pdf> , p 27-30

[91] European Digital Rights and others, 'Joint Public Letter to EU lawmakers on patients' rights in the European Health Data Space' (2023) <https://edri.org/wp-content/uploads/2023/04/Joint-public-letter-on-consent-in-EHDS-2.pdf> accessed 10 December 2023

[92] Compromises and Asymmetries in the European Health Data Space (n 47) 352

human behaviour have been deployed, raising concerns about privacy compromises and power imbalances.[93]

In general, the storage and transfer of sensitive data across various databases heighten the risks of data breaches.[94] Additionally, as data moves farther from its original source, individuals are less likely to be aware of who accessed their data and for what specific purposes.[95] Simultaneously, insights drawn from health data, when identifiable, could result in decisions or actions that adversely affect individuals, such as denial of insurance, alterations in credit or mortgage status, or targeted marketing of medical products.[96] However, certain health data, especially when linked to disease patterns, holds substantial value even in anonymized or aggregated forms. Yet, these methods only partially mitigate challenges, as the risk of re-identifying individuals remains significant, particularly when health data is handled by large tech companies with extensive data resources.[97]

3.3.Secondary use of sensitive data

The debates within the EU about shaping the EHDS have been quite challenging, particularly regarding the agreements about using health data again for different purposes.[98] One of the most compelling advantages of repurposing health data lies in its pivotal role in fostering scientific

---

[93] ibid
[94] Giorgia Bincoletto, 'Scientific Research Processing Health Data in the European Union: Data Protection Regime vs. Open Data' (2023) 11 J Open Access L 1, 17
[95] Compromises and Asymmetries in the European Health Data Space (n 47) 352
[96] ibid
[97] ibid 353
[98] Giedre Peseckyte, 'EU Parliament solving riddle of secondary use of data in health data space' (*Euroactiv.com,* 10 July 2023) <https://www.euractiv.com/section/health-consumers/news/eu-parliament-solving-riddle-of-secondary-use-of-data-in-health-data-space/> accessed 10 December 2023

research.[99] Another important aspect is how using this health data again can help policymakers. By looking at this vast amount of information, policymakers can learn a lot about the health trends in society, how common certain diseases are, and how well different treatments work.[100] This knowledge helps them create better policies and strategies for healthcare that are based on real evidence, making healthcare more effective for everyone. The benefits of reusing health data also reach into making healthcare systems better. When health data is shared between, for example, hospitals and databases, it allows researchers to check if their findings are true across many institutions or just specific to one. This helps ensure that the conclusions made from research are reliable and can be applied to different groups of people and various healthcare settings.[101] Recital 38 of the Proposal acknowledges that "in order to fully unleash the benefits of the secondary use of electronic health data, all data holders should contribute to this effort in making different categories of electronic health data they are holding available for secondary use."[102] However, delving into the complexities of the secondary use of health data, it is crucial to examine the intricate regulatory framework that governs these practices and ensures their legal adherence.

To begin with, all data processing must respect the principle of purpose limitation, which implies that the data must not be used in a way that is incompatible with the specified, explicit, and legitimate purposes for which they were collected, in accordance with the principle of limitation of processing laid down by Article 5(1)(b) GDPR.[103] Given that this limitation of processing entails a significant impairment of our ability to use data for research, Article 5 GAPR qualifies, however,

---

[99] Compromises and Asymmetries in the European Health Data Space (n 47) 352
[100] Tugce Schmitt and others, 'What does it take to create a European Health Data Space? International commitments and national realities' (2023) Vol 179 Zeitschrift für Evidenz, Fortbildung und Qualität im Gesundheitswesen 1, 6
[101] S. McLennan, and others, 'Practices and Attitudes of Bavarian Stakeholders Regarding the Secondary Use of Health Data for Research Purposes During the COVID-19 Pandemic' [2022] 24 J Med Internet Res 6, 4
[102] EHDS (n 7) recital 38
[103] GDPR (n 5) art 5 (1) (b)

that further processing of personal data for archiving purposes in the public interest, scientific and historical research purposes or statistical purposes is not considered "*incompatible with the initial purposes"*, provided that such processing is carried out in accordance with the provisions of Article 89(1) GDPR.[104] The same Article requires that any processing of data for scientific research purposes be subject to appropriate safeguards for the rights and freedoms of the data subjects.[105] Such safeguards shall ensure that technical and organizational measures are in place, in particular to ensure respect for the principles of minimization of personal data, and may include pseudonymization.[106] Whenever such purposes can be achieved by further processing identification of data subjects should be no longer possible.[107] As a result, the GDPR opens the door to the use of data collected, for example, in medical records for further purposes other than those initially justified for their collections. It basically considers the subsequent purpose such as scientific research to be compatible with the original purpose being the clinical use. However, this interpretation needs to be very nuanced in the bio-health field, since Article 9(4) GDPR provides that "*Member States may maintain or introduce additional conditions, including limitations, with respect to the processing of genetic data, biometric data or data concerning health".*[108] In practice, this has ended up leaving the regulation of these matters to the free will of the Member States, which, as will be discussed below, has not been very encouraging in terms of creating large compatible databases.

Finally, we must not forget that the GDPR places at the forefront the rights enjoyed by every citizen. Among them all, the right to information undoubtedly stands out, enshrined in Article 13

[104] ibid
[105] GDPR (n 5) art 89 (1)
[106] ibid
[107] ibid
[108] GDPR (n 5) art 9 (4)

to 14 GDPR, depending on whether or not the data is obtained from the data subject themselves.[109] Those are probably the primordial rights and logically precede all the others, since if one is not informed of the processing of one's data, they can hardly exercise the right to oppose or suspend the processing, or to rectify, erase, access or transfer the data.[110] Consequently, this is the only right that does not know the theoretical limits[111] beyond those imposed by the obligation of professional secrecy, according to Article 14(5)(d) GDPR[112] and modulations according to pragmatic considerations such as that "*the communication of such information proves impossible or would involve a disproportionate effort",* according to Article 14(5)(b) GDPR.[113]

3.4. Fragmented rules on Member State level

Presently, as indicated by the TEHDAS project striving to establish unified European guidelines for secondary use of health data, there exists significant diversity among Member States in the organization, management, and readiness to facilitate the secondary use of health data within the forthcoming EHDS.[114] The TEHDAS report from April 2023 revealed results and an overview of the health data management of 12 Member States based on the visits carried out under this joint action between 2021-2022.[115] These visits encompassed interviews with key stakeholders in

[109] GDPR (n 5) art 13; GDPR (n 5) art 14
[110] Inigo de Miguel Beriain, 'The Use of Health Data for Biomedical Research in the Light of the Proposal for a Regulation of the European Parliament and of the Council on the European Health Data Space' (2023) 60 Rev Juridica Castilla & Leon 7, 10
[111] ibid
[112] GDPR (n 5) art 14 (5) (d)
[113] GDPR (n 5) art 14 (5) (b)
[114] Towards the European Health Data Space, 'Member states' readiness to benefit from the EHDS regulation varies (2023) <https://tehdas.eu/results/member-states-readiness-to-benefit-from-the-ehds-regulation-varies/> accessed 10 December 2023
[115] Towards the European Health Data Space, 'Country factsheets: Mapping health data management systems through country visits' (2023) <https://tehdas.eu/app/uploads/2023/04/tehdas-mapping-health-data-management-systems-through-country-visits.pdf> accessed 10 December 2023, p 8

national health data and utilized a specifically designed mapping tool to assess and chart the health data management systems within each country, evaluating their readiness for the EHDS.[116]

First of all, the analysis indicates that EU Member States demonstrate a collective determination to participate in the EHDS. Nevertheless, a shared apprehension among these nations revolves around their capability to effectively integrate into the EHDS framework. It is widely acknowledged that there exists a substantial requirement for increased personnel possessing specialized technical and legal knowledge, as well as an extended timeframe to facilitate the envisioned operations within the EHDS.[117] The report highlights that across most nations, data management practices involve coordination among multiple entities, with only a minority employing a centralized organizational approach.[118] Despite the EHDS aim to standardize the secondary use of health data through a unified legal structure, on-site assessments make it evident that all Member States are yet to implement necessary measures to align fully with EHDS prerequisites. Each Member State will require an individualized plan to accomplish these measures. Several countries have voiced a requirement for increased human and financial resources.[119]

To give an example, the governance of health data in Germany showcases a notably decentralized and intricate system. The country's approach to data management is predominantly decentralized, reflecting a highly distributed nature of data storage. Accessing data typically involves individual requests to specific institutes.[120] As noted by Florian Benthin, EY's digital health leader for EU

[116] ibid, p 4
[117] ibid, p 12
[118] ibid, p 11
[119] ibid, p 13
[120] ibid, p 36-37

Institutions, a significant example of this complexity is observed within one university hospital in Germany, which operates multiple EHR-S.[121] On the other hand, Estonia's approach to health data governance is centred around a comprehensive digitalization effort initiated in 2009. The country's health information system has undergone significant digital transformation. Utilizing the Estonian X-road, data sharing occurs securely across all administrative levels. At the core of this structure is the national electronic health information system, a fully digitized e-health platform that consolidates patient data from diverse healthcare providers. This centralized repository of patient information is accessible to both healthcare providers and patients through the national eHealth Portal, ensuring transparency through logged transactions visible to patients. While the national health information system boasts a centralized storage for a segment of electronic health record data from various healthcare providers, all this data is consolidated into one central data warehouse, combining information from distinct operational systems. Despite Estonia's limitation in resources owing to its small size, one of its key strengths lies in the X-road software-based solution, facilitating seamless information sharing across different governmental sectors and administrations within the eGovernment services.[122]

