Anita Kisborsó*

Legal Aspects of Data Sharing in the European Health Data Space

Abstract

This article explores the legal framework for data sharing established by the European Health Data Space Regulation (EHDS), the European Union's first sector-specific data space initiative. The study critically examines the legal implications of the EHDS's mandatory data sharing mechanism, which aims to address structural imbalances in the data economy by compelling both public and private data holders to grant access to electronic health data. The article analyses the EHDS's data access model and contrasts it with traditional data contracts governed by private law. Key legal challenges are identified, including the ambiguous scope of the *general interest of society,* the *limitations of data holders' autonomy* and the lack of established legal concepts for electronic data. The author argues that while the EHDS offers significant benefits, such as a unified dataset catalogue and enhanced access to health data for research and innovation, it also raises concerns about legal clarity, liability allocation, and investment incentives. The article concludes that further harmonisation and clarification are necessary to ensure legal certainty and market trust in the evolving European data economy.

Keywords: European Health Data Space (EHDS), European data strategy, secondary use of electronic health data, data sharing, data permit

* PhD Student at ELTE Law, Department of Private International Law and European Economic Law.

I Introduction

In the global competition, the European Union plans to catch up with the American and Chinese data economies, a goal outlined in the European Data Strategy published on 19 February 2020,[1] as well as the EU legislation based on it and the creation of a single data market. The European Union encourages the free flow of electronic data through regulation and the implementation of EU-level projects to improve the data-driven economy within the European Union.[2]

To achieve this goal, the European Commission has proposed ambitious legislation to make data access easier for businesses and researchers. Furthermore, the European Union aims to create data spaces, genuine single markets for digital data, where economic entities can access high-quality data, both personal and non-personal, public and non-public, to improve their products and services, make informed decisions, and promote innovation. These interoperable, domain-specific, common data spaces[3] – such as those for health, finance, agriculture, energy and mobility – are currently being created. The first and pioneering data space is the European Health Data Space.

The EHDS regulation[4] (EHDS) creates the European Health Data Space by providing common mechanisms, rules, standards, infrastructure and a governance framework for the primary and secondary use of electronic health data.[5] It introduces a *new legal framework for data sharing* in the European data economy through strict regulation and *compulsory data sharing*. The fundamental assumption behind the EHDS is that the insufficient volume of voluntary data sharing is hindering the economy's growth. Imbalances in the data economy and restricted access to digital data result in broad economic inefficiencies. There are two main reasons for this. First, big data companies that have high-quality, large datasets do not have an interest in sharing data, especially with their competitors. Second, despite the EU legal acts[6] already in force, data held by public sector organisations does not enter the data

1 A European strategy for data, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Brussels, 19.2.2020, COM(2020) 66 final, 3.

2 European strategy for data, 16.

3 European strategy for data, 12.

4 Regulation (EU) No 2025/327 of the European Parliament and of the Council of 11 February 2025 on the European Health Data Space and amending Directive 2011/24/EU and Regulation (EU) 2024/2847 [2025] OJ L327.

5 EHDS Article 1(1).

6 The most relevant legal acts for data sharing in the public sector: Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act) OJ L152, and Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information OJ L172.

economy in volumes sufficient to have a significant impact.[7] The EU legislator hopes to reduce such imbalances by introducing a mandatory data-sharing mechanism in the EHDS, which is aimed at combating the concentration of data in the hands of a few powerful players and their low level of transparency.[8]

The aim of this article is to provide an interpretation of the legal characteristics of data sharing under the EHDS mechanism and consider the possible effects of mandatory data sharing in terms of the legal aspects of the data economy. In this article, I will present the subjective and objective scope and objectives of the EHDS, as well as the administrative legal relationship granting access to data in comparison with private law instruments. Furthermore, I will present the elements that may affect the development of the data economy.

The article focuses on the question of the extent to which the new legal framework transforms the legal relationship between data owners and data users, as well as third parties who provide access to data, and what its new elements are compared to the current practice in the data economy.

The main method of this study is interpreting the text of the EHDS and analysing the legal environment of the European data economy and the legal characteristics of data sharing agreements based on model law. The article is structured around three aspects: (1) the legal framework of the EHDS and its administrative decisions concerning data access; (2) a comparative analysis of mandatory data-sharing obligations under the EHDS and private data contracts; and (3) potential impacts of mandatory data sharing and of the EHDS on the health data market. This analysis is both a descriptive and a critical examination of the changes in the data economy introduced by the EHDS for those involved in sharing electronic health data.

II The EHDS and the European Union's data regulation framework

The EHDS entered into force on 26 March 2025. Most provisions of the regulation will become applicable after four years, in 2029. The legal basis is Articles 16 and 114 of the Treaty on the Functioning of the European Union.[9] Article 16 TFEU provides the legal

[7] The reason for this is that the safeguards for data sharing (data protection, technology) and the rules for interoperability have not been developed to the extent that they can ensure the secure provision of data uniformly in the EU. The incentive for Member States to start reusing electronic health data held by public sector organisations is market demand, particularly the need for data from researchers. To meet these needs, the reuse of public sector health data has already been actively initiated in some Member States (eg, Finland and France), providing important knowledge for the implementation of the EHDS.

[8] Marta Musidlowska, *Power to the Health Data Access Bodies. Addressing Governance Challenges for the Secondary Use of Electronic Health Data* (Part 1/3) (EHDS Blogpost Series 2024) <https://www.law.kuleuven.be/citip/blog/power-to-the-health-data-access-bodies-addressing-governance-challenges-for-the-secondary-use-of-electronic-health-data-part-1-3-ehds-blogpost-series/> accessed 1 December 2025.

