Computer Law & Security Review 54 (2024) 105993

Contents lists available at ScienceDirect

Computer Law & Security Review: The International Journal of Technology Law and Practice

journal homepage: www.elsevier.com/locate/clsr

Will the GDPR Restrain Health Data Access Bodies Under the European Health Data Space (EHDS)?

Paul Quinn *, Erika Ellyne, Cong Yao

Health & Ageing Law Lab (HALL), Law, Science, Technology & Society Research Group (LSTS), Faculty of Law and Criminology, Vrije Universiteit Brussel, Pleinlaan 2, 1050 Elsene, Brussels, Belgium

ARTICLE INFO

Keywords:
European health data space
General data protection regulation
Health data access bodies
Health data access permit
Secondary use of health data

ABSTRACT

The plans for a European Health Data Space (EHDS) envisage an ambitious and radical platform that will inter alia make the sharing of secondary health data easier. It will encourage the systematic sharing of health data and provide a legal framework for it to be shared by Health Data Access Bodies (HDABs) based in each of the Member States. Whilst this promises to bring about major benefits for research and innovation, it also raises serious questions given the intrinsic sensitivity of health data. Fears concerning privacy harms on the individual level and detrimental effects on the societal level have been raised. This article discusses two of the main protective pillars designed to allay such concerns. The first is that the proposal clearly outlines several contexts for which a Health Data Access Permit (HDAP) should and should not be granted. The second is that a request for an HDAP must also be compliant with the GDPR (inter alia requiring a valid legal basis and respecting data processing principles such as 'minimization' and 'storage limitation'). As this article discusses, in some instances the need to have a valid legal basis under the GDPR may make it difficult to obtain a data access permit, in particular for some of the commercially orientated grounds outlined within the EHDS proposal. A further important issue concerns the ability of HDABs to analyse the compatibility permit requests under the GDPR and relevant national law at both speed and scale.

1. Introduction

This article looks at the wide discretion granted to Health Data Access Bodies (HDABs) under the proposal for Establishing a European Health Data Space (EHDS).[1] These bodies will have the role of assembling electronic health data from various sources and then allowing third parties to process such data for a range of aims (including but not limited to scientific research). Given that it is expected that consent will not be required (though the potential for an 'opt out' mechanism remains possible) for the involvement of personal data, the creation of the EHDS and the role of HDABs has raised significant concerns amongst some concerning potential privacy harms to individuals and other detrimental effects on the societal level.[2]

The EHDS foresees two primary protective pillars which are designed to allay such concerns. Taken together it is hoped that these pillars will reduce the risk of harm both at the individual and societal level. The first is the wide-ranging discretion granted to the HDABs to grant a data access permit together with a set of principles that outline when such a permit should and should not be granted. In doing so the drafters of the EHDS regulation have seemingly attempted to force HDABs to take into

Abbreviations: EDIB, European Data Innovation Board; EHDS, European Health Data Space; EHR, Electronic Health Record; GDPR, General Data Protection Regulation; HDAB, Health Data Access Body; HDAP, Health Data Access Permit; IVDR, In Vitro Diagnostics Regulation; MDR, Medical Device Regulation.

* Corresponding author.
E-mail address: Paul.Quinn@vub.be (P. Quinn).

[1] European Commission, Proposal for a regulation - The European Health Data Space COM (2022) 197/2 https://health.ec.europa.eu/publications/proposal-regulation-european-health-data-space_en accessed 17 Apr 2023 ('EHDS proposal'). For the avoidance of doubt, all 'EHDS proposal' mentioned in this article refers to this version.

[2] In the original proposal of the EHDS no form of consent was foreseen. During the pier review process of this article it became common knowledge that the institutions had agreed on a form of 'opt-out consent' for participation of one's data in the EHDS. This was evidenced in a document widely leaked with the reference "Interinstitutional File: 2022/0140(COD)". It outlined an agreement to allow forms of 'opt out consent' for both primary and secondary data processing. This indicates a shift in direction to a similar strategy to that used by the UK's NHS for allowing secondary data processing for research. See: https://digital.nhs.uk/services/national-data-opt-out

https://doi.org/10.1016/j.clsr.2024.105993

Available online 2 July 2024

account key requirements in terms of both the benefits and harms to individuals and society. The second is a requirement that in order for a data access permit to be granted the envisaged processing must be compliant with the General Data Protection Regulation (GDPR).[3] This includes *inter alia* the existence of a valid legal basis and the need to follow data processing principles such as 'data minimization' and 'storage limitation'. In doing so the EHDS will rely on the comprehensive framework outlined in the GDPR to guarantee the correctness of any processing from a data protection point of view.

This article will explore these two key pillars guarding against incorrect reuse of secondary data through the EHDS. In particular, it will seek to discern, how they are likely to interact, what protection they truly offer and what other problems they may create. Following an exploration of the main elements that form the EHDS (Section 2) the authors of this article will explore the grounds for which HDABs may grant a data access permit. The reasons provided within the EHDS framework are often not clear and will likely create a wide discretion for data access bodies that may serve to create unpredictability and variability across various European Member States. The same is true for the grounds provided in Article 34 for situations where a data access permit should not be granted (discussed in Section 4). Once again, a number of these grounds are very broad, meaning that HDABs will also receive a broad discretion to refuse to grant data access permits for a range of reasons. As the authors of this paper further discuss, this gives rise to concerns surrounding the non-granting of data access permits that have hitherto not received much discussion. In Section 5, the reliability of the GDPR as a 'backstop' will be further discussed. The need for data recipients to possess a legal basis will pose an important additional requirement, that may, in a number of circumstances, be difficult to meet, even in instances where Article 34 of the EHDS might seem to indicate that a data access permit should be granted. Furthermore, as the authors of this paper will further discuss, there exist serious doubts about the capacity of HDABs to properly scrutinize requests given the diverse legal backgrounds of the various Member States, the inherent complexity involved in many forms of health data processing and the serious resources that will be required to do so.

2. The aims of the European health data space

2.1. The European Data Strategy and the European Commission's ambition

The European Commission has the ambition to make Europe a "Data-driven society" by creating a genuine single market for data. As part of the European data Strategy, it has decided to create a number of data spaces in key economic sectors and public domains.[4] It is hoped that cooperation in these sectors will improve data pooling and sharing. According to the Commission, the idea is supported by three main pillars. They are :[5]

(i) *deploy data-sharing tools and services for the pooling, processing and sharing of data by an open number of organisations, as well as federate energy-efficient and trustworthy cloud capacities and related services;*

(ii) *include data governance structures, compatible with relevant EU legislation, which determine, in a transparent and fair way, the rights concerning access to and processing of the data;*

(iii) *improve the availability, quality and interoperability of data – both in domain-specific settings and across sectors.*

It is intended that new architectural designs will make it easier for these spaces to promote data sharing where there is an economical, social, or scientific justification. Such architectures will be regulated by governance frameworks that the EU will outline in forthcoming legislative acts.[6] The aim behind the ambition is to improve the overall level of data sharing, which has thus far not been accomplished due to a range of legal and technological obstacles combined with a general unwillingness to share data.

Accordingly, the EU will implement four broad sets of measures for data-sharing systems,[7] including reusing specific categories of data held by public sector bodies,[8] developing data intermediation services,[9] creating and encouraging the role of data altruism[10] for the public interest, and establishing the European Data Innovation Board (EDIB) for best data sharing practice across the EU.[11] It seeks to provide businesses, public administrations and individuals in Europe with a reliable and safe environment for data sharing and exchange. In this way, these data spaces will enhance the innovative activities of data-driven products and services through the Single Market in the EU and support a competitive and integrated European data economy.[12]

2.2. EHDS as part of the EU data strategy

The Commission's first in-depth proposal for a data space was for the European Health Data Space. It corresponds to the EU's Data Strategy, encompassing the Data Governance Act and the proposed Data Act.[13] It is designed to improve and complement existing EU regulations, such as the General Data Protection Regulation (GDPR), Medical Device Regulation (MDR),[14] and the In Vitro Diagnostics

[3] 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) [2016] OJ L119/1 ('GDPR').

[4] European Commission, A European Strategy for Data (Communication) COM (2020) final < https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0066 accessed 17th Apr 2023.

[5] European Commission, Staff working document on data spaces https://digital-strategy.ec.europa.eu/en/library/staff-working-document-data-space accessed 17th Apr 2023.

[6] 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 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32022R0868. ('Data Governance Act') accessed 17th Apr 2023. The Data Governance Act provided a legal infrastructure for designing and managing data spaces at the EU level.

[7] European Commission, Data Governance Act Explained https://digital-strategy.ec.europa.eu/en/policies/data-governance-act-explained accessed 17th January 2023.

[8] Data Governance Act, Chapter *II*.

[9] Data Governance Act, Chapter *III*.

[10] Data Governance Act, Chapter *IV*. Data altruism is the concept of individuals and companies voluntarily giving their consent or permission to make their data available in the use of public interest.

[11] Data Governance Act, Chapter *VI*.

[12] European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, A European Strategy for Data < https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0066> COM(2020) 66 final, accessed 17 Apr 2023.

[13] Proposal for a regulation of the European Parliament and of the Council on Harmonised Rules on Fair Access to and Use of Data (Data Act) COM (2022) 68 final https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2022%3A68%3AFIN.

[14] Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC (Medical Device Regulation) [2017] OJ L117/1 ('MDR').

Regulation (IVDR).[15] However, while these regulations provide general and horizontal provisions, the EHDS is focused solely on the health and care sectors.[16]

At the sectoral level, the EHDS proposal is the result of several trends in the health sector that emerged around the same time.[17] *First*, it was recognised that fragmented implementations of the GDPR hampered cross-border health care in the EU. The GDPR not only provides a solid framework for data protection in the EU but allows Member States to introduce further specifications to adapt the Regulation in national law, particularly in the area of health.[18] The varying interpretation and implementation of the GDPR has resulted in an unnecessarily fragmented landscape in the EU, which raised concerns about the interoperability and standardisation of data, in particular health data.[19] The uneven legal landscape surrounding the use of health data also created significant legal uncertainties, resulting in barriers and additional costs for digital health product manufacturers and health service providers to enter other Member States' markets.[20] As a result, there is a need to improve easy access and exchange of health data and hence, improve the quality and delivery of health care in the EU and the innovations of the various technologies and practices that it requires.