Moreover, many Member States highlighted legal impediments as the primary hurdles hindering the secondary utilization of health data. Presently, there exists a disparity in the interpretation of the GDPR among countries and even within organizations within the same country.[123] The majority of these Member States lack dedicated national laws governing the secondary use of

---

[121]Giedre Peseckyte, 'EU Parliament solving riddle of secondary use of data in health data space' (*Euroactiv.com*, 10 July 2023) <https://www.euractiv.com/section/health-consumers/news/eu-parliament-solving-riddle-of-secondary-use-of-data-in-health-data-space> accessed 10 December 2023

[122] Towards the European Health Data Space, 'Country factsheets: Mapping health data management systems through country visits' (2023) <https://tehdas.eu/app/uploads/2023/04/tehdas-mapping-health-data-management-systems-through-country-visits.pdf> accessed 10 December 2023, p 28-29

[123] ibid, p 12

health data. Despite possessing substantial data repositories, most of the visited countries outlined the difficulties researchers and policymakers encounter when accessing data from various repositories. These challenges stem from varying, protracted, and occasionally opaque procedures for data access.[124]

For example, the governance of health data in the Czech Republic currently lacks specific guidelines or laws tailored for the digital health sector.[125] Consequently, the utilization and processing of health data via various digital health solutions fall outside the exemptions outlined in Article 9, Paragraph 2 of the GDPR, which pertain to national regulations. This absence of specific legislation implies that obtaining consent from the data subject, typically the patient, becomes imperative and this necessity extends to the secondary usage of health data.[126] Furthermore, there exists no regulatory framework enabling healthcare providers or research organizations to utilize pseudonymized data for research purposes without explicit consent.[127] Even in cases of anonymized data, caution is advised when releasing such datasets due to potential re-identification risks.[128] In certain medical scenarios, individuals can be re-identified based solely on their diagnosis, especially when disseminated among professionals, such as in specialized articles or conferences, where additional information may inadvertently lead to the identification of the data subject. In comparison, Finland is the first country to have adopted an act specifically targeting the secondary use of health data back in 2019.[129] Part of this pioneering move was an

---

[124] ibid
[125] Dubanska & Co, 'At a glance: data protection and management of health data in Czech Republic' (*Lexology.com,* 25 January 2023) <https://www.lexology.com/library/detail.aspx?g=63a1a593-a72d-4c94-8b5c-958301c02965&utm_source=Lexology+Daily+Newsfeed&utm_medium=HTML+email+-+Body+-+General+section&utm_campaign=Lexology+subscriber+daily+feed&utm_content=Lexology+Daily+Newsfeed+2023-06-16&utm_term=> accessed 10 December 2023
[126] ibid
[127] ibid
[128] ibid
[129] Act on Secondary Use of Health and Social Data 2019

establishment of the Findata authority, designed to streamline access to health data for research and policy formulation purposes.[130] This legislative effort serves as the bedrock for the EHDS.[131] The development of this act prioritized transparency and confidence in both governmental bodies and public authorities. Notably, a significant shift brought about by the Act on Secondary Use of Health and Social Data in Finland pertains to the permissions process. Previously, individual healthcare and social service providers held decision-making power over data use within their possession, often requiring multiple authorizations for research reliant on data from various sources. This system also allowed for potential discrepancies where one organization might grant data access while another refused. While streamlining data utilization, the Act also imposes substantial constraints on how and where data can be processed to ensure robust personal data protection. Effective from May 1, 2021, data access is restricted to secure information processing environments endorsed by accredited inspection bodies in Finland, with Findata's environment being the primary default option.[132] Notably, the Finnish Innovation Fund Sitra has been entrusted with leading the collective effort among EU member states to realize the EHDS.[133]

Furthermore, there exist significant variations among countries regarding the extent to which health data has been digitized. Even among countries with similar levels of digitization, the methods of data collection and storage formats differ widely and are often incompatible. As an illustration, the MyHealth@EU platform has only been adopted by ten Member States and

---

[130] Global Alliance for Genomics & Health, 'GDPR Brief: the Finnish Secondary Use Act 2019 (May 2020 bonus brief)' (2020) <https://www.ga4gh.org/news_item/ga4gh-gdpr-brief-the-finnish-secondary-use-act-2019-may-2020-bonus-brief/> accessed 10 December 2023

[131] Towards the European Health Data Space, 'Country factsheets: Mapping health data management systems through country visits' (2023) <https://tehdas.eu/app/uploads/2023/04/tehdas-mapping-health-data-management-systems-through-country-visits.pdf> accessed 10 December 2023, p 33

[132] ibid

[133] Towards the European Health Data Space, 'Sitra has been appointed to lead a project of 29 countries to realise the European health data space' (2023) <https://tehdas.eu/news/sitra-has-been-appointed-to-lead-a-project-of-29-countries-to-realise-the-european-health-data-space/> accessed 10 December 2023

presently caters to just two services: electronic prescriptions and patient summary records.[134] This limited implementation contrasts with the eHealth network's recommendation for Member States to adopt standardized electronic health record exchange formats in their procurement processes to enhance interoperability. Given these circumstances, creating a unified data space becomes unfeasible, particularly considering the absence of established data quality standards. It is important to note that we are still far from implementing standards that ensure the reliability and usefulness of the foundational data that will constitute the EHDS.[135]

Additionally, the interpretation and implementation of Article 89 GDPR, especially concerning the concept of using data for purposes other than the original one, have varied significantly across different countries. As mentioned earlier, the Regulation mandates the incorporation of several safeguards to protect individuals' data against processing that might infringe upon their rights or freedoms. It also stipulates that Member States or Union law can make exceptions to this right. However, substantial discrepancies have been observed in how this clause has been developed and applied within different Member States, leading to several issues in practice.[136]

The Health and DG Food Safety assessment of the EU Member States' rules on health data described it by stating that '*it is clear from the responses provided by the correspondents that the Member States have not implemented such legislation in a homogenous way, resulting in a complex and fragmented landscape for researchers to navigate. Consequently, differences between Member States in the way the GDPR is implemented and interpreted in the area of*

[134] EHDS (n 7) explanatory memorandum, p 10
[135] Inigo de Miguel Beriain, 'The Use of Health Data for Biomedical Research in the Light of the Proposal for a Regulation of the European Parliament and of the Council on the European Health Data Space' (2023) 60 Rev Juridica Castilla & Leon 7, 16
[136] ibid

scientific research has made data exchange between Member State and EU bodies for research purposes difficult and in some cases highly technical.'[137]

3.5. Discrepant Legal Foundations for Secondary Use of Health Data in the EU

As one of the main goals of the EHDS is to create a common space to facilitate health data access and reuse, this can only be achieved by creating clear rules enhancing collaboration in the research. According to investigations into the implementation of the GDPR, researchers have discovered that requirements related to consent or Article 9 research exemptions have been ineffective.[138] As previously explained, the GDPR is founded on the principle of purpose limitation, a key aspect of data protection that mandates controllers to confine data collection and its reuse to specific objectives[139]. In contrast, establishing a health data space with an aim to enhance research involves enabling the reuse and exchange of data acquired from various origins for varied purposes, while upholding individual rights. However, current data protection methods have proved suboptimal, excessively prioritizing individual consent as the primary legal foundation for data reuse[140].

The GDPR demands specific consent as a prerequisite for data processing to be considered legitimate, a condition challenging to fulfil when contemplating data sharing for diverse and yet undetermined aims. Regardless, in some Member States there continues to be an excessive use of consent as the most common basis of legitimacy.[141] However, it is common that at the outset of

---

[137] European Commission (DG Health and Food Safety), 'Assessment of the EU Member States' rules on health data in the light of GDPR' (2021) p 58
[138] Bentzen, H. and others, ‚Remove obstacles to sharing health data with researchers outside of the European Union' (2021) 27 Nat Med 1329
[139] GDPR (n 5) art 5 (1) (b)
[140] J. Bovenberg and others, 'How to fix the GDPR's frustration of global biomedical research' (2020) Science 40, 41
[141] Inigo de Miguel Beriain, 'The Use of Health Data for Biomedical Research in the Light of the Proposal for a Regulation of the European Parliament and of the Council on the European Health Data Space' (2023) 60 Rev Juridica Castilla & Leon 7, 11

conducting a scientific research, meaning at the time of data collection, full identification of a purpose for health data processing is not always possible.[142]

On top of that, Recital 33 GDPR emphasizes that '*data subjects should have the opportunity to give their consent only to certain areas of research or parts of research projects to the extent allowed by the intended purpose'*[143] As a result, Article-29 Working-party confirms that scientific research projects can utilize personal data only when consent is granted for a clearly defined and articulated purpose.[144] Even though the guidelines and the Recital 33 allow an exception that the purpose may be defined on a more general level (also referred to as '*broad consent'*),[145] EDPB has consistently underscored that broad consent, signifying agreement for unspecified future research purposes, fails to meet GDPR's consent requirements, even concerning data sharing related to COVID-19 research.[146] Additionally, The EDPB has also insisted that collection of consent is not the most appropriate for scientific research and in the context of clinical trial given the power differential relationship between the patient and the data controller. It is therefore recommended that its use be avoided.[147]

The GDPR draws a distinction between data processing for public or general interest and data processing for other purposes. At first glance, regulatory bodies of Member States appear to view scientific research as falling within the realm of public interest, potentially permitting a more