[9] Consolidated version of the Treaty on the Functioning of the European Union [2012] OJ C326/47.

basis for EU rules that protect personal data while enabling its free movement within the Union. According to Article 114 TFEU, 'the European Parliament and the Council shall adopt measures for the approximation of the provisions laid down by law, regulation, or administrative action in Member States that have as their objective the establishment and functioning of the internal market'. The creation of uniform rules, as explained by the EHDS, improves the functioning of the internal market, especially in relation to the development and use of health records systems.[10]

Based on the legislative plan of the European strategy for data, the first pillar of the regulatory basis for the European data economy is the development of a horizontal framework.[11] The Data Governance Act (DGA)[12] and the Data Act[13] are the two regulatory legs of this horizontal framework. The two regulations determine how the process and access to data should be structured.[14] Both regulations contribute to increasing access to data, and they are transversal legislation that applies to data across sectors. The DGA promotes voluntary data sharing by structuring the data economy, while the Data Act defines who can create value from data and under what conditions. The Data Act complements the provisions of the DGA and harmonises fair access to data in the case of connected products on online platforms and also defines the overall technical interoperability framework required for data exchange.[15]

The EHDS, building on the rules of the DGA and the Data Act, contains sector-specific rules[16] as *lex specialis* law by establishing data sharing tools and platforms, governance frameworks, and establishing data quality, availability and interoperability.[17] The EHDS focuses on two major areas regarding the exchange of electronic health data: the primary and secondary use of health data.

The primary use of health data refers to the processing of health data for the provision of healthcare, which involves assessing, maintaining, or restoring the state of health of the natural person to whom those data relate.[18] For instance, if a Hungarian citizen needs to see

[10] EHDS Recital 1.

[11] Quentin Fontaine, Jan Clinck, 'The European Health Data Space Proposal: A First Look at the Newest Piece of the EU Data Sharing Puzzle' (2022) 6 European Pharmaceutical Law Review 87, DOI: 10.21552/ehpl/2022/2/8

[12] Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act) OJ L152.

[13] Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act) OJ L2023/2854.

[14] Jürgen Taeger, Jan Pohle, *Computerrechts-Handbuch, Informationstechnologie in der Rechts- und Wirtschaftspraxis* (C.H. Beck 2025, München) Teil 12: 120.5 Rn.18.

[15] European strategy for data 8.

[16] B. Martens, 'Are new EU data market regulations coherent and efficient?' (2023) Working Paper, 21/2023, Bruegel, 1.

[17] Fontaine and Clinck 88.

[18] EHDS Article 2(1)(d).

a doctor in Germany, the German doctor can access important data related to the Hungarian patient. The primary use of electronic health data, as defined in the EHDS, therefore supports the free movement of individuals.[19]

This article deals only with the *secondary use of electronic health data*, the second major part of the regulation. The DGA lays down generic conditions for the reuse of public sector data and does not create a genuine right to its reuse, but rather ensures that no data users are discriminated against. EDHS, however, supplements this framework with a *right to secondary data use*, which establishes a purpose-bound, genuine data access claim as a subjective right.[20]

While the DGA adopts the term *'re-use', the EHDS regulation uses the term 'secondary use',* which refers to the processing of electronic health data for purposes set out in the EHDS, other than the initial purposes for which it was collected or produced (primary use). The term 'secondary use' used by the EHDS specifically refers to the reuse of electronic health data according to the mechanism set out in Chapter IV of the EHDS. Thus, the EHDS uses a unique term for the reuse of electronic health data that only applies to the reuse of data under the scope of this legislation. In other words, when we talk about the secondary use of health data, in legal terminology, we are talking only and exclusively about the use of data associated with the EHDS procedure.

III Subjective and objective scope of the EHDS

1 Data holders

The regulation contains obligations for all health data holders from both the private and public sectors. The subject matter of the regulation includes both publicly held data and data held by for-profit, non-profit businesses, non-governmental organisations or any other legal entities. Only natural persons and microenterprises are exempted from the regulation.[21] Member States may provide in their national law that the data-holder-related duties of certain categories of data holders are to be fulfilled by intermediation entities.[22]

---

19 Éva Gellérné Lukács, Az európai egészségügyi adattérről szóló rendelettervezet (Draft regulation on the European Health Data Space) (2024) (2) EU Jog 3, DOI: 10.55413/561.A2400201.EUO

20 Thomas Hoeren, Ulrich Sieber, Bernd Holznagel, *Handbuch Multimedia-Recht, Rechtsfragen des elektronischen Geschäftsverkehrs* (C.H. Beck 2024, München) Teil 16.8 Rn. 18, 19.

21 EHDS Article 2(2)(t).

22 EHDS Article 50(3).

2 Data users

The regulation does not contain any provisions regarding who can request data. In terms of the purposes of secondary use and the process of accessing data, it can be stated that data can be requested by anyone from the European Union or the EEA[23] who can ensure the conditions required by the regulation during data processing (data protection and security conditions) and uses the data for the purposes specified in the regulation. Based on the intended use of the data identified in the regulation, the main target audience of the EHDS includes economic actors interested in healthcare research, product and service development and treatment processes, as well as AI developers, public sector organisations and educational institutions. In other words, anyone from PhD researchers to researchers at large pharmaceutical companies, AI developers to universities, to Member States and EU decision-making bodies.

3 Health data access bodies

All Member States will designate one or more health data access bodies (HDAB) as governance and decision-making bodies responsible for secondary use in line with the EHDS mechanism. The HDABs assess requests for data, issue permits to the data users, and request that the data holders provide data to data users. The HDAB has authority and supervisory powers. The HDAB can be considered a kind of intermediary between the data holder and the data user.[24]

These designated authorities will play a significant role in the development of the single health data market, as the right to issue data permits remains within the competence of the Member States.[25] The development of a uniform decision-making practice based on objective criteria will decisively determine the efficiency of the single health data market and the trust of data subjects, data holders and data users, as per the EHDS data-sharing mechanism.

4 Operators of the secure processing environment (SPE)

The HDABs shall provide access to pseudonymised or anonymised personal electronic health data only through an SPE, which is subject to technical and organisational measures and security and interoperability requirements.[26] A SPE is a safeguard intended to preserve

[23] The EHDS will provide the opportunity for international organisations and third countries to access the HealthData@EU platform on the basis of Article 75, 10 years after the entry into force of the EHDS, on the basis of reciprocity. The international expansion of the EHDS is one of the longer-term objectives.

[24] Musidlowska.