Second, it became increasingly clear that structural problems prevent multiple users from benefiting from the use of electronic health data. The interpretation of the law is complex at the national level, and it is not always easy for patients to exercise their rights (as granted by the GDPR), including accessing and sharing them on a national and EU level.[21] Also, natural persons cannot benefit from innovative treatments due to processing barriers in health data. Accessing the necessary data for better healthcare products and services is challenging for researchers, innovators, regulators, and policymakers.[22] They face significant barriers in accessing health and patient information due to the inadequate data sharing infrastructure and the restrictive regulatory framework.[23] This also hampers innovative healthcare activities in the EU and the EU's ability to respond to health emergencies.[24]

Third, the COVID-19 pandemic demonstrated the value and possibility of interoperability of health data systems at the Union level.[25] The lack of accessible, comprehensive, and integrated patient-level data has been identified as a critical barrier to COVID-19 research.[26] The pandemic showed the urgent need to ensure rapid and secure access to health data to better prepare for future health crises, including improved information sharing and research at the EU level and enhanced cooperation among Member States for greater healthcare integration.[27] However, scholars have argued that the lack of a common framework for the use and re-use of electronic health data has posed key barriers to COVID-19 scientific research.[28] Therefore, the secondary use of health data has rightfully become a policy priority. The COVID certificate served as an inspiration, demonstrating Europe's ability to provide innovative solutions and transform them into unrivalled international standards.[29] As a result, the European Commission has committed to establishing a European 'Health Union'.

2.3. The core ambitions of the EHDS

The EHDS initiative is primarily proposed as an extension and improvement of the GDPR in terms of its application to health data.[30] In response to the above-mentioned barriers and challenges, it seeks to complement the rights provided by the GDPR to achieve its objectives more effectively. The proposal consists of 76 articles organised around two main pillars. The first pillar (Article 1–32) addresses issues related to the primary use of health data. It seeks to facilitate the re-use of health data by consumers, provide portability[31] between health service providers in support of second opinions, and increase competition between service providers.[32] The proposal introduced a series of rules for the primary use of health data, such as the design and development of electronic health registers,[33] the interoperability of electronic health record systems across the EU, and wellness application rules.[34] The second pillar (Article 33–58) established the legal framework for the EU's secondary use of health data. The secondary use of electronic health data is linked to various themes and purposes. This includes traditional notions of scientific research[35] as well as its application to the innovation of new products or services related to "public health or social security or ensuring high levels of quality and safety of health care, or medical products or devices."[36] Other permitted areas will include

[15] Regulation (EU) 2017/746 of the European Parliament and of the Council of 5 April 2017 on in vitro diagnostic medical devices and repealing Directive 98/79/EC and Commission Decision 2010/227/EU (In Vitro Diagnostics Regulation) [2017] OJ L117/176 ('IVDR').

[16] EHDS proposal, at 3.

[17] J Scott Marcus and others, 'The European Health Data Space' [2022] SSRN Electronic Journal https://www.ssrn.com/abstract=4300393 accessed 27 January 2023.

[18] GDPR, Article 9 (4).

[19] Hansen, J, Wilson, P, Verhoeven, E, Kroneman, M, Kirwan, M, Verheij, R & van Veen, '*Assessment of the EU Member States' rules on health data in the light of GDPR*' (2021) European Union, Luxembourg. https://doi.org/10.2818/546193. 5/17/2024 11:01:00 PM

[20] EHDS proposal, at 1.

[21] Ibid. See also Hansen and others (n 18). 9-10.

[22] Jakov Vukovic and others, 'Enablers and Barriers to the Secondary Use of Health Data in Europe: General Data Protection Regulation Perspective' (2022) 80 Archives of Public Health 115.

[23] Jasper Bovenberg and others, 'How to Fix the GDPR's Frustration of Global Biomedical Research' (2020) 370 Science 40.

[24] EHDS proposal, at 1. See also Marcus, J.S. et al., 2022, (n 16), at 10.

[25] Ibid.

[26] Stuart McLennan, Leo Anthony Celi and Alena Buyx, 'COVID-19: Putting the General Data Protection Regulation to the Test' (2020) 6 JMIR Public Health and Surveillance e19279.

[27] Evelina Tacconelli and others, 'Challenges of Data Sharing in European Covid-19 Projects: A Learning Opportunity for Advancing Pandemic Preparedness and Response' (2022) 21 The Lancet Regional Health - Europe 100467.

[28] Ibid, see also Stuart McLennan and others, 'Practices and Attitudes of Bavarian Stakeholders Regarding the Secondary Use of Health Data for Research Purposes During the COVID-19 Pandemic: Qualitative Interview Study' (2022) 24 Journal of Medical Internet Research e38754.

[29] European Commission, EU Digital COVID Certificate https://commission.europa.eu/strategy-and-policy/coronavirus-response/safe-covid-19-vaccines-europeans/eu-digital-covid-certificate_en accessed 22nd September 2023.

[30] EHDS, at 3 and 7. See also in Recital 11, the EHDS goes beyond Article 20 GDPR with the respect to portability of personal data.

[31] Under Article 20 GDPR, the data subject "... shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided ..." The right to data portability is in principle already in place, but the GDPR does not clarify how to apply it to health data.

[32] Marcus and others (n 16).

[33] EHDS proposal, Article 7.

[34] EHDS proposal, Chapter *III*.

[35] EHDS proposal, Article 34 (1)(e).

[36] EHDS proposal, Article 34(1)(f). Article 34 (1)(g) also permits the reuse of secondary data for training AI algorithms for similar purposes.

dealing with public health threats,[37] improving healthcare delivery and related services, and education and training-related activities.[38]

The proposal thus has multiple ambitions—for individuals, physicians, and for research.[39] It aims to (a) strengthen patient control over their data; (b) establish rules for electronic health records (EHR) systems to promote reliability, security and interoperability; (c) establish rules for the secondary use of health data; and (d) establish mandatory cross-border infrastructures.[40] In line with the main focus of this article, the following sections will focus on the rules the EHDS lays down for the secondary use of health data. A fuller explanation of the other goals of the EHDS is beyond the scope of this article.

3. The EHDS will facilitate a broad range of secondary purposes

As discussed in Section 2, the facilitation of the re-use of health data is a major pillar of the EHDS proposal. As the following section will discuss, Article 34 of the proposed regulation lays out a number of very broadly worded contexts for which data permits will be granted for secondary use. Whilst the proposal identifies 'scientific research' as a valid reason for granting a permit,[41] a quick look at Chapter IV of the proposal shows that the scope of envisaged purposes for secondary sharing goes far beyond what would ordinarily be considered as 'scientific research', encompassing the management of public services and innovation in a variety of industries that are linked to the health or social care sector.[42] The EHDS sees the following contexts as being suitable for the granting of a data permit:

3.1. For reasons of public interest in the area of public and occupational health (Article 34(a))

The EHDS will allow electronic health data to be shared in order to improve public and occupational health where such sharing would be in the public interest under Article 34.1(a).[43] The intention seems to be to provide data to public authorities so that they can detect and monitor threats to human health. A number of key areas where a data permit may be granted are outlined, including;

- Where such use is intended *inter alia* to allow public health officials to plan responses to public health threats such as epidemics of transmissible disease or other chronic health problems that are prevalent in society (of both a national and an international nature).
- To allow public authorities to monitor the safety of healthcare and of medicinal products or medical devices.

The above however appear to be only intended as indicative suggestions and given that they are prefaced by the phrase "such as", do not appear to be exhaustive in nature. It appears therefore that a more general possibility to grant data licenses for public health related purposes exists. This is remarkably similar to the legal basis that exists under Article 9(2)(i) of the GDPR for the processing of sensitive data (including health data).[44] The authors of this paper would argue that this similarity indicates that the intention behind the drafters of the GDPR is to ensure that where potential data controllers possess a legal basis under Article 9 of the regulation, they would be able to obtain a data permit under the EHDS to obtain the data they required for secondary processing.

Perhaps concerningly, Article 34 of the EHDS proposal does not itself specify precisely who can receive data (preferring to describe the purpose instead). In the case of processing for occupational health, this may give rise to some concerns given the wide range of commercial entities that could claim to be interested in such matters and who may claim to be acting under the guises of public health concerns. Such concerns may be greater where national legislation permits a wide range of commercial entities to make use of the public health exception foreseen under the GDPR.[45] The authors of this paper would argue that due attention needs to be drawn to the risk that such open provisions could be subject to abuse where the purpose of 'improving occupational health' is used as cover to obtain access to electronic health data. This and other difficulties will be discussed in further depth in Section 5 given that one of the most important protections against improper use will be found in ensuring that the GDPR and relevant national law relating to the use of Article 9(2)(i) is followed correctly.

3.2. To support public sector bodies in the health or care sector (Article 34 (b))

Chapter IV states that data should be made available where it can allow public bodies in the health or care sector to carry out their 'mandates' better.[46] It seemingly permits any public body that can be linked to those sectors to access electronic health data for secondary use if it can make the case that such access would allow it to carry out its functions better. Two factors make this a potentially wide-ranging possibility to grant data licenses;

First, the concept of 'public bodies in the health or social sector' itself is extremely wide. A number of factors contribute to this. Notably, the concept of public bodies is seen as including not only entities at the national but also the EU level. The purposes for which such entities use the data they receive are also not defined, the sole restriction being that they use it in line with their "mandates" and that the public bodies in question be in the "health or social sector". Given the enormous range of public bodies that exist within the health and social sectors and the tasks they carry out, the EHDS proposal entails making electronic health data available for a range of purposes that are very difficult, if not impossible to define. Most strikingly the terms' health sector' or 'social sector' are not defined in the early texts of the EHDS proposal. The drafters appear therefore to leave the discretion in determining which entities are in the health and social sector to the discretion of the Health Data Access Bodies. They will presumably be guided by how such bodies are recognized under national law according to their 'mandates'.

Second, the notion of what a 'mandate' is, is also not defined or restricted. It seems that a mandate may be for anything so long as it is somehow connected to the health and social care sector. Not only do the types of entities in these sectors vary enormously, but so too will the functions they carry out. Certain activities may be classified as healthcare in one Member state but not in another.[47] The same is true for the

[37] Article 34 (1)(a) for example permits reuse for "activities for reasons of public interest in the area of public and occupational health, such as protection against serious cross-border threats to health, public health surveillance or ensuring high levels of quality and safety of healthcare and of medicinal products or medical devices.

[38] EHDS proposal, Article 34 (1) (d).

[39] N Schutte and others, 'How Can Population Health Research Benefit from a European Health Data Infrastructure?' (2021) 31 European Journal of Public Health https://dx.doi.org/10.1093/eurpub/ckab164.126 accessed 16 July 2023.

[40] European Commission. European Health Union: A European Health Data Space for People and Science https://ec.europa.eu/commission/presscorner/detail/e%20n/ip_22_2711 accessed 22nd September 2023.

[41] EHDS proposal, Article 34(1)(e).

[42] A broader discussion about the bounds of what can be considered as scientific research can be found in section 5 of this article.

[43] EHDS proposal, Article 34(1)(a).

[44] GDPR, Article 9(2)(g).