[142] Article 29 (n 90) p 28
[143] GDPR (n 5) recital 33
[144] Article 29 (n 90) p 28
[145] ibid
[146] Guidelines 03/2020 (n 76) p 6
[147] European Data Protection Board, 'Opinion 3/2019 of the EDPB from 23.1.2019 on concerning the Questions and Answers on the interplay between the Clinical Trials Regulation and the GDPR' (2019) < https://edpb.europa.eu/our-work-tools/our-documents/opinion-art-70/opinion-32019-concerning-questions-and-answers_en)> accessed 10 December 2023

lenient approach toward data sharing requirements or exemptions from certain rights of data subjects. This may include the right to restriction of processing, object to processing, and rectify inaccuracies in personal information held by companies.[148]

Despite the initial assumption, the utilization of the so-called research exemption provisions has led to uncertainties for data controllers in practical application. Firstly, there's a notable absence of explicit guidance on how scientific research, conducted in the interests of the public or general interest, must be precisely defined under the GDPR, especially in cases where commercial entities are involved[149]. Although the GDPR preamble mentions "privately funded research" as an instance of scientific research, significant questions persist regarding the implications for for-profit versus non-profit privately funded research. There's also ambiguity surrounding how to prioritize public interest over private and commercial interests.[150] Beyond funding considerations, various aspects of research, such as the significance of research questions to the population under study, models for equitable benefit sharing, and fair access to research databases, remain unaddressed when determining research within the public interest as per the regulation.[151] Secondly, the implementation of rules pertaining to the "research exemption" has primarily been delegated to Member States under the GDPR. This approach has resulted in the adoption of divergent methodologies across the EU, creating a fragmented landscape.[152] According to recent findings from a survey, 18 countries have thus far developed specific national regulations concerning scientific research and public interest, with only nine countries incorporating distinct provisions

[148] M. Shabani, 'Will the European Health Data Space change data sharing rule' (2022) Science 1357, 1358
[149] Kieran C. O'Doherty and others, 'Toward better governance of human genomic data' (2021) Nat Genet 1, 3
[150] Inigo de Miguel Beriain, 'The Use of Health Data for Biomedical Research in the Light of the Proposal for a Regulation of the European Parliament and of the Council on the European Health Data Space' (2023) 60 Rev Juridica Castilla & Leon 7, 20
[151] ibid
[152] ibid

regarding research carried out by private sector organizations. This discrepancy highlights the variation in interpretation and application of public interest as a legal foundation for processing data for research purposes across different European jurisdictions.[153]

In conclusion, various legal structures, particularly concerning the access to sensitive health data, act as barriers to data sharing among organizations.[154] Governments worldwide, including those in the EU, have initiated data infrastructures and occasionally established legal frameworks to enable secondary use of health data. However, researchers argue that overreliance on consent as a legal basis for scientific research, and therefore, secondary use of health data might devalue certain scientific research endeavours.[155] Because of all the above-mentioned reasons, the EU Commission's Proposal for EHDS as a data governance framework will resolve this fragmentation of rules to provide a more cost-effective alternative to consent for the collection and processing of electronic health data. Simultaneously, this proposal aims to facilitate cross-border interoperability among health data systems and reuse of health data for different purposes.

4. THE RELATIONSHIP BETWEEN THE EHDS AND GDPR

4.2. Legal Basis of the EHDS

Above, this paper has analysed the lawful basis for processing of sensitive data and its secondary use in the context of scientific research. The following section will show how the legislators of the

[153] European Commission (DG Health and Food Safety), 'Assessment of the EU Member States' rules on health data in the light of GDPR' (2021) <https://health.ec.europa.eu/system/files/2021-02/ms_rules_health-data_en_0.pdf,> p 60

[154] European Data Protection Supervisor, "Preliminary Opinion 8/2020 on the European Health Data Space," November 17, (2020) <https://edps.europa.eu/data-protection/our-work/publications/opinions/preliminary-opinion-82020-european- health-data-space_en.> accessed 10 December 2023, p 8

[155] Victoria Chico, 'The impact of the General Data Protection Regulation on health research' (2018) 128 British Medical Bulletin 109, 115

Proposal which as a novel governance structure aims at effectively managing health data, signified compliance outlined in the GDPR. Acknowledging this, the EDPB recognized instances within the Proposal where Union law establishes lawful grounds and exceptions for processing health data, all within the established structure of the GDPR as explained in the previous sections.[156]

4.2.1. Transfer of data to health data access bodies

In delineating the legal framework governing the secondary purpose data processing – a focal point of this paper - the Proposal expressly recognizes specific clauses within the GDPR as the foundational basis. One of the various facets pertinent to such processing is the exchange of the data between the data holder and the health data access entity which will be analysed in the subchapter below. This disclosure of data by the data holder hinges upon the legal foundation outlined in Article 6(1)(c) GDPR while it has to meet requirements for exception for processing of data, particularly health-sensitive information according to Article 9 (2)(h), (i), and (j) GDPR.[157]

4.2.2. Access to health data

Concurrently, the Proposal acknowledges that the legal foundation for soliciting access to health data will find footing in GDPR Article 6 (1)(e) and (f) GDPR. This implies that a prospective data applicant must pivot their justification for access on either a task performed in the public interest or their legitimate interests. Should the data applicant opt for the former, it necessitates referencing another pertinent EU regulation or national statute mandating the processing of health data for their tasks' compliance. This emphasizes the imperative link between the data request and the

[156] Joint Opinion EDPB-EDPS (n 4) p 3
[157] EHDS (n 7) recital 37

predefined legal obligations.

Alternatively, in relying on the applicant's legitimate interests, the proposal itself assumes the role of substantiating such a claim. Consequently, the decision-making process of the health data access entity has a more administrative role, tasked primarily with determining the conditions under which the requested health data can be accessed. As articulated in the subchapter related to the health data access body’s function, its decision-making process underscores the regulatory parameters defining access to the requested data rather than weighing the legitimacy of the applicant's interests.

4.2.3. Exceptions to processing of sensitive data

The Proposal deviates from established norms regarding the use of sensitive data, including health-related information which is generally prohibited. It makes use of the Article 9 (1) (h) to (j) GDPR which carve out specific exceptions to this prohibition. These exceptions encompass substantial public interest, preventive and occupational medicine, management of health or social care systems and services, cross-border public health threats, scientific and historical research, and other statistical purposes.

The 'research exemption' provided by Article 9 (2) (h) to (j) GDPR and Article 89 GDPR presents a broad and permissive framework for the collection and processing of sensitive data, notably health data. Scholars have advocated for clarifications within this provision, emphasizing the necessity of establishing a clearer connection between scientific research and the broader public interest, a relationship that the GDPR doesn't explicitly articulate.

As can be observed, the EHDS highly depends on being compatible with the GDPR. Since the Regulation already provides means for processing of sensitive data, any new proposed regulation such as EHDS must clearly reference the existing provisions of rights and established procedures under the GDPR framework. According to the Joint Opinion of the EDPB and EDPS, the Proposal merely provides for some 'add-ons' to those existing GDPR rights of data subjects and their main concern lies in the fact that some of the proposed categories personal data and purposes for which they can be processed might in turn weaken those rights to privacy.[158] Much is still called for by way of improvement of proposed provisions in terms of clarity. These concerns will be analyzed in further sections.

4.3. Definition of secondary use of health data

The very first inconsistency of the Proposal with the GDPR pointed out by the EDPB and EDPS in its Joint Opinion was the definition of the secondary use of electronic health data which as a concept does not appear in the Regulation and even deviates from the actual established GDPR concept of 'further processing of personal data'[159]. Consequently, the EDPB and the EDPS advocate for the rectification of these definitions in alignment with the GDPR.[160] Specifically, they propose clarifying the connection between the definition of secondary use of electronic health data as defined in the Proposal and the notion of 'further processing of personal data' as outlined in the GDPR.[161] According to them, this clarification should particularly consider the unique provisions already granted by the GDPR for scientific research purposes. However, it is understandable that the 'secondary use of electronic health data' as described by the EHDS does not completely align

[158] Joint Opinion EDPB-EDPS (n 4) p 3
[159] Joint Opinion EDPB-EDPS (n 4) para 42
[160] ibid
[161] ibid, para 87

with the 'further processing' according to the GDPR. The GDPR already offers a broad and accessible framework collection of sensitive data and its further processing, however, the Regulation does not specifically articulate a link between a scientific research and public interest. This is one of the reasons why the legislators of the Proposal attempt to create a unified framework to promote use of electronic health data in public as well private sector, and thus to innovate the EU data-driven healthcare. Nevertheless, the EDPB argues that the definition of the 'secondary use' in the Proposal must be corrected and must better clarify its link with the GDPR definition for 'further processing'.

This aligns with another observation made by the EDPB that the purposes for which the electronic health data can be processed for secondary use under Article 34(1) of the Proposal contain such categories which indeed fall under the various categories of grounds for exception of processing in Article 9(2) GDPR (e.g. processing complies with activities intended for protection against serious cross-border threats, to scientific research, education, etc.)[162] However, the concern is raised in regard to the assessment of the data application (as per Article 45 of the Proposal) by the health data access bodies. According to the Article 46 of the Proposal the health data access bodies decide whether the data application fulfils the requirements set forth in the Article 45 of the Proposal and is submitted for the purposes listed in Article 34 of the Proposal instead of Article 9(2) GDPR specifically targeting the rules for processing of sensitive data. Surely, it would probably pass by the EDPB if the purposes offered for secondary processing of sensitive data in Article 34 complied with those of Article 9(2) GDPR. Unfortunately, that is not the case. More specifically, the purposes identified as incompatible with the GDPR by the EDPB are processing

[162] EHDS (n 7) art 34 (1)

for '*development and innovation activities for products or services contributing to public health or social security or ensuring high levels of quality and safety of health care, of medical products or of medical devices*' and '*training testing and evaluating of algorithms, including in medical devices, AI system and digital health applications (...)'* listed in Article 34(1)(f) and (g). In the context of this thesis, point (h) of Article 34(1) of the Proposal should also raise questions as another option for intended purpose of processing also includes '*providing personalised healthcare consisting in assessing, maintaining or restoring the state of health of natural persons, based on the health data of other natural persons*.'