[25] Mark Ryan, Paula Gürtler, Artur Bogucki, 'Will the real data sovereign please stand up? An EU policy response to sovereignty in data spaces' (2024) 32 International Journal of Law and Information Technology 25, DOI: doi.org/10.1093/ijlit/eaae006

[26] EHDS Article 73(1).

the rights and freedoms of natural persons and other persons who have certain rights related to the processing of their electronic health data.[27] The EHDS is not clear as to whether the HDAB must have an SPE or whether the data must be loaded into an SPE designated by the data user from the market. The requirements for the SPE will be included in an implementation act of the European Commission, where this should be clarified. If the data user must use an SPE provided by the HDAB, they may only use those technical tools during the processing of data that are available in that SPE, while in the case of an SPE chosen from the market, the data user has the option of using one with technical tools appropriate to their purposes. This interpretation of the EHDS would contribute to the revival of market competition among SPE operators, while the HDABs would not be burdened with the operation of the SPE.

5 Minimum categories of data

The scope of the regulation covers a wide range of health data. The regulation lists as a minimum category those data that are to be considered health data under the scope of the regulation. These data types go far beyond health data in the general sense. Health data is not only data related to the patient's condition, but also data generated in connection with the process of health care, the activities performed by professionals, data related to the distribution of financial resources and the expenditures of care institutions, social security data, social care data, personal data collected by IoTs or wellness applications and data generated by health devices.

With regard to data protected by intellectual property or trade secrets, the regulation requires that this must also be made available under appropriate contractual obligations. This means that the data holder cannot prohibit the release of data on the grounds that the data is part of intellectual property or a document protected by trade secrets.

The EHDS provides an opportunity for Member State regulation to allow natural persons, as data subjects, to exercise an opt-out right to the processing of their data for secondary use. Without this right, the data protection rights of data subjects would be significantly limited.[28] This option, however, greatly influences the usability of the data and, ultimately, the goals sought to be achieved through processing. The effectiveness of the mandatory sharing of personal health data and the achievement of the public interest objective it seeks to achieve, therefore, largely depend on the trust of the data subjects. The socio-cultural structure of the Member States, their ethical rules and the creation of social trust in data sharing will be decisive in the development of a single health data market.

[27] EHDS Recital 77.

[28] Taeger, Pohle Teil 12: 120.5 Rn. 30–33.

IV Purposes of the secondary use of health data – Objectives of the EHDS

The EHDS creates a right to data for secondary use only according to the purposes set out in the regulation. There are four main categories of purpose. The first is public purposes, namely decision-making, regulatory activities, public health surveillance, and compiling statistics. These purposes are reserved for public sector bodies. The second category is education and teaching activities. The third category is scientific research for development and innovation activities for products or services, as well as training, testing and evaluating AI algorithms, including, for example, medical devices. The fourth category is the improvement of healthcare delivery, the optimisation of treatment and the provision of healthcare.[29] All four categories serve one overarching goal: access to data for secondary use should contribute to the general interest of society.[30]

Unfortunately, the definition and scope of the *general interest of society* remain unclear. The secondary use of health data should benefit society by enabling the development of new medicines, medical devices and healthcare products and services at affordable and fair prices for Union citizens.[31] A data permit can only be issued if the purposes outlined in Article 53 are met – for example, scientific research. The definition of scientific research is quite broad, including innovation activities associated with products and services and training algorithms. These criteria are very general, and it would probably not be difficult to demonstrate an intention to meet them.[32] Without additional clarification, it will be difficult to distinguish between secondary use serving the general interest of society and profit-oriented secondary use, particularly in the case of scientific research.

V Administrative decisions concerning the secondary use of health data

1 Legal concept regarding electronic data

The EHDS introduces a new legal relationship in the European data market concerning health data. Horizontal regulations on the data economy of the EHDS involve adapting rules from contract law to prevent contractual imbalances and ensure data sharing by data

[29] EHDS Article 53.
[30] EHDS Recital 61.
[31] EHDS Recital 61.
[32] Maret Kruus, 'The Public Interest Requirement in the Secondary Use of Health Data in Scientific Research: The Examples of Estonia and Finland' (2023) 32 Juridica International 64, 72, DOI: https://doi.org/10.12697/JI.2023.32.06

holders.[33] Even when data is held by governmental institutions, horizontal legal acts presume a contractual relationship between the data holder and the data recipient or data user. The terms and conditions of contracts or agreements concerning data sharing between parties depend on the governing contract law, sector-specific rules and other mandatory regulations of the European Union.[34]

Electronic data is non-competing,[35] non-rivalrous,[36] and tradable,[37] and it has economic value within the data economy. Through copying, transmitting, or sharing, information of economic value can be reproduced without limit. An important element of the data economy is that products and services based on data, with added value, appear on the market through the use of raw digital data.[38] With the emergence of the data economy, data law as a new legal regime has arisen that does not abide by state law. It rather demands transnational legal institutions because the territory of the data economy is the territory of the digital world, not the physical one. The internet has made data borderless. The ubiquitous nature of digital data determines the legal regime governing the legal relationship between data holders and data users, which is established by the law chosen by the parties.

In most legal systems, data as the subject matter of a contract covering data sharing is difficult to bundle into traditional legal concepts that usually focus on trade in items that are either real property, goods, or intangible assets such as shares, intellectual property rights and licences.[39] The reason for this lies in the characteristics of digital data mentioned above. There is no common legal concept regarding electronic data in the European Union either. The European Union does not create legal institutions for data and does not establish sui generis law for data. Determining the terms and conditions for data shared between businesses, governmental institutions and individuals remains the responsibility of the parties; however, applicable binding regulations must be taken into account.

---

33 For example, Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act) OJ L2023/2854 or Regulation (EU) 2022/1925 of the European Parliament and of the Council of September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act) OJ L265.

34 For example, in the case of the Internet of Things, the rules of the Data Act must be taken into account.

35 Jiang Ye, 'Solution to the Dilemma of Data Factor Circulation and Transaction in the Context of Law-Based Business Enabling Environment' (2024) 12 China Legal Sci 29, 46.

36 Josef Drexl, 'Designing Competitive Markets for Industrial Data – Between Propertisation and Access' (Max Planck Institute for Innovation & Competition Research Paper Series, 2016) 28, 46.