[45] Laura Bradford, Mateo Aboy and Kathleen Liddell, 'COVID-19 Contact Tracing Apps: A Stress Test for Privacy, the GDPR, and Data Protection Regimes' (2020) 7 Journal of Law and the Biosciences lsaa034.

[46] EHDS proposal, Article 34(1)(b).

[47] J Schreyögg and others, 'Defining the "Health Benefit Basket" in Nine European Countries' (2005) 6 The European Journal of Health Economics 2.

social sector which may vary enormously, with public entities having far wider mandates in some states compared to others.[48] In some states, such activities may be largely public whilst in others they may be to a lesser or greater extent commercialized.[49]

3.3. To produce national, multi-national and union-level official statistics related to health or care sectors (Article 34(c))

The EHDS makes clear that data permits can be granted to facilitate the creation of statistics at both the European and national levels. The creation of such statistics is important in order to debate and execute policy decisions effectively. Evidence-based medicine has been at the heart of healthcare for decades. Without correct statistical information that can be used for research, this would be impossible. Whilst the need for statistics appears uncontroversial, one strange aspect of Article 34(c) is that it is not explicit about who should be granted a data permit or for what purposes. The authors of this paper would however point out the use of the word 'official' in this provision. Although one cannot be certain, it could be argued that this is intended to mean that only official agencies (such as Eurostat) at both the Union and Member State levels should be able to make use of this provision. This would inter alia seemingly exclude commercial organizations and campaign groups that might want to create their own statistics in order to call for a change in policy or pursue a commercial agenda.

3.4. Education or teaching activities in health or care sectors (Article 34 (d))

The EHDS will provide an important source of material for teaching and training activities in healthcare. Obvious examples could relate to using secondary data to train medical professionals or allowing medical institutions to optimize their methods. The use of complex EHRs would prove a valuable educational tool for trainee health personnel, in particular in best practice in using EHRs and correctly integrating them into their practice.[50]

What is notable is that unlike the public health orientated ground above, this ground for granting a data permit does not clearly up with one of the grounds for processing sensitive data in Article 9 GDPR. Though academic activities do enjoy some privileges under data protection law, including for teaching purposes (i.e., in Article 85 of the regulation), this does not mean that a legal basis for using sensitive data under Article 9 will not be required.[51] As the authors of this paper will further discuss in Section 5 this seemingly means that HDABs will have to be a little more creative in terms of the legal basis they will permit under the GDPR for such activities.

3.5. Scientific research related to health or care sectors (Article 34(e))

This ground for granting a data license is hardly controversial. The need to foster scientific research is used a number of times in the recitals of the proposals to justify its existence.[52] The EHDS seems to view scientific research in a wide manner, stating that the EHDS should support scientific research "…including private research, development and innovation". This wide definition seemingly means that many types of actors will be able to ask for a data access permit, and for a wide variety of purposes. The essence of this provision is seemingly that a health data access body should grant a data access permit whenever a potential processor wants to process data for scientific research and (as Section 5 discusses in more detail) they have (as is demanded by the GDPR) a valid legal basis in Union or Member State law.[53] Such a wide possibility for granting a health data access permit could create controversy given the wide range of actors that might make use of such a provision for a wide range of purposes including product innovation. Whilst there are some reasons to think the GDPR may pose some further limits on the definition of scientific research (including as Section 5 will further discuss because of a recent European Data Protection Board opinion), some will find the open-ended nature of this provision concerning given the inherently sensitive nature of the EHDS' content.

3.6. Development and innovation activities for products or services contributing to public health or social security (Article 34(f))

A further goal of the EHDS proposal is to facilitate the innovation of products and services relating to health care or social security.[54] Such activities are increasingly data-hungry and as a result, secondary health data is often highly sought after.[55] This is for example particularly true in the design and manufacture of medical devices. It is also the case for the design and surveillance of medicinal products,[56] meaning that secondary health data, i.e., from EHRs is in particular demand.

Access to electronic health data will accordingly likely be granted for designing, testing and follow-up studies on the performance of medical devices. The same is true for medicinal substances, which must undergo a very strict regime of testing and post-market surveillance to be permitted in Europe. Electronic health data could allow for such processes to be met in a cost-effective manner. The drafters of the EHDS proposal accordingly seem to be hoping that the availability of such data will allow for greater levels of innovation in terms of medical devices and medical substances in Europe.

Similarly, the availability of electronic health data could be useful for evaluating healthcare practices, management and healthcare delivery strategies.[57] The availability of large pools of electronic health data, *inter alia* from EHRs, would allow for existing practices to be evaluated more easily and would therefore allow for improved tailoring of such activities. This could allow for a range of practices to be optimised, spanning from particular treatment methods to the structure and mechanisms of health care delivery.[58]

As Section 5 will discuss in further depth below, the above grounds for granting a data licence, go beyond the classical vision of what scientific research is. It encompasses activities that are more readily categorised as innovation activities related to the improvement of medical devices or products. Those familiar with the GDPR and in particular the legal basis relevant for the processing of sensitive data would however point out that such a vision may be considered synonymous with the

[48] Jacques Defourny and Marthe Nyssens, 'Social Enterprise in Europe: Recent Trends and Developments' (2008) 4 Social Enterprise Journal 202.

[49] Jacques Defourny and Marthe Nyssens, 'Social Enterprise in Europe: At the Crossroads of Market, Public Policies and Third Sector' (2010) 29 Policy and Society 231.

[50] Akshay Rajaram and others, 'Training Medical Students and Residents in the Use of Electronic Health Records: A Systematic Review of the Literature' (2020) 27 Journal of the American Medical Informatics Association: JAMIA 175.

[51] Miranda Mourby and others, 'Governance of Academic Research Data under the GDPR—Lessons from the UK' (2019) 9 International Data Privacy Law 192.

[52] Recital 41 for instance states "The provision of the data should also support activities related to scientific research (including private research), development and innovation, producing goods and services for the health or care sectors, such as innovation activities or training of AI algorithms that could protect the health or care of natural persons. "

[53] As section 5 will discuss in more detail, this is required by both Articles 6 and 9 of the GDPR.

[54] EHDS proposal, Article 34(1)(f).

[55] Alison Callahan and others, 'Medical Device Surveillance with Electronic Health Records' (2019) 2 npj Digital Medicine 1.

[56] Hans-Georg Eichler and others, 'Data Rich, Information Poor: Can We Use Electronic Health Records to Create a Learning Healthcare System for Pharmaceuticals?' (2019) 105 Clinical Pharmacology & Therapeutics 912.

[57] FJ Martin-Sanchez and others, 'Secondary Use and Analysis of Big Data Collected for Patient Care' (2017) 26 Yearbook of Medical Informatics 28.

[58] Siobhan O'Connor, 'Secondary Data Analysis in Nursing Research: A Contemporary Discussion' (2020) 29 Clinical Nursing Research 279.

vision of scientific research put forward by the GDPR. In particular, the recitals of the regulation make clear that the vision of scientific research should be broad and not restricted to classic notions of commercial interest or being not for profit.[59] Such a definition is arguably capable of capturing innovation activities such as those foreseen here within the EHDS proposal activities for products or services contributing to public health or social security.

3.7. Training, testing and evaluation of algorithms, including in medical devices (Article 34(g))

Similar to the potential use outlined above for medical products and substances, the EHDS proposal foresees a more specific possibility for providing electronic health data for purposes related to the training, testing and evaluation of algorithms.[60] This is clearly linked to the provision of electronic health data for the production of products used in health care (including most notably medical devices). In providing a standalone ground of provision for the EHDS, the drafters of the proposal are clearly signalling their realization of the importance of software in healthcare specifically[61] and towards innovation in the European economy more generally speaking. In terms of the former the EU's medical device framework, it recognizes that software (including using AI) can itself be part of a medical device or even constitute a medical device by itself.[62] The training, testing and evaluation of algorithms used in such devices require large amounts of data (data for which it may often not be feasible to obtain directly from patients).[63] As a result, the ability to obtain large data sets for secondary use can be crucial for developers.[64] It may also be essential for obtaining and maintaining regulatory approval (given that such devices must be monitored when placed on the market).[65]

3.8. Providing personalized healthcare consisting of assessing, maintaining or restoring the state of health of natural persons, based on the health data of other natural persons. (Article 34(h))

The contexts outlined in Article 34 (f) can be contrasted with many of the others presented in article 34. This is due to the fact that, unlike those grounds, Article 34(h) relates to the treatment of specific individuals. This can be contrasted with others which relate to activities on a larger scale and are likely to have an effect on many people. It seems that the drafters of the EHDS have in mind particular situations where medical professionals may want to discern what experience elsewhere can tell them about the treatment of a particular condition. One could imagine that such a possibility could be useful, particularly in less common or rare conditions. In such instances, medical professionals could presumably make requests for secondary data that was relevant to such contexts. Given that the EHDS demands that data holders make EHRs available for secondary processing, these could be one useful source of information in such contexts.[66] As is discussed in Section 5 however it is not entirely clear which legal basis should or could be used in such a processing context (given that the typical legal bases used by medical professionals relate to a patient's own data being used for their treatment and not for deciding on the best choice of treating another patient).

4. Areas of secondary use which the EHDS will not facilitate

Whilst the EHDS proposal contains very broad provisions that permit the re-use of electronic data for a wide range of activities, the proposal also specifically forbids the re-use of electronic health data for a number of important purposes.[67] The authors of this paper would argue that some of the forbidden processing purposes are significant. This is primarily for two reasons.

First, some of the proposed areas where a data license should not be provided are extremely broad (in particular as is discussed below where a proposed data use may cause "harm to individuals or societies").[68] They will cover a large range of activities in a number of important sectors. The scope of these restrictions should not be underestimated and will represent significant contexts for which the secondary data processing possibilities the EHDS offers will not be available. Given the discretion some of the provisions in Article 35 appear to bestow on data access bodies, it is also difficult to clearly delineate their impact at this time, something that may create a certain lack of clarity and confusion going forward.[69]

Second, some of the purposes for which a data license will not be granted are not illegal, and in a number of instances may affect normal commercial practices. This includes for instance use of secondary data for research within the insurance industry and in marketing.[70] This is noteworthy because the processing of personal data for such purposes may in certain instances be permissible under the GDPR, i.e., using the scientific research exception.[71] As is discussed further below, the fact that Article 35 goes beyond simply ruling out data sharing for illegal use and forbids sharing for a range of processing activities that may be legal (inter alia under the GDPR) may be a testament to the sensitive political character of the EHDS in general. In this context, the inclusion of such broad prohibitions or discretions not to grant a data license probably represented a pragmatic assessment on the part of the Commission of what was necessary to garner the necessary political consensus to push the EHDS proposal through the various stages of the EU legislative process. The authors of this paper would argue that whilst some discretion is necessary, the level of discretion presented in Article 35 is

[59] Recital 157 of the GDPR for instance states … "Where personal data are processed for scientific research purposes, this Regulation should also apply to that processing. For the purposes of this Regulation, the processing of personal data for scientific research purposes should be interpreted in a broad manner including for example technological development and demonstration, fundamental research, applied research and privately funded research."