Article 34(1) reveals a broad scope, notably encompassing points (f) and (g), which could seemingly incorporate various aspects falling under the expansive domain of 'artificial intelligence.' Additionally, point (h) appears to allude directly to the data-intensive realm of healthcare Internet of Things (IoT), comprising wearables, sensors, and actuators.[163] It's crucial to contextualize Articles 34(1)(f) and (h) alongside Article 37(1)(i), which mandates health data access bodies to endorse *'AI systems, their training, testing, validation, and the establishment of standardized norms for their utilization in health.*' This pairing intensifies the concerns arising from the EHDS Proposal, particularly regarding the overly stretched categorization of electronic health data in Article 33 of the Proposal, compounded by an open-ended framework for data access. As a result, merging these controversial Articles exacerbate the potential issues surrounding the access to a diverse array of health data under the proposed regime. It lays the groundwork for scenarios wherein technology companies could conceivably seek and potentially acquire data permits encompassing information from insurance firms, educational institutions,

[163] Compromises and Asymmetries in the European Health Data Space (n 47) p 355

meditation applications, and more.[164] Such endeavors might aim to develop personalized recommendation systems promoting 'healthy lifestyles.' The Joint Opinion' aptly emphasizes the necessity for aligning Article 34(1)(f) and (g) EHDS with GDPR Article 9(2) while advocating for the exclusion of certain data categories specified in Article 33(1) EHDS, particularly points (f) and (n).[165] These points pertain to person-generated electronic health data and information concerning insurance status, professional status, wellness, and behavioural data, respectively.[166]

A holistic interpretation of Article 34, coupled with Articles 37 and 33, illuminates a latent opportunity for entities like Big Tech or others with substantial technological, logistical, and financial capabilities to exploit an administrative pathway for accessing and processing broadly defined health data.[167] This pathway bypasses several requirements outlined in the GDPR Article 9(2). By including a *description of the safeguards planned to prevent any other use of the electronic health data*[168] and *a description of the safeguards planned to protect the rights and interests of the data holder and of the natural persons concerned*[169], such entities, equipped with technical proficiency and infrastructural support for tasks like 'training, testing, and evaluating algorithms,' gain access to extensive health data repositories.[170]

Allowing secondary use of health data for activities involving algorithmic development in AI systems and digital health applications introduces significant concerns related to procedural justice

---

[164] ibid
[165] Joint Opinion EDPB-EDPS (n 4) para 36
[166] Compromises and Asymmetries in the European Health Data Space (n 47) p 351
[167] Tamar Sharon, 'When digital health meets digital capitalism, how many common goods are at stake?' (2018) 5 Big Data & Society 1, 3
[168] EHDS (n 7) art 45 (2) (e)
[169] EHDS (n 7) art 45 (2) (f)
[170] Tamar Sharon, 'From hostile worlds to multiple spheres: towards a normative pragmatics of justice for the Googlization of health' 24 Medicine, Health Care and Philosophy 315, 325

and it effectively reshapes the landscape of legal and policy discourse.[171] Notably, it offers tech giants novel avenues for accessing health data and leveraging their expertise within the health domain, previously beyond their native purview.[172] Thanks to this framework, they are granted access to data without the necessity of acquiring explicit consent from data subjects or providing exhaustive justifications under a 'research exemption.'[173] Instead, they can lawfully access data by presenting cases for algorithmic projects while outlining measures to safeguard individuals' data. Furthermore, the administrative nature of the data access procedure, coupled with a broad definition of health data, potentially accommodates applications lacking scientific validity or endorsing pseudoscientific research pursuits, such as 'Emotional AI' applications.[174] These projects may evade scrutiny as long as they fit within the parameters set forth in the Proposal. This dynamic could significantly impact the evaluation of scientific merit and ethical considerations for data usage within the EHDS framework.

4.4. Who can access the health data?

4.4.1. Data holders

In the context of the EHDS and its proposed provisions delineating the definition of data holders, certain discrepancies emerge that challenge the framework established by the GDPR. The EHDS, as per Article 33(1) of the Proposal, introduces a legal obligation mandating data holder, under Union Law, to provide specific categories of electronic health data for secondary use. This particular provision is underscored by Article 41(1), which reinforces this new obligation, supplementing any existing legal requirements in Union law or national legislation implementing

[171] Compromises and Asymmetries in the European Health Data Space (n 47) p 356
[172] ibid
[173] GDPR (n 5) art 9 (2)
[174] Compromises and Asymmetries in the European Health Data Space (n 47) p 357

Union law.[175] However, scrutiny from the EDPB and EDPS as highlighted in their Joint Opinion, accentuates the potential conflict between the EHDS provisions and GDPR stipulations. While Article 33(1) of the Proposal ostensibly aligns with the GDPR's framework by serving as legal grounds under Article 6(1)(c) GDPR and providing an exception to the prohibition outlined in Article 9(1) GDPR for data holders to process and provide personal electronic health data, it introduces a layer of legal uncertainty.[176]

A significant point of contention revolves around the definition of 'data holder' within the EHDS framework. According to Article 33(3) of the Proposal, entities mandated to share data encompass those within the health or care sectors, including public and private health providers, research entities in these sectors, and certain Union institutions and agencies. The EHDS defines a *'data holder' as 'any natural or legal person, which is an entity or a body in the health or care sector, or performing research in relation to these sectors.*'[177] This definition leads to ambiguity and inconsistencies regarding which entities are mandated to share health data. There is confusion about whether powerful digital entities controlling databases valuable for healthcare research, such as Google, DeepMind, Facebook, Microsoft, Amazon, or Apple, fall within the EHDS framework's definition of data holders.[178] Similarly, various health applications accumulating sensitive health data might not explicitly fit within the defined 'entities performing research' category.

This ambiguity becomes more apparent when comparing the obligation placed on data holders to share data with the broader eligibility for entities to access health data. While the EHDS confines data holders to those within the healthcare sector or involved in relevant research, it doesn't restrict

[175] EHDS (n 7) art 41 (1)
[176] Joint Opinion EDPB-EDPS (n 4) para 45
[177] EHDS (n 7) art 2 (2) (y)
[178] Carmela Troncoso, 'Deploying Decentrelized, Privacy-Proximity Tracing', 65 Communication of the ACM 48, 50

access to health data solely to such entities. Instead, it permits *'any natural or legal person'* meeting the Proposal's specified purposes to request access to health data.[179] The discrepancy between the selective obligations of data holders and the inclusive access provision raises questions about the EHDS's underlying policy rationale. Is there an expectation for entities outside the healthcare sphere to contribute to health research and innovation? If so, why are not such entities classified as 'data holders' alongside their role as potential 'data users'?

4.4.2. Uncertainties surrounding data access

Beyond the paramount concern regarding who will wield access to sensitive health data, which fundamentally shapes the apprehension of data subjects and EU citizens, there exists a profound uncertainty regarding the assurance that pertinent institutions engaged in health-related research will indeed secure access to the data. The EHDS Proposal's deficiencies in establishing a clear legal foundation under the GDPR for data users to access personal data, despite obtaining a data access permit, compound this uncertainty.

In essence, the EHDS Proposal shifts the responsibility to data users to discern an appropriate legal basis under EU or Member State law, obliging them to navigate and identify the specific legal framework encompassing both Article 6 and Article 9 GDPR.[180] Presently, as described above, across various EU Member States, disparities persist regarding the necessity of patient consent for data utilization in research as per Article 9 (2) (a) GPDR, or the permissibility of organizations to rely on the research exemption outlined in Article 9 (2) (j) and Article 89 (1). This regulatory

[179] EHDS (n 7) art 2 (2) (y)
[180] EHDS (n 7) art 49

disparity remains unaddressed within the EHDS Proposal, leaving it to the discretion of the data user to determine the applicable legal basis for the pertinent data processing activities.[181]

Crucially, the EHDS Proposal falls short in harmonizing and standardizing these divergent rules, thereby failing to provide a unified framework for data users seeking lawful access for secondary use. This failure to harmonize leaves a notable void, potentially limiting data users in accessing specific data types lawfully. The absence of harmonization not only casts doubt on the seamless access of pertinent institutions engaged in health research to the necessary data but also underscores the uncertainty surrounding the types of data that can be lawfully accessed for secondary utilization. As a result, such regulatory ambiguity poses substantial challenges to data users, potentially impeding their ability to access data for legitimate research purposes within a consistent and legally sound framework.

4.5. Access to data from digital health applications

Apart from the confusion regarding which entities are eligible to provide access to health data, the Proposal raises concerns by covering the manufacturers of 'wellness applications'. It is a reference to devices or software designed by the manufacturer to handle electronic health data for objectives unrelated to healthcare.[182] Those encompass entities creating apps aiming to offer individuals wellness or nutritional guidance, as well as wearable devices gathering data on physical exercise.[183] Recital 35 of the Proposal underscores the necessity for users of wellness applications, including mobile apps and similar platforms, to be informed about these applications' capabilities

[181] Lee WB, Choi SJ., 'Secondary Use Provisions in the European Health Data Space Proposal and Policy Recommendations for Korea' (2023) Healthc Inform Res 199, 204
[182] The Use of Health Data for Biomedical Research (n 110) 32
[183] EHDS (n 7) art 31

to connect and share data with EHR-S or national electronic health platforms, particularly when the data produced holds relevance for healthcare purposes.[184] However, the EHDS Proposal lacks explicit delineation concerning the lawful conditions governing the connectivity and data transmission between wellness applications and EHR-S or national electronic health solutions within the framework of data protection legislation.[185] Although Recital 35 highlights the importance of user awareness regarding the connectivity and data-sharing functionalities of wellness applications, the EHDS Proposal falls short in providing detailed regulatory guidance governing these connections.