37 Herbert Zech, 'Data as a Tradeable Commodity' in Alberto De Franceschi (ed), *European Contract Law and the Digital Single Market* (Cambridge University Press 2017) DOI: https://doi.org/10.1017/9781780685212.004; Bingwan Xiong, Jiangqiu Ge, Li Chen, Unpacking data: China's 'bundle of rights' approach to the commercialization of data (2023) 13 (2) International Data Privacy Law 104, DOI: https://doi.org/10.1093/idpl/ipad003

38 Jiang Ye 42–44, 49, 51.

39 The Principles for a Data Economy (Data Transactions and Data Rights) – American Law Institute and European Law Institute, as Adopted and Promulgated BY The American Law Institute on May 18, 2021 and The European Law Institute on September 1, 2021, 6.

The legal framework for the processing of personal data is coherent throughout the EU, as the protection of personal data is ensured as a fundamental right by the GDPR.[40] However, a comprehensive legal framework has not been implemented in the field of non-personal data, as there has been no EU regulatory requirement to uniformly define the legal nature of non-personal data as data that does not enjoy protection, thereby ensuring its free flow and breaking down legal barriers within the EU.[41]

Therefore, with regard to the system of secondary use of EHDS, the legal assessment of data (whether pseudonymised personal or anonymised or non-personal data), regardless of whether it is health data or not, *does not have a uniform dogmatic background*, which may result in differences in legal assessment between Member States. Therefore, the need for legal interoperability, ie the compatibility of the laws of the Member States,[42] also arises in order to ensure the predictability and legal certainty of the operation of data spaces.

2 Data permits and data requests are two types of administrative decisions

Regarding data sharing, the EHDS does not regulate specific contractual agreements between the data holder and the data user, except in cases where contractual agreements address data containing information protected by intellectual property rights or trade secrets.[43] The regulation establishes an administrative relationship between a designated public sector body, the HDAB and the data user. The HDAB is not necessarily the same entity as the data holder from which the data user seeks the dataset. If the HDAB and the data holder are the same entity, the HDAB does not act as a data holder. Within this legal framework, data holders and data users are not directly contractually linked with each other;[44] they do not have a direct legal relationship.

A data applicant may submit either a data access application for pseudonymised or anonymised data at the personal level or a data request for data in an anonymised statistical

[40] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) OJ L119, 4.5.2016.

[41] Anastasiya Kiseleva, Paul De Hert, 'Creating European health data space: obstacles in four key legal areas' (2021) 5 (1) European Pharmaceutical Law Review 28, DOI: https://doi.org/10.21552/eplr/2021/1/5

[42] Krisztina Davidovics, Réka Kovács, Péter András Gaál, 'Az egészségügyi adatok másodlagos használata az EU-ban: Az európai egészségügyi adattér rendelet kapcsán felmerülő jogi kihívások a TEHDAS közös fellépés eredményeinek tükrében' [Secondary use of health data in the EU: Exploring the legal challenges of the upcoming European Health Data Space Regulation in light of the findings of the TEHDAS project] (2024) 23 (Special Issue) Digitális Egészségügy 10, DOI: 10.53020/IME-2024-KSZ-101

[43] F. Casarosa, F. Gennari, 'Data Sharing in the Internet of Medical Things: Between the Data Act and the EHDS' (2025) 16 (Special Issue) European Journal of Risk 21, DOI: doi:10.1017/err.2025.18

[44] Manon Vanderhaeghe, 'Owning What You Make: Commercially Sensitive Information and Secondary Use of Electronic Health Data for Research Purposes in the EHDS' (EHDS Blogpost Series, 2024) <https://www.law.kuleuven.be/citip/blog/owning-what-you-make-commercially-sensitive-information-and-secondary-use-of-electronic-health-data-for-research-purposes-in-the-ehds/> accessed 1 December 2025.

format. In the first case, the data user is entitled to access the data specified in the data permit within an SPE operated by the HDAB or a third party. In the second case, the anonymised data in statistical format is transmitted directly to the data user.

Once the HDAB issues a data permit or approves the data request, the data holder is obligated to provide the dataset specified in the permit or the request to the HDAB or directly to the data user if the data holder is designated as a trusted health data holder.[45] Data holders do not have the right to object to the HDAB's decision. However, they may consult on the possibilities and technical requirements of data collection.

Within the legal framework of the EHDS, the issuance of a data permit or approval of a data request by the HDAB means that health data specified in the data access application or in the data request and held by entities subject to data-sharing obligations must be provided to the data user under the law of the HDAB of the given Member State in whose jurisdiction the data holder falls. Given that the application and the request are submitted by the applicant to a public sector body, which is obliged to provide access to the data through a specific procedure and on the basis of criteria specified in a regulation, it can therefore be stated that the request is a public law right of access to data.[46]

The EHDS does not regulate the relationship between the two types of decisions. The difference between the two decision methods is that, in the case of a data permit, personal or anonymised data is made available by the HDAB in an SPE, while in the case of a data request, the data is transferred in a statistical format. The regulation only defines the data permit as an administrative decision; it does not attach a definition to a data request. The decision-making process is not regulated either; during the assessment of a data application, the HDAB, taking into account the principles of risk- and data minimisation, may decide, after consultation with the data requester, to release data only in a statistical form instead of a data permit, treating the request as if it had been a data request, not a full application. The question then arises as to whether this constitutes a refusal, whether the data is transferred through a new procedure, or whether it is the result of a tacit agreement between the parties – the HDAB and the data user – within the same official procedure.