[60] EHDS proposal, Article 34(1)(g).

[61] William J Gordon and Ariel D Stern, 'Challenges and Opportunities in Software-Driven Medical Devices' (2019) 3 Nature Biomedical Engineering 493.

[62] Emilia Niemiec, 'Will the EU Medical Device Regulation Help to Improve the Safety and Performance of Medical AI Devices?' (2022) 8 DIGITAL HEALTH 20552076221089079., Anastasiya Kiseleva, 'AI as a Medical Device: Is It Enough to Ensure Performance Transparency and Accountability in Healthcare?' (8 November 2019) https://papers.ssrn.com/abstract=3504829 accessed 14 September 2022.

[63] I Glenn Cohen and others, 'The European Artificial Intelligence Strategy: Implications and Challenges for Digital Health' (2020) 2 The Lancet Digital Health e376.

[64] Anastasiya Kiseleva, Dimitris Kotzinos and Paul De Hert, 'Transparency of AI in Healthcare as a Multilayered System of Accountabilities: Between Legal Requirements and Technical Limitations' (2022) 5 Frontiers in Artificial Intelligence https://www.frontiersin.org/articles/10.3389/frai.2022.879603 accessed 14 September 2023.

[65] Sarah Jabri, 'Artificial Intelligence and Healthcare: Products and Procedures' in Thomas Wischmeyer and Timo Rademacher (eds), *Regulating Artificial Intelligence* (Springer International Publishing 2020) https://doi.org/10.1007/978-3-030-32361-5_14 accessed 15 February 2023.

[66] EHDS proposal, Article 33(1)(a).

[67] EHDS proposal, Article 35.

[68] EHDS proposal, Article 35(c).

[69] A wide discretionary power also seems confirmed in recital 42 of the EHDS proposal which inter alia states "… Health data access bodies should not be influenced in their decisions on access to electronic data for secondary use. However, their independence should not mean that the health data access body cannot be subject to control or monitoring mechanisms regarding its financial expenditure or to judicial review"

[70] EHDS proposal, Article 35(b).

[71] GDPR, Article 9(2)(j).

concerning. This, and the fact that there will be scope for HDABs in 27 different countries to interpret Article 35 of the proposal differently raise serious concerns about consistency and potential abuse of discretion.

Article 35 rules out the provision of a data license in the following circumstances:

4.1. Taking decisions detrimental to a natural person based on their electronic health data (Article 35(a))

The EHDS will not provide electronic health data where it is to be used to arrive at 'detrimental decisions'[72] that can have negative consequences for individuals. The EHDS proposal indicates that in order to qualify as 'detrimental decisions', they must produce "legal effects or similarly significantly affect those natural persons". This language is notable in that it is similar to that used in Article 22 of the GDPR concerning the use of automated decision-making. In Article 22 however, there is no mention of the word 'detrimental'. The existence of "legal effects concerning him or her or similarly significantly affects him or her" is sufficient.[73]

This would therefore seem to relate primarily to the potential risk of discrimination in terms of the provision of goods or services or employment.[74] As Binns and Veale[75] point out "Recital 71 of the GDPR, EDPB guidance has elaborated with several other examples of decisions whose effects would qualify as significant, including dynamic pricing which effectively excludes certain people from buying certain goods or services." The authors of this paper would also argue that given the nature of electronic health data, further related risks could occur for example where electronic health data could be used to discern that the provision of certain services to certain categories of people would be less likely to be profitable (i.e., perhaps because of the presence of certain health indicators or other factors).

Importantly, the term 'detrimental decisions' is not defined. This is an important point of differentiation with the wording used in Article 22 of the GDPR. This means that the provision will be open for interpretation by the data access bodies. On the one hand, given that the term 'detrimental' could be interpreted in extremely wide terms, in a broad range of contexts, this provision seemingly grants broad discretion to those responsible for granting permits to refuse to do so. On the other, the inclusion of the word "detrimental" in the EHDS proposal but not in the related phrasing of Article 22 of the GDPR would seem to indicate that the intention has been to reduce the scope. The authors of this paper would submit that further guidance on this will be needed in the future in order to prevent confusion and discontent at decisions made by those given responsibility under the EHDS.

4.2. Decisions to exclude from insurance contracts or alter insurance premiums (Article 35(b))

The EHDS proposal also forbids the use of electronic health data in order to exclude individuals from insurance policies or to conduct processes that will ultimately relate to altered premiums. This latter aspect appears to concern the potential use of electronic health data made available by data access bodies to insurance companies (or third parties on their behalf) to conduct research to optimise premiums or even exclude potential customers from coverage. This exclusion seemingly goes beyond the use of personal data to exclude those from whom it may directly link and appears intended to also cover cases where electronic health data is used to make conclusions about the exclusion or the creation of higher premiums for certain categories of people. There is a clear demand on the part of the insurance industry for research data in order to arrive at broad conclusions (and not to make decisions about particular inidvidual from whom the data may be derived).[76] Such a demand cannot seemingly be accommodated by the EHDS and data access bodies according to Article 34 of the proposal.

Whilst such a grounds for refusal of a data permit may have significant ethical grounds, the authors of this paper would submit that it was also considered politically expedient of the EHDS proposal drafters to exclude such a possibility given that it would likely greatly increase resistance to the EHDS in general and possibly render an agreement on a definitive legal text impossible.

4.3. Advertising or marketing activities towards health professionals, organisations in health or natural persons (Article 35(c))

In comparison to the US, the advertising or marketing of healthcare-related products or services is tightly regulated in Europe. Directive 2008/83 EC on the Community code relating to medicinal products for human use for example makes it illegal to advertise prescription drugs. It also imposes specific rules for direct-to-consumer advertising of over-the-counter drugs.[77] In this pre-existing legal context, the EHDS proposal's prohibition on the sharing of data for secondary use for marketing activities is curious. It seems once again the discretion granted to HDABs to refuse data licenses extends far beyond preventing that which is already prohibited by law.

This may be relevant for example with regards to certain forms of marketing directed at health care professionals for medicinal substances, or for certain forms of medical or well-being services (i.e., for which advertising may generally be permitted because they fall outside of current legislative prohibitions on advertising) .[78] Depending on the Member State in question, some of these activities may be permissible to a lesser or greater extent. This includes for example advertising for certain forms of direct-to-consumer genetic testing for health, wellness and lifestyle reasons.[79]

It is not clear why the drafters of the EHDS proposal have set aside marketing activities as being so specifically undesirable. Such activities can sometimes have an important and useful role in bringing the attention of certain stakeholders to suitable products and services. In

[72] The authors would point out that because of the way the article is worded in Article 35 of the proposal, the wording is actually "taking decisions detrimental to a natural person based on their electronic health data; in order to qualify as "decisions", they must produce legal effects or similarly significantly affect those natural persons;"

[73] For further discussion on Article 22 of the GDPR see Reuben Binns and Michael Veale, 'Is That Your Final Decision? Multi-Stage Profiling, Selective Effects, and Article 22 of the GDPR' (2021) 11 International Data Privacy Law.. As the authors point out (p320) this provision is also very similar to "the Law Enforcement Directive, the GDPRs sister instrument for police and criminal justice".

[74] This is a concern raised by GDPR Recital 71 which raises related concerns including the possibilities of effected credit scores. It also says Such processing includes "profiling that consists of any form of automated processing of personal data evaluating the personal aspects relating to a natural person, in particular to analyse or predict aspects concerning the data subject's performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, where it produces legal effects concerning him or her or similarly significantly affects him or her.'

[75] Binns and Veale (n 71). At 320.

[76] Ehab Hasan, 'Chapter 29 - Examples from Administrative Claims Data and Electronic Health Records' in Cynthia J Girman and Mary Elizabeth Ritchey (eds), *Pragmatic Randomized Clinical Trials* (Academic Press 2021) https://www.sciencedirect.com/science/article/pii/B9780128176634000027 accessed 28 February 2023.

[77] Louiza Kalokairinou, Pascal Borry and Heidi Carmen Howard, 'Regulating the Advertising of Genetic Tests in Europe: A Balancing Act' (2017) 54 Journal of Medical Genetics 651.

[78] William Davies, *The Happiness Industry: How the Government and Big Business Sold Us Well-Being* (Verso Books 2015).

[79] Jacqueline A Hall and others, 'Transparency of Genetic Testing Services for "Health, Wellness and Lifestyle": Analysis of Online Prepurchase Information for UK Consumers' (2017) 25 European Journal of Human Genetics 908.

areas such as well-being and nutrition, marketing is already common.[80] Their exclusion appears to reflect an ideological position that is common across much of Europe relating to commercial activities in the domain of health care, and therefore could be seen to reflect popular concerns about the use of electronic health data and therefore also the acceptability of a framework such as that foreseen within the EHDS. Again, it could be argued that the adoption of this position was motivated by political concerns as much as it was by ethical or legal questions.

4.4. Providing access to, or otherwise making available, the electronic health data to third parties not mentioned in the data permit (Article 35 (d))

The EHDS will not grant licenses to entities intending to make the electronic health data provided available to other unknown third parties. This will protect against potential privacy harms and other detrimental effects that could be produced when permit holders are able to pass on electronic health data to unknown third parties. Given the potential breadth in terms of potential third party use it is beyond the scope of this paper to go into depth on such issues. Once again, however, it seems likely that the EU Commission, in proposing this such a limitation, was not only motivated by reducing the possibilities for such harms but also by the need to maintain trust and confidence in the notion of the EHDS. As Section 5 below will discuss in further detail, where electronic health data is also personal data, the requirements of the GDPR would seemingly prevent transmission to third parties in most cases. One major issue that still needs to be resolved is the consequences that will come into play if data holders do not respect this aspect of their data permit. This issue will be particularly pertinent where the data user in question may have the possibility under the GDPR to allow processing by a third party (perhaps using the scientific research exemption as outlined in Article 9 of the GDPR) or where the electronic health data that has been provided does not constitute personal data. Recital 49 of the EHDS proposal states:

"In order to strengthen the enforcement of the rules on the secondary use of electronic health data, appropriate measures that can lead to penalties or temporary or definitive exclusions from the EHDS framework of the data users or data holders that do not comply with their obligations. The health data access body should be empowered to verify compliance and give data users and holders the opportunity to reply to any findings and to remedy any infringement. The imposition of penalties should be subject to appropriate procedural safeguards in accordance with the general principles of law of the relevant Member State, including effective judicial protection and due process."