Analysis of Article 33 within the Proposal, outlining the minimum categories of electronic data for secondary use, sheds light on the status of personal data generated by wellness applications. It becomes evident that once this data is incorporated into an EHR-S or is processed by entities falling under the EHDS definition of data holders as per Article 2 (2) (y) of the Proposal, it aligns with the established categories of data intended for secondary use. Consequently, personal data originating from wellness applications becomes subject to the obligation of data holders to make such data available for secondary use, adhering to the EHDS Proposal's stipulated provisions in Chapter IV.[186]

The EHDS Proposal implicitly acknowledges the inclusion of personal data generated by wellness applications within the spectrum of health data designated for secondary utilization. By encompassing these data categories within the realm of data holders' obligations, the Proposal lays the groundwork for potential integration of wellness application-generated data into the broader

[184] EHDS (n 7) recital 35
[185] Joint Opinion EDPB-EDPS (n 4) para 81
[186] ibid

spectrum of health data utilized for secondary purposes. Nevertheless, the absence of explicit regulatory frameworks delineating the lawful connectivity and data transmission modalities between wellness applications and EHR-S, or national electronic health solutions, presents a notable regulatory gap within the EHDS Proposal. Addressing this gap is crucial to establish clear guidelines governing transparent and compliant data sharing practices while upholding the principles of data protection legislation.

The mandatory availability of electronic health data derived from medical devices, wellness applications, and other digital health tools for secondary utilization necessitates careful consideration against the backdrop of rapid technological advancements in mobile and wearable technology. Notably, the increasing popularity of 'quantified self' apps and devices empowers individuals to document various facets of their personality, mental state, physical condition, behavioural patterns, and locations. Such diverse data processing demands significant attention, as it may not be readily recognized as health data processing by the concerned individuals.[187] Nevertheless, this emerging paradigm presents substantial privacy risks, particularly when this data is used for supplementary purposes, combined with other datasets, or shared with third parties.[188] The processing of such data carries inherent risks, including the potential for unequal or unjust treatment based on assumptions or actual health status derived through profiling.[189] These assessments, whether accurate or not, often delve into profoundly intimate aspects of an individual's private life.

[187] Joint Opinion EDPB-EDPS (n 4) para 80
[188] ibid
[189] ibid

Moreover, the risks associated with this data processing extend to the reliability and accuracy of information generated by medical devices, wellness applications, or other digital health tools. Both the EDPB and the EDPS acknowledge the EHDS's attempt, under Article 33(3) of the Proposal, to define the scope of data generated by these sources for secondary use. However, they underscore the lack of clarity regarding the specific data falling within this category and the absence of defined mechanisms for evaluating its validity and quality. Similarly, within the EHDS Proposal, Articles 3(6), 33(1)(a), 33(1)(f), and 33(1)(n) set the framework for individuals to insert data into their EHR-S or for data holders to directly provide data. Nonetheless, the EHDS Proposal lacks clarity concerning the validation and quality assessment of data sourced from individuals' EHR-S or directly supplied by data holders.[190]

Considering these complexities and inherent risks, the EDPB ultimately recommended the complete exclusion of wellness applications and other digital health tools from the EHDS Proposal's scope.[191] This recommendation stems from the intricate nature of the data generated by such applications and the associated challenges in adequately safeguarding individuals' privacy rights within the EHDS framework.[192]

The EHDS, in its current form, introduces complexities and inconsistencies regarding data holder definitions, access provisions and the sources of data warranting careful scrutiny within the GDPR's overarching framework. Indeed, harmonization is essential to ensure clarity, consistency, and the protection of individual data rights within the evolving landscape of health data sharing and utilization. However, the legislators must critically assess whether such broad definition of

[190] The Use of Health Data for Biomedical Research (n 110) 33
[191] Joint Opinion EDPB-EDPS (n 4) para 36
[192] ibid

'data holder' will create trust among the EU citizens. The access to health data should be granted only to those for which it is necessary in order to perform a health-related task. Lastly, the source of the data should always be reliable as it is necessary in order to comply with principle of accuracy as per Article 5(1)(d) GDPR. Addressing these concerns is vital to ensure comprehensive protection of individuals' privacy rights in the ever-evolving landscape of health data utilization.

4.6. Right to information?

The issuance of data permit by the health data access bodies which will allow access to sensitive health information and guarantee its processing through the secure environment, potentially by third parties raises concerns also in connection to the data subjects' rights across Member States. Notably, there's a departure from Article 14 GDPR as Article 38 (2) of the Proposal suggests that health data access bodies are not mandated to provide specific information to individuals regarding the use of their data for particular projects under a data permit.[193] Instead, these bodies are obligated to offer general information, provided on a monthly basis, encompassing all received data permits, requests, and applications.[194] This departure from the GDPR's established regulatory framework, described as an 'explicit derogation' from consent provisions by the 'Joint Opinion,' raises questions about its necessity and compliance with GDPR principles. While cost-efficiency might justify these deviations, it remains unclear why existing restrictions in Article 14 (5)(b) and (c) GDPR related to scientific research wouldn't suffice.[195] Furthermore, this Proposal shifts the responsibility of informed consent – traditionally a requirement for sensitive data collection and

[193] EHDS (n 7) art 38 (2)
[194] ibid
[195] Compromises and Asymmetries in the European Health Data Space (n 47) p 360

processing – onto the newly established health data access bodies, mandating them to disclose general information within 30 working days of a data permit's issuance.[196]

While flexibility in medical research data usage may be justified, the proposal fails to differentiate between entities seeking access. It equates the legitimate needs of medical research groups with potentially less accountable entities, such as technology companies pursuing AI development or experimental projects described previously.[197] This approach raises concerns, especially considering past controversial agreements between technology companies and public sector bodies involving patient data.[198]

The result of the restricted information approach in Article 38 (2) of the Proposal at the end limits interested parties, including data subjects, journalists, and NGOs, from timely information and scrutiny of imminent actions related to health data, both nationally and across borders. This raises pertinent questions about its alignment with GDPR principles of transparency and information provision regarding sensitive data processing. The Proposal's purported aim to empower individuals in managing their data lacks clarity in execution. While there is a shift toward transparency obligations, it remains debatable whether this adequately supports individuals in taking control of their data. The absence of provisions addressing different stakeholders' varied needs and potential misuse of health data by certain entities underscores the need for more meticulous considerations within the Proposal. In essence, the questions persist: Is Article 38 (2) congruent with GDPR principles of transparency and sensitive data processing? How effectively does the proposal facilitate individuals' control over their data, and what measures ensure this

[196] EHDS (n 7) art 37 (1) (q) (ii)
[197] Compromises and Asymmetries in the European Health Data Space (n 47) p 360
[198] Compromises and Asymmetries in the European Health Data Space (n 47) p 361

control is actualized? These critical inquiries underscore the complexity and potential implications of the proposed framework within the EHDS.

4.7. Fair and secure data sharing

In recent years, significant research attention has focused on upholding FAIR principles, aiming to ensure data's findability, accessibility, interoperability, and reusability through responsible sharing. However, notable absence remains in the discussion concerning approaches that prioritize fairness for individuals whose data is shared and utilized for various purposes.[199]

Thus far, individuals have had minimal meaningful involvement in the governance of data sharing. While consent has been utilized to grant individuals some control over their health data, the inadequacies of different consent models have been extensively debated in academic literature and policy documents.[200] Introducing additional consent, such as data altruism consent, provides individuals with the choice to consent to their data being shared for the broader public interest.[201] However, this approach does little to bolster their ability to negotiate how their data is shared, the conditions under which it is shared, and the subsequent distribution of outcomes arising from its use.[202]

The establishment of collective data governance, exemplified by initiatives like the EHDS, poses challenges due to the ongoing ambiguity surrounding what constitutes "fair" data sharing from a citizen's standpoint.[203] This ambiguity stems from varying individual perceptions of "fairness";

---

[199] Boeckhout M. and others, 'The FAIR guiding principles for data stewardship: fair enough?' (2018) 26 Eur J Hum Genet 931
[200] Dianne Nicol and others., 'Consent insufficient for data release' (2019) 364 Science, 445-446
[201] Mahsa Shabani, 'Will the European Health Data Space change data sharing rules?' (2022) 375 Science 1357, 1359
[202] ibid
[203] ibid

while some directly associate it with the degree of control they wield over their data, others demand transparent benefit-sharing models and equitable distribution of research outcomes.[204] Consequently, some private entities have recently introduced innovative models to share the financial benefits of data sharing with individuals.[205] However, public research bodies and regulators have predominantly refrained from adopting such approaches.[206]

Apart from the 'fairness' of processing the sensitive health data of patients, the objection raised by the EDPB and EDPS also relates to its security. In their Joint Opinion they state that it would be appropriate to include a more concrete description of the safeguards foreseen for the processing of the data, in accordance with Article 89 (2) GDPR.[207] The reference to safeguards is present in Article 45 (2) (e) and (f) of the Proposal already discussed in this thesis. The Joint Opinion considers this it to be vague. Throughout the text it is required to offer the data to third parties for the purposes provided for in Article 34 of the Proposal, wherever possible in anonymised format. In the event that the transmission of such personal electronic health data cannot be anonymized, the data should be provided in pseudonymised format.[208] Some argue that this could function as a reasonably secure system, which will probably need to be refined in practice[209], however, allowing anonymisation as a guarantee of security of health data of such sensitive nature should indeed be considered ineffective in this day and age.