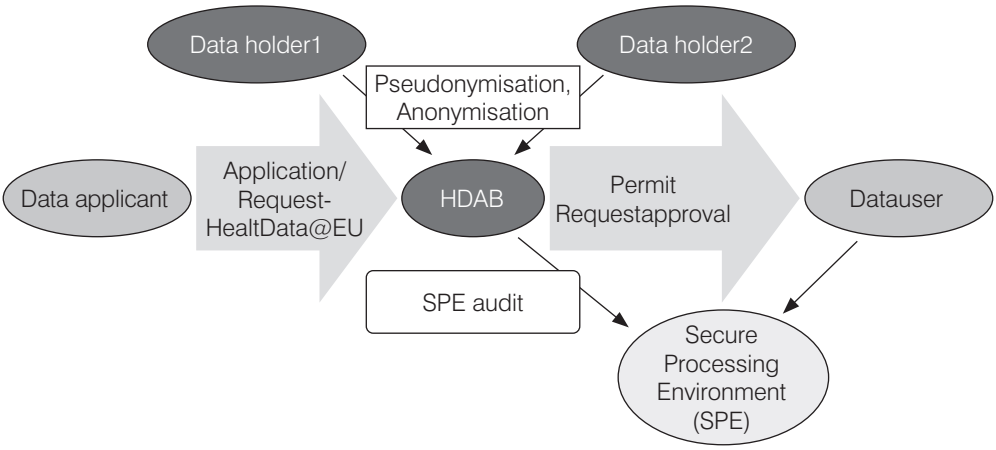
3 Process of data access

The process of applying for data access begins with the submission of a data access application form. The data applicant must complete and submit a form on an online platform to initiate the process. The applicant selects the datasets to which they wish to apply for access from the dataset catalogue. The applicant does not even specify the data holder, but the dataset.[47]

45 In a simplified procedure for access to health data from a trusted health data holder, the permit is issued by the HDAB on the proposal of the trusted data holder.

46 Hoeren, Sieber Teil 16.8 18.

47 Hoeren, Sieber Teil 16.8 24.



The HDAB's task is to contact the data holder.[48] The HDAB assesses the application and, if necessary, requests additional information from the applicant. The HDAB evaluates the application and request based on principles of data minimisation and purpose limitation. The HDAB ensures that access is granted only to data that is adequate, relevant and limited to what is necessary for the purpose outlined in the application.[49] If the application meets the regulatory requirements, the HDAB issues the data permit.

For a data permit, the HDAB fulfils its obligation by providing access to the data user in an SPE. The data user can only access and process the data through authorised natural persons approved by the HDAB and listed in the data permit. The SPE enables the HDAB to control and monitor the use of the data, meaning that every action performed by authorised individuals is logged and can be traced by the HDAB. The medium remains under the HDAB's control, preventing unauthorised copying or transfer of the original data from the SPE. Only non-personal electronic health data which do not contain any personal electronic health data should be downloaded by the health data users from such an SPE.[50]

In the case of an approved data request, the anonymised data in statistical format is transferred directly to the data user by the HDAB. This type of data is associated with a low risk of re-identification, so it does not require processing within a controlled environment. In this scenario, the HDAB transfers full control of the data to the data user. Furthermore, the data user is solely responsible for implementing the safeguards outlined in the data request to prevent any misuse of the data. Once transmitted, the data is entirely under the data user's control, allowing them to process, copy, modify, or transfer it.

[48] If the application concerns data located in multiple Member States, the HDAB will contact the HDAB of the relevant Member State via the HealthData@EU service in order to fulfil the data request (Article 75).

[49] EHDS Article 66(1).

[50] EHDS Recital 77.

One of the most significant obligations of data users in the EHDS mechanism is that they must publicly disclose the results or outputs of secondary data use, including information relevant to healthcare provision, within 18 months of completing the data processing. By publishing the results, the data user demonstrates that the use of digital health data according to the EHDS mechanism has fulfilled the purpose outlined in the data permit and has ultimately contributed to the benefit of European society.

The data access process is illustrated in the figure on page 130.

4 Enforcement

According to the EHDS, data holders are obliged to make their data available to the HDAB.[51] If a data holder withholds the requested health data from the HDAB or fails to meet the deadline, the HDAB will enforce compliance. In cases of non-compliance or delays, the HDAB may impose periodic penalty payments or exclude the data holder from the system.[52] Additionally, or as an alternative to these enforcement measures, the HDAB may impose administrative fines.[53] Ultimately, the secondary use of health data is a right of the data user and an obligation of the data holder. The goal of the EHDS is to ensure the availability of electronic health data held by any entity within the European Union with a high level of certainty while at the same time upholding private interests in data protection and data subject to intellectual property protection or confidentiality. To achieve this equilibrium between individual and collective interests,[54] EHDS treats data requests as official matters and applies coercive measures to ensure compliance in a centralised procedure subject to administrative control.[55]

51 EHDS Article 60(2).

52 EHDS Article 63 and 64. During the period of the exclusion, the data holder remains obliged to make their data accessible.

53 EHDS Article 64.

54 Valentina Colcelli, Roberto Cippitani, 'Circulation of Personal Data and Non-Personal Data within the European Research Area for Research and Health Purposes' (2023) 11 (2) Journal of Open Access to Law 17.

55 F. Casarosa and F. Gennari.

VI Data permits versus data contracts[56]

1 Data contracts

The EHDS applies to electronic health data held by both public and private sector bodies without hindering or replacing contractual arrangements or other existing mechanisms. The regulation does not affect access to electronic health data for secondary use as agreed upon within the framework of contractual or administrative decisions between public or private sector entities.[57] The EHDS will therefore not exclude or prohibit data users from obtaining electronic health data under other legal frameworks. Namely, the EHDS mechanism will not be the exclusive legal framework for sharing health data.[58] If, for example, concluding a data license agreement is burdensome for a data requester and its purposes of use are in line with the EHDS, the EHDS mechanism is an alternative solution.[59] Data users will have the opportunity to choose between the EHDS mechanism and other legal relationships to access electronic health data on the data market. They may apply for health data through the EHDS mechanism and enter into an administrative legal relationship with the HDAB, or they may enter into a contract with the data holder. The data requester must consider several aspects when choosing which path to take.