Article 10(3) seems to leave the precise details of this for future legislative acts stating:

"The Commission is empowered to adopt delegated acts in accordance with Article 67 to supplement this Regulation by entrusting the digital health authorities with additional tasks necessary to carry out the missions conferred on them by this Regulation and to modify the content of the annual report."

4.5. Use of electronic health data leading to the development of products or services that may harm individuals and societies at large (Article 35(e))

Whilst Article 35 of the proposal does give some specific examples of harmful products or services (e.g., to produce illicit drugs, alcoholic beverages, and tobacco products), it also provides a very broad possibility for data permits to be refused where they could lead to "goods or services which are designed or modified in such a way that they contravene public order or morality". Again, as with Article 35(d) above the EHDS proposal does not go into further detail in terms of defining what contravening public order or morality is.[81] This appears once again to leave broad discretion to those responsible for granting data permits in determining what products or services would meet such criteria.[82]

5. Key limiting factors on data access body discretion

As was explained in the foregoing section, the EHDS appears to permit a wide spectrum of uses of concerned electronic health data. Article 34 appears to provide very broad discretion for the granting of data licenses by HDABs to a wide array of actors for a broad range of purposes.[83] In Section 4 above the authors of this paper described one important protective pillar against misuse of this broad discretion, i.e., the contexts outlined in Article 35 for which a proposal may not be granted. A second key protective pillar is that the discretion granted to HDABs is limited by a requirement to only grant a data access request when the proposed processing would be GDPR compliant. This factor must be considered in addition to the contexts outlined in Article 34 for which a data access permit request should not be granted (discussed above in Section 4). The remainder of this paper will look at how GDPR will limit the potential re-use grounds under Article 34 EHDS.

5.1. Data permits general and the GDPR

Perhaps the most important limiting factor for HDABs is that they must ensure that the proposed processing is generally GDPR compliant. The GDPR applies to personal data, this includes all data that is not anonymous, including highly pseudonymized data.[84] Given that personal data has a higher research value than non-personal data, many access requests will in all likelihood be for personal data.[85] The preamble of the proposal makes it clear that the processing of personal electronic health data is subject to the GDPR[86] and that the proposed EHDS legal framework is the legal grounds for the HDAB (or data holder) to make data available but does not itself provide a legal basis for data recipients to process personal data. It states:

"This Regulation provides the legal basis in accordance with Articles 9(2)(g), (h), (i) and (j) of Regulation (EU) 2016/679 for the secondary use of health data, establishing the safeguards for processing, in terms of lawful purposes, trusted governance for providing access to health data (through health data access bodies) and processing in a secure environment, as well as modalities for data processing, set out in the data permit…This Regulation creates the legal obligation in the sense of Article 6(1) point (c) of Regulation 2016/679 for disclosing the data by the data holder to health data access bodies…This Regulation also meets the conditions for such processing

[80] Min Yan and others, 'Mobile Apps for Healthy Living: Factors Influencing Continuance Intention for Health Apps' (2021) 166 Technological Forecasting and Social Change 120644. This includes for example in the area of health apps.

[81] The authors note that the terms "public order" or "morality" are not produced elsewhere in in the proposal or in the explanatory materials provided with it.

[82] The criteria of contravening "public order or morality themselves are noteworthy in that resemble conditions founding with the qualifying paragraphs of article delineating rights withing the European Convention of Human Rights.

[83] As Article 46(6) of the proposal states: "The data permit shall set out the general conditions applicable to the data user, in particular: (a)types and format of electronic health data accessed, covered by the data permit, including their sources; (b)purpose for which data are made available; (c)duration of the data permit;(d)information about the technical characteristics and tools available to the data user within the secure processing environment; (e)fees to be paid by the data user; (f)any additional specific conditions in the data permit granted.

[84] The fact that pseudonymous data is personal data is clear from the definition of the former in Article 4(5) GDPR.

[85] Paul Quinn, 'The Anonymisation of Research Data—A Pyric Victory for Privacy That Should Not Be Pushed Too Hard by the EU Data Protection Framework?' (2017) 24 European Journal of Health Law 347.

[86] Recital 4: The processing of personal electronic health data is subject to the provisions of Regulation (EU) 2016/679 of the European Parliament and of the Council.

pursuant to Articles 9(2) (h), (i), (j) of the Regulation 2016/679. Therefore, in this case, this Regulation provides the legal basis under Article 6 and meets the requirements of Article 9 of that Regulation on the conditions under which electronic health data can be processed."[87]

Here the legislators are outlining that it is the EHDS itself, (in line with Article 9 of the GDPR) that provides the legal basis for the assembly and communication of data by the HDAB and data holders and the processing that is necessary in doing so. The regulation itself however does not provide a legal basis for the further processing of personal electronic health data by a recipient once a data access permit has been granted to them. As the preamble to the proposal further states:

"*At the same time, the data applicant should demonstrate a legal basis pursuant to Article 6 of Regulation (EU) 2016/679, based on which they could request access to data pursuant to this Regulation…(T)he data user should demonstrate its legal basis pursuant to Articles 6(1)(e) or (f) of Regulation 2016/679 and explain the specific legal basis on which it relies as part of the application for access to electronic health data…If the user relies on 6(1), point (e) it should make reference to another EU or national law, different from this Regulation mandating the user to process personal health data for the compliance of its tasks*"[88]

In order to obtain a data access permit, the data user will therefore be required to explain the legal basis they are going to use to process the data in question. This may include references to national law *inter alia* when a public interest base is used.[89] This is because the GDPR makes clear that where a public interest basis is used (e.g.., in order to justify processing for scientific research), such processing must be supported by Union or Member State law. Given that national law concerning health data is still highly heterogeneous, the potential legal bases that could be used to justify such processing can vary enormously.[90]

Perhaps one of the most remarkable phrases within the recitals of the proposal relates to the potential use of the legitimate interest base. Here the proposal states:

"If the lawful ground for processing by the user is Article 6(1), point (f), of Regulation (EU) 2016/679, in this case it is this Regulation that provides the safeguards. In this context, the data permits issued by the health data access bodies are an administrative decision defining the conditions for the access to the data."[91]

The wording used here is remarkable in that it appears to indicate that one of the purposes of the EHDS is to facilitate the potential use of the 'legitimate interests base'. It will do this by providing appropriate 'safeguards'. This presumably means appropriate institutional, technical and security measures. This will facilitate the use of the legitimate interest legal basis because the existence of such 'safeguards' can be used by the prospective data controller to argue that the required proportionality balancing test[92] (where the purpose of processing is assessed against the risks to data subjects) has been met. Whilst this does not guarantee that the requirements of legitimate interest will be met, it will in certain circumstances make things easier for potential data recipients who might want to rely on this legal basis.

5.2. Ensuring that a valid legal basis exists

Proving compliance with the GDPR in a data access request will require a number of important steps. Crucially, the scope of potential processing activities should be sufficiently detailed and circumscribed so as to be able to determine what kind of processing is and is not included within the specified purpose. Such a step is critical if a HDAB is to be able to make an analysis of whether a valid legal ground exists or not.[93] This step is not only crucial in determining which legal basis is appropriate (or not) but also in demonstrating what data protection safeguards should be applied in a particular context.

Applicants for a data permit must outline their choice of legal basis and justify their selection.[94] Given that the EHDS will not be consent-based (at least in terms of a GDPR based understanding of the notion of consent), there are (as the EHDS proposal outlines) a limited number of other potentially applicable options (at least in terms of the GDPR – the situation concerning national law may be more complex). Where the data constitutes sensitive data (a likely common occurrence with electronic health data), the data recipient will also need to demonstrate a legal basis under Article 9 of the GDPR. The authors of this paper would argue that given the practical aspects and limitations of data re-use and the grounds under Article 34 EHDS, it seems likely that most data access permit requests will fall into one of two categories. These could be loosely grouped under 'public interest-based processing' and processing for commercial reasons falling under the 'legitimate interest' grounds. The possibilities and difficulties of both approaches are further discussed below.

5.2.1. Public interest processing activities

One of the most important motivations behind the EHDS was to create and facilitate the processing of secondary electronic health data for public interest reasons. This could include for purposes of scientific research, public health or in order to improve the management of healthcare systems. A simple analysis (see Section 3 above) of Article 34 of the EHDS proposal[95] shows that many of the permitted grounds for granting a data permit overlap with the main public interest legal basis

[87] EHDS proposal, Recital 37.

[88] Recital 37, GDPR. We presume the omission of Article 9 is an oversight, or to be understood as falling under the reference to Article 6. Indeed, paragraph 37 of the Interinstitutional File: 2022/0140(COD) now refers to Article 9 GDPR :*"The purpose of processing electronic health data for secondary use, one of the legal bases set out in Article 6(1), points (a), (c), (e) or (f), of Regulation (EU) 2016/679* ***combined with Article 9(2) of that Regulation*** *should be required…*"

[89] Recital 4 also states "the data user should demonstrate its legal basis pursuant to Articles 6(1), points (e) or (f), of Regulation (EU) 2016/679 and explain the specific legal basis on which it relies as part of the application for access to electronic health data pursuant to this Regulation: on the basis of the applicable legislation, where the legal basis under Regulation (EU) 2016/679 is Article 6(1), point (e), or on Article 6(1), point (f), of Regulation (EU) 2016/679. If the user relies upon a legal basis offered by Article 6(1), point (e), it should make reference to another EU or national law, different from this Regulation, mandating the user to process personal health data for the compliance of its tasks."

[90] Paul Quinn, 'Research under the GDPR - a Level Playing Field for Public and Private Sector Research?' (2021) 17 Life Sciences, Society and Policy 4.

[91] Preamble para 37. This principle appears to have been similarly provided for in the Interinstitutional File: 2022/0140(COD), preamble 37 reads as follows: "*If the health data user relies upon a legal basis offered by Article 6(1), point (e), or on* ***Article 6(1), point (f), of Regulation (EU) 2016/679*** *or Article 5(1), point (a) of Regulation (EU) 2018/1725, in this case it is* ***this Regulation that should provide the safeguards required under Article 9(2) of Regulation (EU) 2016/679*** *or Article 10(2) of Regulation (EU) 2018/1725*".

[92] Pablo Trigo Kramcsák, 'Can Legitimate Interest Be an Appropriate Lawful Basis for Processing Artificial Intelligence Training Datasets?' (2023) 48 Computer Law & Security Review 105765.

[93] This analysis will have to be performed subsequently to the analysis demanded by Articles 33 and 34 of the proposal i.e., relating to contexts for which a health data access permit should or should not be granted. For more see section 3 and section 4 of this paper.