---

[204] Murtagh MJ and others, 'Engaged genomic science produces better and fairer outcomes: an engagement framework for engaging and involving participants, patients and publics in genomics research and healthcare implementation' (2021) Wellcome Open Res 2021 1, 4

[205] Ahmed E, Shabani M., 'DNA Data Marketplace: An Analysis of the Ethical Concerns Regarding the Participation of the Individuals' (2019) 10 Front Genet 1, 3

[206] ibid

[207] Joint Opinion EDPB-EDPS (n 4) para 25

[208] EHDS (n 7) art 44 (3)

[209] The Use of Health Data for Biomedical Research (n 110) 27

4.8. Anonymisation

The aim of data anonymisation is to transform personal data in such a manner that the data subject is no longer identified or identifiable.[210] Effective anonymisation process, hence, reduces the risk of re-identification.[211] That can be achieved by using additional information which will make it easier to identify the subject.[212] However, in this day and age, Big Data has acquired special importance and to design an effective anonymisation solution becomes more complicated.

Big Data is a concept arising out of the practice of large companies such as Meta or Apple which handle data daily also due to an increase of computational storage, decrease of storage costs, cloud computing or Internet of Things.[213] It is a reference to large volumes of complex data that is processed at a very high speed.[214] To get more specific, we can extract three main categories of Big Data by its characteristics, also known as 3 Vs: volume, variety, and velocity.[215] Therefore, Big Data is data that contains greater variety, arriving in increasing volumes and with more velocity. Data sets comprising of Big Data are so voluminous that traditional data processing software is not capable of managing them.[216] On the other hand, this innovation allows to address such business issues that were hardly tackled before.[217]

---

[210] Imperva, 'What is Data Anonymization?' <https://www.imperva.com/learn/data-security/anonymization/> accessed 10 December 2023
[211] Ira S. Rubinstein & Woodrow Hartzog, 'Anonymization and Risk' (2016) 91 Wash L Rev 703, 733
[212] Alvaro Moreton & Ariadna Jaramillo, 'Anonymisation and Re-Identification Risk for Voice Data' (2021) 7 Eur Data Prot L Rev 274, 275
[213] Oracle, 'What is Big Data?' < https://www.oracle.com/big-data/what-is-big-data/> accessed 10 December 2023
[214] ibid
[215] ibid
[216] ibid
[217] ibid

Since anonymous data guarantees that an individual will not be singled out when linked with other available information, the whole dataset needs to be deeply analysed before the right anonymization approach is selected.[218] Once the data volume increases, this process gets more costly and challenging as the mere exclusion of the direct identifiers like name, ID, place of residence or gender is not sufficient.[219] On top of that, the velocity of Big Data also implies that the data needs to be processed at the high-speed and consequently often in real-time. The difficult performance of the analysis must result in the final selection of the anonymization strategy, calculation of the privacy and utility metrics.[220] Hence, it is not unexpected that the procedure is inherently challenging.

Moreover, this research revealed a critical concern: even when data is presumed to be anonymized, the risks to the fundamental rights and freedoms of individuals persist. Consequently, the GDPR remains applicable, emphasizing the ongoing importance of safeguarding personal data against potential privacy infringements.

Anonymisation means that personal data can no longer identify a natural person. The same is made mandatory by the Proposal in the Article 45(3) and even subjected to appropriate penalties ich such re-identification takes place.[221] For purposes of research, identification of a natural person is not always necessary, and therefore, the data is most often anonymised.[222] However, with modern technologies and lots of information being available online, combating various datasets can easily

---

[218] Gradiant, 'Data anonymization in Big Data scenarios: an open challenge to become GDPR compliant' (*Gradiant.org*, 11.11.2021) <https://www.gradiant.org/en/blog/infinitech-data-anonymization-big-data-gdpr/> accessed 10 December 2023
[219] ibid
[220] ibid
[221] EHDS (n 7) art 45 (3)
[222] Alvaro Moreton & Ariadna Jaramillo, 'Anonymisation and Re-Identification Risk for Voice Data' (2021) 7 Eur Data Prot L Rev 274, 276

result in such a re-identification of anonymised data. In 2015, Latanya Sweeney authored an article that demonstrated her capability to re-identify supposedly anonymized datasets procured from a hospital.[223] She accomplished this by cross-referencing the dataset with newspaper articles from the corresponding year. Through this method, Sweeney successfully identified 43% of the individuals within the anonymized dataset.[224] This study underscored the formidable challenge of truly anonymizing data, highlighting the near impossibility of achieving complete anonymity. On the other hand, it was noted in several studies that various differences exist between Member State as to what constitutes tools likely to be used to identify individuals.[225] In scholarly discussions, it has been observed that data that's made completely anonymous to the best possible extent, with no remaining chance of being linked back to individuals, might become less useful for detailed and sophisticated research purposes.[226]

With respect to the abovementioned findings, it is unlikely to say that anonymization can be effective in this age where Big Data continuous to expand and as the technology advances. The shortcomings of data protection techniques in this area are pointing out to its outdated approach which can be effective when data processing is limited to isolated applications but not today when capabilities of technological advancement enable widespread sharing, combining and storing of large data sets. It has been ruled by Judge Michal Agmon-Gonen of the Tel Aviv District Court that "*given the scope of data collection and use, and trading this information, enables the cross-referencing of information from different databases, and thus also trivial information such as*

[223] Latanya Sweeney, 'Only You, Your Doctor and Many Other May Know' (2015) Technology Science 1
[224] ibid 3
[225] European Commission (DG Health and Food Safety), 'Assessment of the EU Member States' rules on health data in the light of GDPR' (2021) p 111
[226] Christopher Mondschein and Cosimo Monda, 'Chapter 5: The EU's General Data Protection Regulation (GDPR) in a Research Context' in Kubben P and Dumontier M and Dekker A (eds), *Fundamentals of Clinical Data Science* (Cham Springer 2019) 60

location, may be cross-referenced with other data and reveal many details about a person, which infringe upon his privacy."[227] Today, data held by a processor can be readily linked with data beyond the control of the processor thereby enabling re-identification and exposing the processor to liability as well as invading on privacy of individuals.

Even though the anonymisation is permitted as a safe method to secure personal health information, the EDPB and EDPS is right in stating that such broad concept of authorisation as presented in the Proposal opens the door to a possible abusive use of the right of access to electronic health data.[228] It is apparent that anonymisation is likely to allow for identifiability and it seems to be welcome especially in the context of research. As such it should undoubtly inside the scope of the legal regime of data protection. Consequently, additional safeguards accompanying such authorisation mechanism to access the health data should be provided.[229]

4.9. Competence issues

One of the virtues of the Proposal lies in its commendable effort to unify the Member States' regulations governing the processing of data for biomedical research purposes, especially when it comes to secondary use of data. So far, the effort does not appear to be failing in terms of the Commission's more active role in this area by using its executive powers.[230] This is shown in the conferral of implementing powers to Commission by virtue of Regulation No. 182/2011 to ensure uniform conditions for the implementation of this Proposal.[231] as well as the repeal of Article 14 setting up a voluntary network in the Directive 2011/24/EU which showed limited effectiveness

[227] *The Association of Nursing Companies v. The Ministry of Defense* [2017] Tel Aviv District Court 28857-06-17
[228] Joint Opinion EDPB-EDPS (n 4) para 53
[229] Joint Opinion EDPB-EDPS (n 4) para 53
[230] The Use of Health Data for Biomedical Research (n 110) 27
[231] EHDS (n 7) recital 69

of eHealth Network after the evaluation of its digital aspects. As a result, the Article 14 will be replaced by the EHDS.[232] These aspects are crucial for the Proposal's success. The legislators are aware of this because if the implementation of the Directive on cross-border healthcare has shown anything, it is that relying on voluntary action by Member States is not the best strategy available for getting the data flowing.

The problem is that it is not at all easy to determine whether these matters should be regulated by means of a regulation establishing common bases throughout the EU or whether, on the contrary, they should be left to the Member States to regulate.[233] In this area, the EU institutions have to make trade-offs in order to respect the distribution of competences provided for in Article 168 of the Treaty, which states that the Member States are responsible for their health policy.[234] However, EU has been insufficient in this area mostly because of the principle of subsidiarity in Article 5 of the Treaty on the EU which applies and acknowledges measures regarding the rights of individuals concerning their electronic health data. Even though ensuring interoperability and establishing a unified framework for the primary and secondary use of this data might be most effective at the Union level, attempting to regulate this area has proven to be problematic because of the Member States' strong stance for completing their own national policies.