As mentioned above, the legal framework for data sharing in the data economy varies depending on which party's law is applied. In most legal systems, atypical contracts are concluded with regard to digital data, for which the method of analogy is applied. This approach is also reflected in the ALI-ELI Principles,[60] the jointly conducted project by the American Law Institute and the European Law Institute. The ALI-ELI Principles provide model agreements and provisions on the subject of digital data to be used voluntarily by parties. They are designed to promote the harmonisation of existing legal concepts in the data economy.[61] The principles facilitate the drafting of data contracts by providing default rules.[62] The ALI-ELI Principles distinguish nine types of contracts based on their subject

[56] The EHDS defines only the data permit as an administrative decision. Although the EHDS does not mention the data request among the definitions, it is also an administrative decision, given its regulation in the EHDS, which is based on the data permit rules. Hereinafter, a data permit should also be understood as a data request.

[57] EHDS Recital 52 and Article 1(8).

[58] EHDS Recital 52.

[59] Claudia Tessenow, Christian Teichter, Bernard Ziesche, Internet of Medical Things (IoMT): Was bedeuten Data Act und European Health Data Space (EHDS) im Kontext des Post-Market Clinical Follow-up (PMCF)? (2025) (55) Medicina Produkte Recht 64.

[60] The Principles for a Data Economy (Data Transactions and Data Rights).

[61] The scope of the ALI-ELI Principles covers all aspects of the value chain in the data economy. They provide different types of model data contracts, establish a legal framework for data rights, and include model rules for third-party aspects in the value chain.

[62] The Principles for a Data Economy (Data Transactions and Data Rights) Principle 1.

matter, including contracts for the transfer of data, contracts for simple access to data, contracts for the processing of data, and data trust contracts.

Within the EHDS mechanism, the HDAB provides data without any added value, such as analysis or other services. However, this does not mean that raw data is provided to the data user as it exists at the data holder. Only anonymised or pseudonymised data can be provided to the data user, along with anonymised data in statistical format. Furthermore, only data that meets the purpose defined by the data user and does not go beyond what is necessary to achieve this purpose may be made available to them. In order for these requirements to be met, the data holders or the HDAB must first sort, aggregate, anonymise, etc., the data. In this sense, the data is processed to a certain extent, but this does not mean added value in the classical sense, since this processing is carried out in order to comply with the requirements prescribed by the regulation. In other words, the information transmitted by the data must be extracted from the data by the data user through the data processing activity they perform (eg, analyses, AI training, construction of longitudinal patient health histories).

The EHDS is clear regarding the content of accessible data: the data user is not allowed to download the accessed data directly from the SPE. Only non-personal data, including anonymised statistical data, can be downloaded.[63]

According to Principle 7 of the ALI-ELI Principles, a contract for the transfer of data is a transaction in which the supplier[64] undertakes to put the recipient[65] in control of specific data by transferring it to a medium under the recipient's control or by delivering a medium on which the data is stored. According to Principle 8, a contract for simple access to data is one in which the supplier undertakes to provide the recipient with access to specific data on a medium controlled by the supplier, without transferring control. This includes contracts where the supplier allows the recipient to read the data and enables them to process or transfer data within the medium controlled by the supplier. The difference between the two types of contracts is in the characteristics of the service. In the case of data transfer, the usual elements of a sale contract are primarily present (eg transfer of control over data). In the case of providing access to data, the recipient does not receive the data itself, but only access to it. In most jurisdictions, the closest analogy would be a service contract, where the primary service is granting access to data. If the contract includes elements of downloading and transferring non-personal data or derived or inferred data, it may also resemble a contract of sale or lease. The greater the portion of data the recipient is allowed to transfer, the more the transaction resembles a contract for the transfer of data, making it closer in effect to a sales contract.[66]

63 EHDS Article 73(2).

64 Data holder, as defined in European Union terminology.

65 Data user, as defined in European Union terminology.

66 The Principles for a Data Economy (Data Transactions and Data Rights) Principle 8.

Compared to the EHDS mechanism, a data permit, according to its content, closely resembles a contract for simple access to data but contains elements of contracts for the transfer of data. However, with the approval of the data request, the data in statistical format will be transferred to the data user, which is similar to a contract for the transfer of data.

From a formal point of view, a data permit is significantly different from a data-sharing contract, as the data holder cannot choose the applicant or the entity submitting the data request, which could even be a direct competitor.[67]

2 Liability

In the EHDS mechanism, only the HDAB and the data user are in a direct legal relationship. However, *liability issues* may arise from different aspects beyond this relationship. A significant difference between a data contract and this administrative relationship is the lack of control power held by the data holder and the pivotal role of the HDAB.[68] In a contractual relationship, the data transaction typically involves only the data holder (as the supplier) and the data user (as the recipient). In a contract for access to data, only the data holder is liable for performance. In the EHDS mechanism, the applicant may consult the HDAB and, indirectly, the data holder or, directly, if the data holder is designated as a trusted data holder. The HDAB, along with relevant data holders, should assist applicants in selecting suitable datasets or data sources for their intended purpose.[69] Based on these provisions and interpretations, negotiations may occur between the three relevant parties. The HDAB should have the necessary expertise[70] to provide support, and if it does, it assumes full liability for ensuring that the dataset fits the applicant's purpose. Data holders are liable only for ensuring that the dataset conforms to the description provided in the dataset catalogue. In the network of legal relationships created by EHDS, the responsibility of data holders does not exist within the framework of the legal relationship established with the data user. The HDABs are responsible for monitoring and supervising the compliance of both data holders and data users with the regulation's requirements, including ensuring the conformity of datasets for secondary use and the compliance of the data permit by the data users. If they do not comply with the EHDS, they may be subject to administrative penalties.

Data users have the right to lodge a complaint with the HDAB if their rights or interests are negatively affected.[71] Under this provision, data users may also lodge complaints regarding dataset non-conformity. Since the data user can only submit his complaint to the HDAB, it is the obligation of HDAB to have the data holder correct the incorrect or incomplete

67 Vanderhaeghe.
68 Vanderhaeghe.
69 EHDS Recital 73.
70 EHDS Article 55(2)(b).
71 EHDS Article 81(1).

dataset. In other words, HDAB is responsible to the data user to fulfil the data user's warranty claims. To this end, the EHDS provides administrative enforcement tools to the HDAB as mentioned above. However, the EHDS does not explicitly contain these rules regarding the data user's warranty claims, but an administrative supervision and control system ensures the fulfilment of the data user's claims in the event that the data holder (or the HDAB) does not fulfil its obligations specified in the EHDS.