[94] In the European Parliament Draft Committee report 2022/0140(COD) of 10.02.2023, it seems there was a proposal to limit the potential GDPR legal basis applicable for access request by modifying article 34 to the following "*Health data access bodies shall only provide access to electronic health data referred to in Article 33 to a health data user where the processing of the data by the applicant is necessary for one of the following purposes, and* ***in accordance with Article 6(1)(c) and Article 9(2)(g), (h), (i) and (j) of Regulation (EU) 2016/679***". Thankfully, this final phrase was not reiterated in article 34 in the "Interinstitutional File: 2022/0140(COD)".

[95] As section 3 discusses in further depth this includes section 34(1) which specifically invokes public interest as a ground for granting a data license.

in the GDPR (i.e., Article (6(1)(e)).[96] It is important to note however that the GDPR is clear that the possibility to use this legal ground must be further outlined in national law. This means that in order to use such grounds, the data users will, in their application for a data permit, have to identify relevant EU or national law (i.e., not from the EHDS regulation itself), permitting them to process personal electronic health data. Such a condition applies even where it is clear that the processing in question falls under one of the approved types of processing outlined in Article 34 of the proposal. Furthermore in order to demonstrate compliance with the GDPR, potential data recipients will have to show that the processing is necessary to achieve the public interest objective identified and is proportionate to the legitimate aim pursued.[97] Compliance with a relevant legal basis under Article 6 will also likely mean compliance with a relevant base under Article 9 given that if the data is personal is often likely to be of a sensitive nature i.e., health data.

In most cases the need to find a legal basis under Article 9 (for sensitive data) will not pose major difficulties, given the parallels and similarities between Articles 6 and 9 on public interest/health grounds. In such instances, this type of potential recipient will likely be able to use the same legislative authority in national law to meet the conditions under the public interest base of Article 6 and one of the potential bases of Article 9 (i.e., show a legal basis in national law, demonstrate necessity and proportionality etc.).

In terms of GDPR compliance being a limiting factor on the granting of a data permit, the need to show alignment with Articles 6.1 (e) and 9 (1)(g) or (i) is arguably therefore not very onerous. The most demanding requirements linked to this are the need to show other EU or national legislation that is applicable and that such processing is both necessary and proportionate, as well as the fact that the law invoked meets an objective of public interest and is proportionate.[98] In terms of the former, whether potential data recipients can do so will depend on a number of factors, including the nature of the legislation in question, what type of entity they are and naturally, what the intended purposes of processing are. For a number of the proposed contexts for which HDABs are supposed to grant a health data access permit under Article 34 of the EHDS proposal, there will in many instances likely be a legal basis under the GDPR and national law that is readily applicable (e.g., for public interest related processing carried out by public bodies or research institutions such as universities). The types of legislation that exist and which could be linked to Articles 6(1)(e) and 9(1)(g) or (i) GDPR are many and varied. They also differ greatly from Member State to Member State. Some may be very general, outlining broad grounds while others may be quite restrictive. What difficulty potential data recipients will have in meeting such requirements will therefore depend on who they are, what they are doing and in what Member State they are based. Whilst a broad rule of thumb will correctly suggest that it will be generally easier for public-based entities than for commercial entities the correctness of this rule very much depends on the state in question.

5.2.2. Commercial processing activities

Legitimate interest[99] *is often an attractive base for commercial entities:*

Whereas the public interest base in the GDPR is potentially (depending on the Member State legislation in question) more accessible to public bodies and research-orientated organizations such as universities, the legitimate interest base is, without doubt, more accessible to private entities. Such organizations may not have a public interest motive but may wish to carry out research with the goal of fostering innovation or some other related commercial motive.[100] For private sector entities, the 'legitimate interest' base in Article 6 GDPR grants a wide possibility for processing personal data when it can be demonstrated that it is in their legitimate interest.[101] Interestingly, and in contrast to the 'public interest' base outlined above, it is also not needed to identify further applicable Union or National legislation. As a result, Article 6.1 (f) is one of the most commonly used legal bases for private sector entities and will likely be very important for such entities when applying for a data access permit under the EHDS. This is seemingly something the drafters of the EHDS framework wanted to facilitate with their statement that EHDS "Regulation that provides the safeguards" that are required to justify the use of the legitimate interest base (discussed in Section 5.2.1 above).

A three-step test

Despite the fact that the legitimate interest base provides wide possibilities for private sector entities to process personal data and the fact that the EHDS seemingly seeks to facilitate the use of this base, the potential for its use nonetheless still has important limits. Important requirements still remain that will limit the ability of potential data recipients to use this base as a basis for a data access permit. Most importantly potential data recipients will, in order to demonstrate compliance with the GDPR, have to show that they meet a three-step test.[102]

Under the three-step test, *first,* the controller must identify a legitimate interest. For an interest to be legitimate, the interest must be lawful, sufficiently clearly formulated, and present a real and present interest. This therefore rules out potential requests that are ambiguous or speculative in nature.[103] Such purposes can be wide and varied, ranging from commercially motivated product innovation to 'scientific research' that is clearly in the public interest.[104]

Second, it is necessary to show that the identified processing activity is necessary to achieve the interest pursued. This requires a connection between the processing activities and the interest(s) pursued by the data controller. Moreover, it must be assessed whether there are other less invasive means to reach the identified purpose of the processing. Logically this means in the context of an EHDS data request, where it is indicated that the base to be relied upon will be 'legitimate interest', an applicant will have to demonstrate that it is necessary to receive the requested data in question in order to achieve the processing activity's objective. For scientific research and related activities, this implies being able to justify that access to the data itself is required to answer the

[96] Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller Article (6(1)e GDPR). It should be noted that where the data in question in sensitive (as electronic health data will often be) that the equivalent legal bases under Article 9 will be engaged. These are contained withing 9.2 (g) and (i) respectively.

[97] GDPR, Article 6(3) and an expression of Article 52(1) of the Charter.

[98] See GDPR Article 6(3) and Charter, Article 52(1).

[99] Processing is necessary for the purposes of the legitimate interests Article (6 (1)(f) GDPR).

[100] GDPR Recital 47 also makes it clear that the legitimate interest base should not be used by public bodies when carrying out their function.

[101] Chris Jay Hoofnagle, Bart Van Der Sloot and Frederik Zuiderveen Borgesius, 'The European Union General Data Protection Regulation: What It Is and What It Means' (2019) 28 Information & Communications Technology Law 65.

[102] The elements of these tests are further discussed in Irene Kamara and Paul De Hert, 'Understanding the Balancing Act Behind the Legitimate Interest of the Controller Ground: A Pragmatic Approach' (8 August 2018) https://papers.ssrn.com/abstract=3228369 accessed 20 September 2023.

[103] "This requires a real and present interest, something that corresponds with current activities or benefits that are expected in the very near future. In other words, interests that are too vague or speculative will not be sufficient." Article 29 WP Opinion 06/2014 on the "Notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC" - WP217, p.25

[104] Kramcsák (n 90).

research question being posed.[105] For HDABs, this will potentially entail a need to enquire about the scientific merit of the request and the need for the requested data in highly variable contexts. This could range from studies using genomic data to others that are based on medical imagery. As is discussed further below in 5.3 concerning the question of 'data minimization', is not clear if expecting HDABs to undertake such diverse tasks is either desirable or realistic.[106]

Third, a balancing test must be successfully performed. This means that the risk to the fundamental rights and interests of the data subjects should not outweigh the interest of the controller, taking into account i) the importance of the interests at play, ii) the potential impact on these rights/interests, and iii) the safeguards implemented. Generally, in the context of the processing of health data the risk to the fundamental rights and interests of the data subjects will be given significant weight. In such instances, the balancing exercise will accordingly require weighty reasons together with sufficient protections to justify processing. It is in this context that the statement in the EHDS proposal (described above), that the EHDS framework itself should in the context of balancing exercise be considered a 'safeguard', is of importance. This is because when a potential data recipient is trying to access data through the EHDS, the existence of the platform (with its legal and technical underpinning) will assist in arguing that the balancing test has been met. That statement will by itself not be sufficient to tip the balance in favour of the data user's interest (given that such safeguards are one part of the three-part test),[107] but it will make things easier. This would notably be the case for example if one were to compare a commercial entity that was trying to scrape personal data online to one that wanted to gain access to it through the EHDS. The authors of this paper would argue that, in the latter case, the potential data recipient would find it easier to argue that the balancing test had been met.

The likely need to find an accompanying base under Article 9 GDPR

It is important however to remember that in many cases requests for personal data through the EHDS will constitute requests for sensitive data, i.e., health data. This means that it will also be necessary to show a legal basis under Article 9 GDPR has been met. For entities relying on 'legitimate interests' as a legal basis under Article 6, this may be difficult given that there is no direct equivalent base under Article 9. This can be contrasted for example with the situation discussed above for public bodies, universities or other research institutions that may be relying on a public interest base. Where non-public entities are relying on legitimate interest under Article 6 however, the situation is more complex. They may find it harder to avail themselves of legislative authority in national law (as required by Articles 9(1)(g) or (i) GDPR) given that it may be less likely to apply in their context (e.g., being a private entity or having commercial motivations).[108] In cases where personal health data is being requested, the need to also comply with an Article 9 legal basis may therefore in reality make it difficult for non-public sector actors seeking to invoke legitimate interests under Article 9. For commercial entities wishing to carry out commercially motivated research with data obtained from the EHDS, the most likely grounds are likely to be Article 9.1(j) i.e., 'for scientific or historical research purposes'.

One might ask however whether a number of the activities within the EHDS proposal (and for which one might imagine the use of legitimate interests as a legal basis under Article 6 of the GDPR can be legitimately considered as 'scientific research'. This notably includes activities that can be described as falling under the umbrella of 'innovation'. In the context of the GDPR at least there is no simple answer. To begin with, the regulation certainly does not see scientific research as a narrow concept. As Recital 159 of the GDPR states:

"For the purposes of this Regulation, the processing of personal data for scientific research purposes should be interpreted in a broad manner including for example technological development and demonstration, fundamental research, applied research and privately funded research"

This points to a very open mind in terms of what the drafters of the GDPR regarded as 'research', with a concept that does not discriminate between research of varying types (e.g., public, private or commercially motivated). Despite this, it would probably not be wise to view the concept of scientific research under the GDPR as boundless. In its opinion of the 6 January 2020[109] EDPS states:

"*Scientific research applies the 'scientific method' of observing phenomena, formulating and testing a hypothesis for those phenomena, and concluding as to the validity of the hypothesis…. The conduct of research must allow testing of hypotheses, with both the conclusion and the reasoning transparent and open to criticism. Openness and transparency help distinguish between science and pseudo-science.*" … *"For the purposes of this Preliminary Opinion, therefore, the special data protection regime for scientific research is understood to apply where each of the three criteria are met:*

-personal data are processed;
-relevant sectoral standards of methodology and ethics apply, including the notion of informed consent, accountability and oversight;
-the research is carried out with the aim of growing society's collective knowledge and wellbeing, as opposed to serving primarily one or several private interests."[110]

The authors would argue that this definition posed by the EDPS is an attempt to narrow the scope of what one could consider to be scientific research (i.e., from the extremely broad reading which prima facie seems to be encouraged by the GDPR). Most notably it appears to exclude activities that are narrowly focused on forms of innovation for commercial motives. If the EDPS is correct, this would be significant because it would seemingly exclude some of the contexts under Article 34 EHDS for which a data access permit should be granted. As Section 3 of this paper discussed in greater depth this could include for 'development and innovation activities for products or services' (Article 34 (1)(f)) or for the 'training, testing and evaluating of algorithms' (Article 34 (1)(g)). This borad EHDS vision also seems to be supported by Recital 41

[105] One wonders if this means that data users/applicant/controller will have to argue why they are making a data access request and not a data request under Article 47 EHDS. Arguably, also following the principle of minimization – the data request should be the first port of call, with only the possibility to request access to data (anonymized or pseudonymized) as a second step requiring scientific justification. The risk here is that the HDAA will take on the role of 'research statistics bureau' as well as administrative authority, which is not the intention and has other budgetary implications.