On the other hand, the question is also complex: once the competence of the EU institutions is recognized, what should be done if the provisions of the Proposal were to conflict with the regulations drawn up in the Member States with regard to the processing of health data described in Chapter III section (c) of this thesis? In this respect, the Joint Opinion of the EDPB and EDPS

[232] EHDS (n 7) recital 73
[233] The Use of Health Data for Biomedical Research (n 110) 28
[234] ibid

has pointed out that the Proposal should *clarify how the exception to Article 9(1)* GDPR (regarding the prohibition of processing of sensitive data), *stemming from the Proposal but as yet not being explicitly specified in any of the provisions of the Proposal, intend to reconcile with all different national Member States' laws*[235] which are based on Article 9(4) allowed to introduce further conditions with regard to processing of data concerning health.[236] It is well known that, in principle, the Regulations are binding, so that they can be applied in all the Member States. Those countries whose regulations contradict the Proposal should find a compatible interpretation or amend them. However, the important question raised is no longer whether the law of the Member States can prevail or not, but whether the delegation made by the GDPR should be considered repealed after the adoption of the EHDS.[237] Or whether the opposite should be considered. The need to answer this thorny question has been clearly stated in the Joint Opinion. However, it is believed that the only possible solution is for the provisions adopted by the Member States not to impose restrictions to the free exchange of personal data, since the opposite would not only be contrary to the provisions of the Proposal but also to the very spirit of the GDPR, as expressed, for example, in Recital 53.[238]

Although there may be a sense of jurisdiction conflict and doubts about the applicable law, these debates are diluted in a single and obvious certainty that both the GDPR and this Proposal oblige the Member States to remove obstacles to the free circulation of such data. Thus, if there are provisions in any of the national regulations that may conflict with the provisions of the Proposal, at this point, they must be interpreted in a compatible manner, or, ultimately, amended or repealed.

---

[235] Joint Opinion EDPB-EDPS (n 4) para 89
[236] GDPR (n 5) art 9 (4)
[237] Joint Opinion EDPB-EDPS (n 4) para 109
[238] GDPR (n 5) recital 53

5. POLICY OPTION TO ACHIEVE PRIVACY PROTECTION

Currently, heavy negations are taking place at the EU Parliament and the EU Council over the text of the EU Commission's Proposal. The Proposal is considered to have a sensitive nature and together with its complexity, lengthy and challenging debates are required on all the levels, starting from the civil society, through experts, policymakers and other stakeholders.[239] As expected, the co-rapporteur of the Proposal has signalled that the agreements regarding the secondary use of health data were the hardest to reach.[240] One of the central discussions revolves around patients' autonomy over their health information and the mechanisms that should be in place to safeguard their consent.

The Commission's initial proposal raised eyebrows due to the decision not to incorporate patient input regarding the reuse of their data described in the previous chapter. This raised immediate scepticism among various stakeholders, including members of the Parliament.[241] According to Sokol, a prominent figure in this discussion, the notion of implementing such a proposal without considering patients' preferences was deemed unlikely to gain approval from the Parliament. As a response, the rapporteurs of the EHDS proposal recommended an "opt-out" option.[242] This mechanism allows patients who prefer not to have their health data utilized for secondary purposes to choose exclusion from the system.[243] However, it's important to note that the proposal omitted the "opt-in" option, which would involve obtaining explicit consent from patients.[244] Sokol

[239] EU Parliament solving riddle of secondary use of data in health data space (n 98)
[240] ibid
[241] European Parliament, 'EP supports creating EU Health Data Space to boost access to data and research' (2023) < https://www.europarl.europa.eu/news/en/press-room/20231208IPR15783/ep-supports-creating-eu-health-data-space-to-boost-access-to-data-and-research> accessed 28 December 2023
[242] EU Parliament solving riddle of secondary use of data in health data space (n 98)
[243] ibid
[244] ibid

highlighted the perceived inadequacy of the opt-in approach due to concerns regarding insufficient data for research, particularly in areas such as rare diseases, where large datasets are crucial.[245] Sandra Gallina, the director-general of the Commission's DG SANTE, emphasized the necessity of considering individuals who might not be part of a large demographic pool. Gallina stressed the importance of enabling the sharing of health data for the benefit of smaller populations without disregarding privacy concerns.[246] Gallina expressed firm support for the Commission's proposal, indicating a reluctance towards implementing opt-outs, primarily due to the financial implications for member states. However, she acknowledged the necessity of allowing patients a say in how their data is utilized.

Meanwhile, the European Parliament's civil liberties committee (LIBE) and health committee (ENVI), which jointly oversee the EHDS proposal, exhibited varying degrees of leniency regarding data usage. Members of LIBE appeared more cautious and stringent compared to their counterparts in ENVI.[247] Civil society groups, exemplified by the European Digital Rights Association (EDRi), have been actively advocating for stronger patient empowerment concerning the secondary use of health records within the EHDS framework. A petition, supported by over 100,000 individuals, urged for explicit consent from patients regarding the sharing of their medical records for secondary purposes.[248] Despite the Parliament's suggestion of the opt-out option, those supporting the petition deemed it insufficient. They continue to push for explicit consent, a stance

---

[245] ibid

[246] EU40, 'European Health Data Space: a milestone for patient empowerment' (2023) <https://www.eu40.eu/news/european-health-data-space-a-milestone-for-patient-empowerment/> accessed 10 December 2023

[247] European Parliament, 'REPORT on the proposal for a regulation of the European Parliament and of the Council on the European Health Data Space' (2023) <https://www.europarl.europa.eu/doceo/document/A-9-2023-0395_EN.html> accessed 10 December 2023

[248] European Public Service Union, 'Petition calls on European Parliament to safeguard patient data privacy' (2023) <https://www.epsu.org/article/petition-calls-european-parliament-safeguard-patient-data-privacy> accessed 10 December 2023

echoed by shadow rapporteurs aligned with these advocacy efforts.[249] Shadow rapporteur Petar Vitanov stressed the inadequacy of the opt-out option, highlighting the collective intent to pursue stronger measures during negotiations.[250] Even if the opt-out option is eventually adopted to align with the proposed standards in the EHDS, ensuring a sense of security and trust among individuals within the system remains paramount.[251] The need for a balance between facilitating data utilization for research while respecting individual privacy rights remains a critical focal point for ongoing deliberations within the Parliament and the Council.

6. CONCLUSION

The EHDS proposal marks a significant departure in the handling of electronic health data within the EU. Aimed at establishing a comprehensive framework for the secondary use of health data, the Proposal seeks to harness the immense potential of health information for research, policymaking, and technological innovation. However, this ambitious initiative presents significant concerns regarding its alignment with the GDPR. The EHDS framework appears to deviate substantially from the established GDPR provisions, which serve as the fundamental cornerstone governing health data processing across the EU. This deviation introduces legal uncertainties and challenges the existing normative and regulatory landscape for accessing and utilizing electronic health data. While acknowledging the potential benefits of leveraging health data for scientific research, evidence-based policymaking, and healthcare advancements, it is imperative to recognize the inherent risks and compromises associated with this endeavor. The

[249] ibid
[250] Giedre Peseckyte, 'GDPR harmonisation could be key to unleashing health data's potential' (*Euroactiv.com,* 4 October 2023) <https://www.euractiv.com/section/health-consumers/news/gdpr-harmonisation-could-be-key-to-unleashing-health-datas-potential/> accessed 10 December 2023
[251] ibid

EHDS lacks mechanisms to uphold the fundamental rights of individuals, particularly concerning their right to privacy and control over their medical records. Crucially, the EHDS disregards the GDPR's foundational principles by not affording individuals the necessary consent and control mechanisms over the sharing and commercial exploitation of their health data. The proposal sidelines patient autonomy and doctor-patient confidentiality, essential elements safeguarded by established data protection laws.

The EHDS framework's inclination towards administrative efficiency and technological advancements inadvertently compromises individual privacy rights, exposing sensitive health records to potential exploitation by various entities, including researchers, pharmaceutical companies, and tech giants, without explicit patient consent. Despite its objective to modernize and harmonize healthcare systems across the EU, the EHDS Proposal comes at a cost — the erosion of individuals' rights to privacy and control over their medical data. The proposal's intent to create a harmonized approach for health data usage overlooks the importance of preserving individuals' rights enshrined in the GDPR. Addressing the challenges posed by the fragmented landscape of Member State laws on health data processing, ensuring transparency, and creating a secure environment for patient data are complex tasks. However, the current EHDS Proposal significantly restricts data subjects' rights to data protection, rendering it incompatible with the GDPR. The need for a balanced approach that respects individual rights while advancing healthcare innovation remains a paramount consideration in shaping the future of health data governance in the EU.

Bibliography

Legislation

1. Act on Secondary Use of Health and Social Data 2019
2. COM (2022) 68 final; Regulation (EU) 2017/745 of the European Parliament and of the Council on medical devices (Medical Devices Regulation) [2017] OJ L 117/1
3. Consolidated version of the Treaty on the Functioning of the European Union [2012] OJ C326/47 (TFEU)
4. Directive (EU) 2016/1148 of the European Parliament and of the Council concerning measures for a high common level of security of network and information systems across the Union [2016] OJ L 194/1
5. Directive 2011/24/EU of the European Parliament and of the Council of 9 March 2011 on the application of patients' rights in cross-border healthcare [2011] OJ L 88/45
6. European Commission, 'Proposal for a Regulation of the European Parliament and of the Council on the European Health Data Space', COM (2022) 197 final
7. Proposal 2022/0047 (COD) for a Regulation of the European Parliament and of the Council on harmonized rules on fair access to and use of data (Data Act)
8. Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L 199/1
9. Regulation 2022/868 of the European Parliament and of the Council on European Data Governance (Data Governance Act) [2022] OJ L 152/1

Court's Decisions

1. Case C-101/01 *Lindqvist* [2003] ECR I – 12992
2. *The Association of Nursing Companies v. The Ministry of Defense* [2017] Tel Aviv District Court 28857-06-17

European Data Protection Board Documents

1. Article 29 Working Party, ‘Guidelines on consent under Regulation 2016/679’ (2018)
2. European Data Protection Board, ‘Opinion 3/2019 of the EDPB from 23.1.2019 on concerning the Questions and Answers on the interplay between the Clinical Trials Regulation and the GDPR’ (2019)
3. European Data Protection Board, European Data Protection Supervisor, ‘EDPB-EDPS Joint Opinion 03/2022 on the Proposal for a Regulation on the European Health Data Space’ (2022)
4. European Data Protection Supervisor, “Preliminary Opinion 8/2020 on the European Health Data Space,” November 17, (2020)