The regulation only provides brief guidelines on the complaint process and decision. The HDAB informs the data user about the progress of proceedings and the final decision, but no further procedural details are outlined. It is unclear where the burden of proof lies. Since the issuance of a data permit involves an administrative decision, complaints regarding its content must also be resolved through administrative procedures, which vary by Member State law. If rectification is required, the process is unclear, raising concerns about how non-conformity or performance deficiencies will be resolved by the HDAB or the data holder.

This way, the liability is shared by the data holders, data users and the HDAB. The impact of this shared responsibility on potential non-compliance remains to be seen. However, it can already be stated that the balance of power between the parties is not equal, as the HDAB appointed by the Member States has the most decision-making power.[72]

Without uniform, standardised criteria, the assessment on which the HDAB bases its decision may lead to different results in different Member States. In order to create a single European data market, it is absolutely necessary to create uniform legal, theoretical and political criteria on which the HDABs can base their decisions. Since HDABs are public bodies, the political dependence of HDABs on the current governments of the Member States may also arise.[73]

Liability issues may be more complicated if the HDAB assessing the application also makes a decision on the access to data of data holders from other Member States, particularly if the data application concerns data falling under the jurisdiction of several states.

3 Operator of the SPE

The HDAB provides access to data in an SPE, allowing it to control access and monitor data usage by the data user. Within this controlled environment, the HDAB or the data holder retains full control over data access at all times.[74] The SPE may be operated by the HDAB, the data holder, or an independent service provider. The HDAB has the authority to monitor and regulate data usage by the data user for up to 10 years.[75] Over this period, the HDAB, the data user and the SPE provider will hold rights and have obligations towards each other.

[72] Ryan, Gürtler 26.
[73] Musidlowska.
[74] EHDS Recital 77.
[75] The duration may be extended once in a period which does not exceed 10 years – EHDS Article 68(12).

However, the exact nature of these legal relationships is not yet well-defined. An independent provider is likely not subject to the data permit, but the HDAB can only fulfil its role if it has full access to the data and its associated logs. The data user may designate the SPE, making them responsible for concluding a contract with the service provider, paying the associated processing fees and ensuring the HDAB retains control over data access through contractual provisions. The outline of this agreement will remain subject to negotiation by the parties, as the EHDS does not provide further provisions.

4 The other route

The EHDS will provide one option for health data access in the European Union, but only for public interest purposes. For commercial purposes, such as marketing, data users may still enter into contracts with any data holder. For example, if a data user intends to increase the sales of a healthcare product and requires in-depth analysis to make marketing decisions, they may negotiate and conclude data contracts with health data holders to obtain digital health data. If the HDAB rejects an application, the data applicant still has the option to rely on freedom of contract and procure digital data from the data economy. In this case, however, the data user's right to access the data can only arise based on the joint contractual will of the parties.

VII Potential impacts of mandatory data sharing

1 Public control over health data held by private data holders

Mandatory data sharing raises legal concerns for private data holders. The scope of the EHDS covers the electronic health data categories set out in Article 51, held by data holders as defined in Article 2(2)(t), with exemptions provided in Article 50 for natural persons and microenterprises. Among others, data holders include all legal persons developing products or services intended for the health, healthcare, or care sectors, as well as those developing or manufacturing wellness applications. Private sector data holders are obligated to share their data under an administrative decision enforceable by the authorities of the Member States. Moreover, even based on a decision by an authority of another Member State, if the data application concerns data falling under the jurisdiction of several states.

If data are considered resources in the data economy, enforced sharing by public authorities means that health data holders' control and sovereignty over the data they produce, collect, and use for analysis and predictions will be restricted. It will no longer be the data holders' decision whether to keep their data or share it with other market players. The question arises as to whether forced data sharing enhances the competitiveness of the European Union more effectively than voluntary data sharing by the private sector.

According to the data strategy, the general principle should be to facilitate voluntary data sharing, and only in specific circumstances should access to data be made compulsory in sector-specific cases. This should occur only if a market failure is identified or can be foreseen, which competition law cannot resolve. Furthermore, the legitimate interests of data holders should be taken into account.[76] However, without regulation, private data markets prevent the full realisation of the social value of data.[77] Considering this, the circumstances of the healthcare sector in the European Union justify mandatory data sharing in the field of health. However, the rationale underpinning mandatory data sharing in the EHDS is not clearly specified in its preamble.

The fact that the data holder cannot choose the partner with whom it would share its data, nor the conditions and price according to which it would do this, is difficult to reconcile with the interests of economic operators.[78] Mandatory data sharing at a price fixed by authorities may erode willingness to invest in data collection and could lead to a negative response in terms of data supply.

2 The price of digital data

In an ideal situation, parties mutually agree on the price of data. In contract law, the parties have the right to negotiate and settle the price. However, due to the information paradox, the value of the information contained in the data is not known to the data user until they have access to it. If a particular item of information is of different value to economic agents, this asymmetry leads to both a non-optimal purchase of information at a given price and a non-optimal allocation of the acquired information.[79] This information paradox makes it difficult to agree on the price of data access during contractual negotiations.[80] Furthermore, a consensus-based price is only possible if there is no significant disparity in bargaining power between the parties in the data economy. SMEs are undeniably in a weaker position compared to big tech companies. In other words, the value of data shared on a contractual basis is influenced by several factors, which make it impossible to determine a 'single price' for the data.

Under the EHDS mechanism, the price of data is essentially the cost of making health data available for secondary use. This includes all or part of the cost associated with assessing the application, preparing and anonymising or pseudonymizing the data. The fees for data access and the processing of the data permit are non-negotiable between the parties, with one exception: the data user is required to pay the portion of fees related to the data holder's costs

[76] European strategy for data 13.

[77] Martens 2.

[78] Musidlowska.

[79] Kenneth Arrow, *Economic Welfare and the Allocation of Resources for Invention in The Rate and Direction of Inventive Activity: Economic and Social Factors* (Princeton University Press 1962, Princeton, NJ) 615.