[106] It is worth noting that in the Parliament's proposed amendments to Article 44.1, the HDDA body should "ensure that access is only provided to requested electronic health data **necessary** and relevant for the purpose of processing indicated in the data access application by the data user and in line with the data permit granted." Assessing the necessity of data is clearly a task that legislators envision the HDAA being able to carry out.

[107] In Article 45(2) the data user has to provide measures/safeguards to prevent function creep and to protect the rights and interests of the data holder and of the natural persons concerned.

[108] Quinn (n 88). One might also presume that if they could use such a public interest themed legal basis they would not need to rely on legitimate interests under Article 6 of the GDPR in the first place (given that they could have claimed a public interest base under Article 6 also).

[109] European Data Supervisor, "A Preliminary Opinion on data protection and scientific research", 6 January 2020, p.13.

[110] European Data Supervisor, "A Preliminary Opinion on data protection and scientific research", 6 January 2020, p.10.

of the EHDS proposal which states:

"The provision of the data should also support activities related to scientific research (including private research), development and innovation, producing goods and services for the health or care sectors, such as innovation activities or training of AI algorithms that could protect the health or care of natural persons".

This statement is notable because it proposes a wide definition of scientific research, similar to the original outlined in recital 159 of the GDPR. The authors of this paper would however argue that this apparent difference in vision of what constitutes scientific research in the EHDS proposal and the EDPS opinion described above may not actually be of major practical consequence. This is because, in the context of the EHDS proposal, the fact research relating to the "innovation or the production of goods" relates specifically to the 'health or care sectors' means that such activities can be considered as having sufficient 'societal purpose' to meet the EDPS definition of scientific research also.

In other contexts, certain activities may be more problematic, however. The concept of 'innovation' for example is broad. It may not follow a precise recognized methodology and, depending on who is involved, it may not be subject to reliable accountability or oversight practices. Whether this fits into the notion of scientific research as far as the GDPR is concerned is something that HDABs will have to determine for each request.

A final issue once again that will make utilization of a base such as Article 9(1)(g) of the GDPR difficult for commercial organizations in some instances is that HDABs will have to verify whether supporting legislation exists under national law and whether it is applicable to the entity and type of processing in question. As is discussed above this is a condition when using one of the likely relevant bases under Article 9. The different Member States have adopted very different approaches in their relevant legislation.[111] Some may have taken a very general approach to allowing scientific research in the abstract, whilst others may be very specific relating to more definite activities.[112] Likewise, some may specify what types of entity can use the provision in question (e.g., defined public bodies, public bodies in general or any public or private entity) whilst others may be silent on this issue, with their application being determined primarily by the goals of the processing in question. In certain member states it may be necessary to show that processing is 'in the public interest' whilst in others this may not be the case. This disparity in Member State law may lead to some forum shopping.[113] It also raises another difficult question - which local law will data users have to meet when requesting data through the EHDS? Imagine an Italian company requesting data from a Danish HDAB. Would it have to comply with Italian or Danish national law on health data (or both)? Unfortunately, a full exploration of this question is beyond the scope of the current paper.

5.2.3. Other types of data requests and potential legal bases

In addition to the two main categories of data requests outlined above, there are types of requests under Article 34 of the EHDS that are likely to pose difficulties in terms of having to find the correct legal basis. This includes in order to facilitate teaching opportunities using data obtained from the EHDS. As discussed in Section 3 above, the EHDS proposal in Article 34(1)(d) states that a health data access permit should be granted for "education or teaching activities in health or care sectors". Questions may be raised over how such a permitted use may be in compliance with the need to find a legal basis under Article 9 of the GDPR. From looking at the available bases, with the exception of consent, it is not clear which base would be appropriate. Given that the EHDS will not itself be based on explicit consent, this option does not seem appropriate either.

Even with an expansive reading, the so-called 'scientific research' exception (i.e., Article 9(1)(j)) could likely not be read as covering teaching or training activities. The only remaining realistic possibility could be seeking authorization for such activities under the guise of 'substantial public' interests as outlined in Article 9(1)(g). The authors would however underline the importance of the word 'substantial' in this provision which would seemingly be indicative of a processing purpose that was without doubt in line with an important public interest need. This case could perhaps be made for the teaching of doctors, nurses or other important medical professionals, without which society would face serious health problems. It is arguably doubtful that such purposes could be stretched to include a number of commercial domains where a substantial public interest reason was less clear. This could be a problem, for example, for any proposed teaching purpose linked to the wellbeing, sport or lifestyle sectors. Even in instances that were clearly of substantial public interest, there would be a need (as indicated by the requirement for Union or Member State law in Article 9(1)(g)) to point to specific legislation at the Member State Level authorizing such activities. This requirement essentially means that in order for a HDAB to grant a request under Article 34(1)(d) of the EHDS proposal for teaching or educational purposes, it will seemingly have to corroborate that the necessary legislation exists at national law that is compatible with Article 9(1)(g) of the GDPR. Without such legislation, entities will not be able to access and utilize the possibility outlined under EHDS proposal Article 34 for such purposes.

An even more perplexing problem is which legal basis should be considered suitable for the purpose outlined in Article 34 (h) of the EHDS proposal, i.e., "Providing personalized healthcare based on the health data of other natural persons". It seems that the drafters of the EHDS have in mind particular situations where medical professionals may want to discern what experience elsewhere can tell them about the treatment of a particular condition. In such instances, medical professionals could presumably make requests for secondary data that was relevant to such contexts. As is discussed in Section 3 however, it is not entirely clear which legal basis should or could be used in such a processing context (given that the typical legal bases used by medical professionals relate to a patient's own data being used for their treatment and not for deciding on the best choice of treating another patient). This is the case with the base outlined in Article 9(2)(h) e.g., where "processing is necessary for the purposes of preventive or occupational medicine". This base is often used by medical professionals to access patient dossiers in the course of their treatment without continually having to ask for consent. Indeed, it forms the mainstay legal basis of many forms of complex healthcare provision. The problem is however that it is usually used to justify the processing of a patient's own data for their treatment, and not that of others.[114] This

[111] Quinn (n 88).

[112] Antonia Vlahou and others, 'Data Sharing Under the General Data Protection Regulation' (2021) 77 Hypertension 1029.

[113] It is also worth noting that under Article 9.4 Member States can introduce specific conditions in relation to the processing of genetic data, biometric data, or data concerning health, which could lead to further local disparities and complications. Although, the amended paragraph 37 of the preamble in the Interinstitutional File: 2022/0140(COD) seems to limit this provision: "*Member States may no longer maintain or introduce under Article 9(4) of Regulation (EU) 2016/679 further conditions, including limitations and specific provisions requesting the consent of natural persons, with regard to the processing for secondary use of personal electronic health data under this Regulation, except as referred to in Article 33(5)*."

[114] Indeed Article 9(2)(h) further states that this base is available when outlined by "Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards." The phrasing here seems clearly indicative of an existing treatment relationship between data subject and health care professional. The existence of such a relationship was also highlighted as being of importance under the equivalent legal basis under the Data Protection Directive 95/46/EC which was the processor to the GDPR. See: "Working Document on the processing of personal data relating to health in electronic health records (EHR)" Adopted on 15 February 2007 00323/07/EN WP 131. Available at: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp131_en.pdf

would not be the case with the context provided for by EHDS Article 34 (h). Given this, the authors of this paper would raise serious questions about which legal basis would be appropriate in these circumstances.

Lastly, it is possible to consider the possibility of applying the 'further processing' mechanism under article 6.4 GDPR for the re-use of data for compatible purposes in the context of data permit/data request. Generally speaking, this mechanism, combined with the presumption of compatibility for scientific research (under 5.1(b)) provides very fertile soil for processing of personal data, opening a vast unknown range of potential processing possibilities. That being said, its use would raise many questions, as it has been subject to divergent interpretations[115] and its applicability in practice may prove very difficult if not impossible. How could one conduct the compatibility test in relation to so many different types and sources of data, would the required information on how and on what grounds the data was initially collected even be accessible to the data user?[116] It seems to be too context dependent to offer a viable, practical solution for data processing linked to data requests. Although, at least regarding further use falling under the presumption of compatibility under 5.1(b) GDPR for scientific research, the EDPB may able to provide better insight or at a 'shortened approach' in its long awaited -yet to arrive-guidance on the matter.[117]

5.3. Other key GDPR/Ethical requirements

In addition to having to meet an applicable legal basis, the GDPR poses many other requirements that are likely to require considerable deliberation. Such deliberation will require the commitment of resources on the part of HDABs, not only in terms of the number of personnel but also the expertise which such personnel possess. Whilst it is beyond the scope of this paper to analyse how all potential GDPR requirements could impact the data obtained from the EHDS, it is possible to point out some very clear issues that will go to the heart of the capacity of HDABs' ability to respond to data permit requests. Two of the most important are the need to ensure compliance with the data protection principles of 'data minimization' and 'storage limitation'. Indeed, Article 44 of the EHDS proposal explicitly demands that respect for these two principles in any potential processing be ascertained before a data access permit is granted. What meeting either of these two principles requires in a particular context cannot be defined in abstract terms but requires a case-by-case analysis that will take into account the particular circumstances involved. Performing this exercise is likely to be difficult for several reasons. The authors of this paper would identify two as being particularly pertinent.