Academic Sources

1. Ahmed E, Shabani M., 'DNA Data Marketplace: An Analysis of the Ethical Concerns Regarding the Participation of the Individuals' (2019) 10 Front Genet 1
2. Alvaro Moreton & Ariadna Jaramillo, 'Anonymisation and Re-Identification Risk for Voice Data' (2021) 7 Eur Data Prot L Rev 274
3. Bentzen, H. and others, ‚Remove obstacles to sharing health data with researchers outside of the European Union' (2021) 27 Nat Med 1329
4. Boeckhout M. and others, 'The FAIR guiding principles for data stewardship: fair enough?' (2018) 26 Eur J Hum Genet 931
5. Carmela Troncoso, 'Deploying Decentrelized, Privacy-Proximity Tracing', 65 Communication of the ACM 48
6. Christopher Mondschein and Cosimo Monda, 'Chapter 5: The EU's General Data Protection Regulation (GDPR) in a Research Context' in Kubben P and Dumontier M and Dekker A (eds), Fundamentals of Clinical Data Science (Cham Springer 2019) 60
7. Dianne Nicol and others., 'Consent insufficient for data release' (2019) 364 Science 445
8. Dubanska & Co, 'At a glance: data protection and management of health data in Czech Republic' (*Lexology.com,* 25 January 2023 <https://www.lexology.com/library/detail.aspx?g=63a1a593-a72d-4c94-8b5c-958301c02965&utm_source=Lexology+Daily+Newsfeed&utm_medium=HTML+email+-+Body+-+General+section&utm_campaign=Lexology+subscriber+daily+feed&utm_content=Lexology+Daily+Newsfeed+2023-06-16&utm_term=> accessed 10 December 2023
9. European Commission (DG Health and Food Safety), 'Assessment of the EU Member States' rules on health data in the light of GDPR' (2021)
10. Giorgia Bincoletto, 'Scientific Research Processing Health Data in the European Union: Data Protection Regime vs. Open Data' (2023) 11 J Open Access L 1
11. Global Alliance for Genomics & Health, 'GDPR Brief: the Finnish Secondary Use Act 2019 (May 2020 bonus brief)' (2020) <https://www.ga4gh.org/news_item/ga4gh-gdpr-brief-the-finnish-secondary-use-act-2019-may-2020-bonus-brief/> accessed 10 December 2023

12. Inigo de Miguel Beriain, 'The Use of Health Data for Biomedical Research in the Light of the Proposal for a Regulation of the European Parliament and of the Council on the European Health Data Space' (2023) 60 Rev Juridica Castilla & Leon 7
13. Ira S. Rubinstein & Woodrow Hartzog, 'Anonymization and Risk' (2016) 91 Wash L Rev 703
14. J. Bovenberg and others, 'How to fix the GDPR's frustration of global biomedical research' (2020) Science 40
15. Kieran C. O'Doherty and others, 'Toward better governance of human genomic data' (2021) Nat Genet 1
16. Latanya Sweeney, 'Only You, Your Doctor and Many Other May Know' (2015) Technology Science 1
17. Lee WB, Choi SJ., 'Secondary Use Provisions in the European Health Data Space Proposal and Policy Recommendations for Korea' (2023) Healthc Inform Res 199
18. M. Shabani, 'Will the European Health Data Space change data sharing rule' (2022) Science 1357
19. Mahsa Shabani, 'Will the European Health Data Space change data sharing rules?' (2022) 375 Science 1357
20. McLennan S, Celi LA, Buyx A, 'COVID-19: Putting the General Data Protection Regulation to the Test' [2020] JMIR Public Health Surveill 6
21. Murtagh MJ and others, 'Engaged genomic science produces better and fairer outcomes: an engagement framework for engaging and involving participants, patients and publics in genomics research and healthcare implementation' (2021) Wellcome Open Res 2021 1
22. Petros Terzis, 'Compromises and Asymmetries in the European Health Data Space' [2022] Eur J Health Law 345
23. S. McLennan, and others, 'Practices and Attitudes of Bavarian Stakeholders Regarding the Secondary Use of Health Data for Research Purposes During the COVID-19 Pandemic' [2022] 24 J Med Internet Res 6
24. Tamar Sharon, 'From hostile worlds to multiple spheres: towards a normative pragmatics of justice for the Googlization of health' 24 Medicine, Health Care and Philosophy 315

25. Tugce Schmitt and others, ‘What does it take to create a European Health Data Space? International commitments and national realities‘ (2023) Vol 179 Zeitschrift für Evidenz, Fortbildung und Qualität im Gesundheitswesen 1
26. Victoria Chico, ‘The impact of the General Data Protection Regulation on health research’ (2018) 128 British Medical Bulletin 109

Other Documents and Web Sources

1. Alex Rajagopalan, ‘Shooting For The Stars: The Bold European Health Data Space (EHDS) Proposed By The EU Commission‘ (*Informationgovernanceservices*, 13 May 2022) <https://www.informationgovernanceservices.com/shooting-for-the-stars-the-bold-european-health-data-space-ehds-proposed-by-the-eu-commission/> accessed 10 December 2023
2. Cyber Risk GmbH, 'The European Health Data Space (EHDS)‘ (*European-helath-data-space.com,* 2022) <https://www.european-health-data-space.com/> accessed 10 December 2023
3. EU40, ‘European Health Data Space: a milestone for patient empowerment‘ (2023) <https://www.eu40.eu/news/european-health-data-space-a-milestone-for-patient-empowerment/> accessed 10 December 2023
4. European Commission, European Health Union: Protecting our health together‘ <https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/promoting-our-european-way-life/european-health-union_en> accessed 10 December 2023
5. European Digital Rights and others, ‘Joint Public Letter to EU lawmakers on patients' rights in the European Health Data Space‘ (2023) <https://edri.org/wp-content/uploads/2023/04/Joint-public-letter-on-consent-in-EHDS-2.pdf> accessed 10 December 2023
6. European Parliament, ‘EP supports creating EU Health Data Space to boost access to data and research’ (2023) <https://www.europarl.europa.eu/news/en/press-room/20231208IPR15783/ep-supports-creating-eu-health-data-space-to-boost-access-to-data-and-research> accessed 28 December 2023

7. European Parliament, 'REPORT on the proposal for a regulation of the European Parliament and of the Council on the European Health Data Space' (2023) <https://www.europarl.europa.eu/doceo/document/A-9-2023-0395_EN.html> accessed 10 December 2023
8. European Parliament, European health data space (*Europarl.europa.eu,* 6 December 2023) <https://www.europarl.europa.eu/thinktank/sk/document/EPRS_ATA(2023)754642> accessed 10 December 2023
9. European Public Service Union, 'Petition calls on European Parliament to safeguard patient data privacy' (2023) <https://www.epsu.org/article/petition-calls-european-parliament-safeguard-patient-data-privacy> accessed 10 December 2023
10. Giedre Peseckyte, 'EU Parliament solving riddle of secondary use of data in health data space' (Euroactiv.com, 10 July 2023) <https://www.euractiv.com/section/health-consumers/news/eu-parliament-solving-riddle-of-secondary-use-of-data-in-health-data-space/> accessed 10 December 2023
11. Giedre Peseckyte, 'GDPR harmonisation could be key to unleashing health data's potential' (Euroactiv.com, 4 October 2023) <https://www.euractiv.com/section/health-consumers/news/gdpr-harmonisation-could-be-key-to-unleashing-health-datas-potential/> accessed 10 December 2023
12. Gradiant, 'Data anonymization in Big Data scenarios: an open challenge to become GDPR compliant' (Gradiant.org, 11.11.2021) <https://www.gradiant.org/en/blog/infinitech-data-anonymization-big-data-gdpr/> accessed 10 December 2023
13. Imperva, 'What is Data Anonymization?' <https://www.imperva.com/learn/data-security/anonymization/> accessed 10 December 2023
14. Oracle, 'What is Big Data?' < https://www.oracle.com/big-data/what-is-big-data/> accessed 10 December 2023
15. Towards the European Health Data Space, 'Country factsheets: Mapping health data management systems through country visits' (2023) <https://tehdas.eu/app/uploads/2023/04/tehdas-mapping-health-data-management-systems-through-country-visits.pdf> accessed 10 December 2023
16. Towards the European Health Data Space, 'Joint Action Towards the European Health Data Space – TEHDAS' (2022) < https://tehdas.eu/> accessed 10 December 2023

17. Towards the European Health Data Space, 'Member states' readiness to benefit from the EHDS regulation varies' (2023) <https://tehdas.eu/results/member-states-readiness-to-benefit-from-the-ehds-regulation-varies/> accessed 10 December 2023
18. Towards the European Health Data Space, 'Packages' (2022) < https://tehdas.eu/packages/> accessed 10 December 2023
19. Towards the European Health Data Space, 'Sitra has been appointed to lead a project of 29 countries to realise the European health data space' (2023) https://tehdas.eu/news/sitra-has-been-appointed-to-lead-a-project-of-29-countries-to-realise-the-european-health-data-space/ accessed 10 December 2023
20. Towards the European Health Data Space, 'TEHDAS study: Member states to harmonize national legislation to enable the secondary use of health data (2023) <https://tehdas.eu/results/tehdas-study-member-states-to-harmonise-national-legislation-to-enable-the-secondary-use-of-health-data/> accessed 10 December 2023