[80] Josef Drexl, 68.

directly to the data holder. If the data holder and the data user fail to agree on the size of the fee, the HDAB may set the fee in proportion to the actual cost of making the data available. In the event of a dispute, both parties may seek resolution through a dispute settlement body established under the Data Act.[81] This rule partially overrides the administrative nature of the EHDS mechanism, allowing a limited negotiation of data access pricing. However, even in such cases, price negotiations remain restricted to marginal costs, meaning that this does not constitute a 'real' consideration freely negotiated by the parties. Furthermore, the data holders transfer the data collected and processed by them without receiving any benefits. The EHDS remuneration system is not suitable for balancing economic interests, thus completely ignoring the value of the data.[82] This may affect the interest of data holders regarding making the necessary investments to improve data quality, as they cannot expect to make a profit from utilising the data that is available as a resource.

3 Data availability

According to the EHDS, the HDAB must evaluate data applications based on the principle that the data requested is adequate, relevant, and limited to what is necessary for the stated purpose in the application. This principle is known as data minimisation.[83] Depending on how the HDABs interpret this principle, data minimisation may affect the market volume covered by data contracts. If data minimization is interpreted broadly and HDABs do not require disproportionate proof that the purpose of the data use can be achieved with less data, the value of data settled in data contracts may decrease, yet obtaining data through the EHDS mechanism may become a more attractive option for data users due to its ease and high certainty of access, legal certainty and low fees. Thus, the uptake of data access through the EHDS mechanism may be large compared to data access through contracts. For actors with less bargaining power (SMEs, start-ups, individual researchers, etc.), the EHDS may be a real solution. It will democratise data access, as opposed to data concentration, where data accumulates in large companies that can afford it.[84] However, in a narrower interpretation, data acquisition from the market through a data sharing agreement remains an option, because it may be easier for data users to obtain data on the data market, as there is no need to enforce the principle of data minimisation or prove that larger amounts of data carrying more information are needed. At the same time, the unequal market power of smaller players will persist, especially compared to that of large online platforms,[85] which the EHDS aims to reduce.

[81] EHDS Article 62(4).
[82] Tessenow, Teichter, Ziesche 65.
[83] EHDS Article 66(1).
[84] Gellérné 16.
[85] Taeger, Pohle Teil 12: 120.5 Rn. 10, 11.

4 The value of datasets

Data holders are required to provide a description of their data, which must be reviewed annually to ensure that the dataset description in the national dataset catalogue is accurate and up-to-date. The description should be provided in the form of metadata, and each dataset must include information regarding its source, scope, main characteristics, and the nature of the health data contained within it.[86]

The regulation establishes a framework for data quality. Datasets may be denoted by a Union data quality and utility label,[87] which is applied by data holders. The data quality and utility label describe the dataset's quality and usage conditions in the form of a graphic, including a rating scale.[88] Through self-assessment by data holders, this quality framework assists data applicants in identifying appropriate datasets for their purposes as specified in their data access applications. These standardised elements provide an overall picture of a dataset. The standardised elements and labels at the European level help *mitigate the risk of information asymmetry* for data users. Moreover, having a standardised data quality system may contribute to a common assessment of dataset value, potentially leading to the establishment of a measurable valuation for digital datasets as assets.

The HealthData@EU platform will serve as a 'pool' of dataset catalogues, likely providing a comprehensive map of existing health datasets within the European Union. These dataset catalogues will not only serve as a starting point for launching data applications within the EHDS mechanism, but they will also offer a detailed repository with comprehensive metadata and all necessary information about the data holder. This transparent landscape of digital health datasets in the whole European Union may have a significant impact on the data economy and could act as a catalyst for parallel mechanisms, such as helping data users identify suitable datasets and data holders without incurring additional costs.

VIII Summary

The EHDS introduces a range of new terminology, processes and relationships. In seeking to balance data protection with the growing demand for data sharing in the data economy, it establishes a mandatory data-sharing mechanism with detailed and strict safeguards to protect personal health data. The EHDS represents a significant intervention in the relationships between parties in the data economy, aiming to address market failures. The European Union

86 EHDS Article 77(1).

87 Except for datasets collected and processed with the support of Union or national public funding – EHDS Article 78(2).

88 EHDS Article 2(2)(z) and 2(2)(aa).

legislator has recognised that granting access to data without additional conditions imposed by data holders is only achievable through a mandatory administrative process.

This article aims to present the legal characteristics of data in relation to the EHDS mechanism, as the fundamental elements of the health data space being built, in comparison with market practices commonly found in the data economy. It also analyses the role, responsibility and advocacy ability of the actors within the EHDS mechanism.

The EHDS obliges not only public sector data holders, but also private data holders to share their health data, which represents a form of public control over privately held health data. Through making digital health data held by the private sector publicly available, the European Union integrates all digital health data into a single health data market. The EHDS justifies this intervention in the data economy by asserting that private-sector data should be accessible only when it serves the general interest of society. However, the content of general interest to society remains unclear.

The EHDS does not encourage but rather obliges data sharing, thereby deeply interfering with previously negotiated data sharing agreements between actors in the health data market through official means. At the same time, regarding the rules governing the legal relationship between data holders, the HDAB, data users and SPE operators, the regulation does not provide sufficient answers to questions that could be resolved through data contracts. Such problematic points are the issue of liability between the actors, liability for warranty and the lack of legal regulation of data as a resource for data producers.

Perhaps one of the biggest positive impacts of the EHDS is the creation of an EU-wide map of datasets, which, based on standardised assessments, will enable data users to obtain cost-effective and reliable insight into the health data market.

The other major outcome is expected to be that access to data will promote data sharing across the European Union to such an extent that economic operators can gain significant experience, develop good practices, and develop secure data sharing practices.

In summary, the legal nature of digital data and the absence of a uniform legal assessment create uncertainty in data flows. The mandatory data-sharing regime introduced by the EHDS, with its administrative legal character, may add to this uncertainty by introducing a new type of legal relationship into the European Union. The EHDS demonstrates that establishing a uniform EU legal framework for digital data, as both an object of circulation and a key component of the data economy, appears essential for the harmonised functioning of the EU data economy.