The *first* relates to the sheer variety of technical expertise that would be required. This will not only require a knowledge of the data that is being requested but also an understanding of how it will be further processed and for what purposes. Given that HDABs will be receiving requests from a wide range of entities, it is not clear how they will be in a position to make such judgments. The variety of different actors that are likely to be interested in the type of data that the EHDS will offer is likely to be enormous, as is their background and their *raison d'être*. Understanding what 'minimization' will entail in a project involving research on genomic data[118] will for example require very different competencies than a project concerning practical issues in the treatment of diabetes.[119] The authors of this paper would argue that it does not seem feasible that HDABs will be in a position to possess sufficient expertise in order to make such decisions in the variety of cases it is likely they will have to do so. Given this one must ask how HDABs will go about making such an analysis.

The *second* relates to the sheer volume of requests that may be likely to occur. The potential EHDS proposal invoked a very broad spectrum of electronic health data (including but going far beyond EHRs). Given this, it seems possible that Data Access Bodies are likely to receive a high volume of requests from many interested parties. One must also take note that the EHDS proposal envisages that HDABs will have to respond to such requests in a given time period.[120] As a result, it seems likely that HDABs are to be under considerable pressure. Whilst one would hope that Member States ensure they are well enough resourced, they are likely to face the same funding pressures that all publicly funded institutions do, e.g., in which funding may be adequate to ensure they function, but not sufficient to ensure they function perfectly. In cases where HDABs are not sufficiently resourced, the reality may be that they will not have the capacity to look at individual requests in a manner that is seemingly demanded by the EHDS proposal.[121]

The problems are furthermore exacerbated by the fact the HDABs are seemingly required to look at the potential application of Member State law and also assess the "ethical aspects of processing". In terms of the former, this adds a further level of complexity, given the continued heterogeneity of data protection law across European Member States (discussed above in (b)).[122] This situation is made more problematic because Data Access Bodies will have to consider requests from potential recipients based in different member states. As a result, those tasked with carrying out such assessments will not only be expected to master

[115] There is a divided interpretation of 6.4 GDPR. One approach reads article 6.4 as prohibiting the re-use of personal data for compatible purposes, when the data was originally collected/processed on the grounds of consent or a MS/EU law, which can often be the case; though not always, with regard to health data. Another approach does not limit the possibility of using the 'further use' mechanism when the data was initially collected on the basis of consent or a MS/EU law. Seeing instead those references in 6.4 as exceptions to having to conduct the compatibility assessment, taking into account the article 29 WP Opinion of 03/2013 on purpose limitation and the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.

[116] In any event, applying this mechanism would require fulfilling the criteria set out under 6.4 GDRP and paragraph 50 of the GDPR preamble, which will be highly dependent on the context of the processing (in particular the source of data, which may not be the same for all data subjects concerned).

[117] It has been repeated numerous times, but we are still awaiting an opinion form the EDPB on the presumption of compatibility with regard to scientific research: European Data Supervisor, "A Preliminary Opinion on data protection and scientific research", 6 January 2020, p.16; and "EDPB Document on response to the request from the European Commission for clarifications on the consistent application of the GDPR, focusing on health research", adopted on 2 February 2021, p.6, available at: https://edpb.europa.eu/sites/default/files/files/file1/edpb_replyec_questionnaireresearch_final.pdf

[118] Paul Quinn and Liam Quinn, 'Big Genetic Data and Its Big Data Protection Challenges' (2018) 34 Computer Law & Security Review 1000.

[119] 'European Data Law Is Impeding Studies on Diabetes and Alzheimer's, Researchers Warn' <https://www.science.org/content/article/european-data-law-impeding-studies-diabetes-and-alzheimer-s-researchers-warn> accessed 21 September 2023.

[120] Article 46 of the EHDS proposal states "A health data access body shall issue or refuse a data permit within 2 months of receiving the data access application"

[121] It is worth noting that in the Parliament's proposed amendments to Article 44.1, the HDDA body should "ensure that access is only provided to requested electronic health data necessary and relevant for the purpose of processing indicated in the data access application by the data user and in line with the data permit granted." Assessing the necessity of data is clearly a task that legislators envision the HDAA being able to carry out.

[122] This situation is explicitly acknowledged by Article 9(4) of the GDPR which permits Member States to maintain divergent law in order to regulate the processing of health, genetic or biometric data.

the complexities of Member State law in their own country but also potentially all other European Countries. One might ask for example is it realistic to expect a Cypriot HDAB to have expertise in Danish law or vice versa. In terms of assessing the "ethical aspects of processing" this need arguably requires a further level of competence that is in many respects distinct from the other more legally focused tasks that the Data Access Body must perform. This will further add to the organization's burden and complexity of the tasks that these entities must perform by ensuring that they engage expertise in ethics and the social sciences.

6. Conclusion

The European Health Data Space has a broad ambition, not only to make Electronic Health Records more available for primary care but also to make a vast array of secondary data available for a number of purposes, including but not limited to classic forms of research. To this end, the EHDS proposal identifies a number of reasons for which data access permits may be granted. Some of these grounds are notable because they are extremely broad in nature. This includes for 'training or education purposes' or 'development and innovation activities for products or services in the area of public health or social security'. Other equally broad reasons include supporting 'public bodies in the health sector area' or supporting 'training, testing and evaluating of algorithms, including in medical devices.'

As outlined in Section 3, the potential breadth of possible processing operations included within these grounds is noteworthy and may indeed give rise to concerns that HDABs have an enormous discretion to allow access to secondary data. These include the potential to provide health data to a wide range of public bodies and to organizations with commercial motives. Such concerns are further heightened given that the EHDS itself will not in general operate on the basis of the consent but will make use of an opt out mechanism. This raises important questions over how electronic health data will be used and for what purposes. Additionally, further concerns exist over the potential for harm on the individual and societal level through the incorrect use of data. As Section 5 of this paper discusses, however, one of the major guarantors embedded into the EHDS framework is that all processing of personal data planned by data recipients must adhere to the GDPR. That is to say that whilst the EHDS regulation will create new legal bases for Data Access Bodies to collect data and store it, it can only be made available to data recipients where they have a legal basis to process it (and where other requirements posed by the GDPR have been met).

On the face of it, this is an important protection that means effectively that the EHDS itself is not *lex specialis* in terms of creating new legal bases for recipients. Rather it just makes it easier for recipients that already have a legal basis to gain access to electronic health data in the first place. Accordingly, whilst some of the potential grounds for making EHDS data available to recipients appear extremely broad, they should be read in the context of the obligation on the part of the HDABs to ensure that data recipients have a valid basis for processing under the GDPR before they grant a permit. Public sector entities attempting to gain access to data under one of the broad grounds outlined in the EHDS proposal (e.g., for scientific research, innovation or teaching) will still (in order to comply with Article 9 of the GDPR) have to point to further authorization in Member State or Union law, in addition to demonstrating necessity and proportionality of processing. Commercial entities will also have to demonstrate a relevant legal basis. For them, this may be more difficult. Doing so for sensitive forms of data may often be difficult given that there is no equivalent of the 'legitimate interests base' in Article 9 of the GDPR. Given that in the case of data obtained through the EHDS, consent will not be the legal basis of processing, potential commercial recipients will also likely have to demonstrate compliance with a legal basis that requires as a condition authorization in EU or Member State legislation (e.g., the scientific research exception in Article 9(2)(j)). In some Member States, this may be more difficult than in others. Some legislation may demand that research is in the public interest or may only be applicable to certain types of bodies (e.g., public bodies, universities or other publicly funded research organizations). Such a requirement will place an important limitation on various commercial entities in a number of Member States that, though seemingly having a processing purpose that falls within one of the grounds within Article 34 of the EHDS proposal, will nonetheless sometimes find it difficult to secure a legal basis in their respective Member State's law permitting processing under the GDPR.

In addition to such substantive legal problems, a number of practical problems become apparent upon a closer examination of the roles that HDABs are expected to undertake. These will seemingly require a vast away of complex expertise and at a scale that is sufficient for the task. This will potentially include for example the ability not only to understand Member State law in their own jurisdiction but also potentially in others given that requests for a data access permit can be made from another state within the EU. How HDABs can realistically be expected to do this given that there are 27 different jurisdictions within the EU is not clear. One possible actor that could play an important role in addressing such issues is the EHDS board,[123] though how it could allow HDABs to understand the law in all other Member States is admittedly hard to envisage.

In addition to this, HDABs will be tasked with ensuring that both the data minimization and storage limitation data processing principles will be complied with for proposed processing operations. As discussed in Section 5 of this paper, making such a determination is not a simple or abstract task but will require both expertise in the type of processing involved (which may require other forms of non-legal expertise e.g., scientific, computational) and the particular context in question. Given the variety and number of requests that HDABs may receive, it is difficult to imagine how HDABs will be able to possess such a capacity given the likely cost in terms of personnel.

Given the issues raised within this paper, the authors would suggest that the need to ensure GDPR compliance by data recipients is an important protective pillar built into the EHDS architecture, but one which should not be overestimated in terms of its protective effects. This vast array of requirements placed upon HDABs raises serious concerns about the feasibility of what they are being asked to do. Given the issues raised within this paper, the authors would suggest that in considering the protections offered by the EHDS framework whilst the need to ensure GDPR compliance is important, it should not be overestimated. In particular, if it is not feasible for HDABs to perform an in-depth analysis themselves of GDPR/ethical compliance, one has to wonder whether there is not a risk that they will in reality become charged with carrying out more administrative functions whereby they are limited to ensuring that the party requesting the data has themselves performed an analysis of how they would comply with the GDPR (in a way that is arguably often the case now with data protection impact assessments). This would represent an unfortunate development given the important role of the GDPR as a backstop or guarantor in ensuring the creation of the EHDS does not bring about harm to data subjects. Without this guarantee that data recipient requests will be examined thoroughly for *inter alia* compliance with the GDPR, serious questions concerning the ability of data subjects to trust the EHDS framework will arise. This could have severe consequences, in particular under a model (which is currently envisaged) that does not foresee a central role for consent of the data

[123] As the EHDS proposal states on page 19, the regulation will create "the 'European Health Data Space Board' ('EHDS Board') that will facilitate the cooperation between digital health authorities and health data access bodies, in particular the relation between primary and secondary use of electronic health data. Dedicated sub-groups such as on primary use of electronic health data and on secondary use of electronic health data may be formed to focus on specific issues or process. The Board will be tasked with promoting the collaboration between digital health authorities and health data access bodies."

subject. History is full of examples of where the misuse of health data has harmed the trust of healthcare users. Without such trust, the risk exists that patients may engage in forms of health care avoidance, which could have negative consequences for their health.

Declaration of competing interest

No financial/personal interest or belief that could affect the author's objectivity.

Data availability

No data was used for the research described in the article.

Further readings

[1] Binns R, Veale M. Is that your final decision? Multi-stage profiling, selective effects, and Article 22 of the GDPR. Int Data Privacy Law 2021:11.
[2] Bovenberg J. How to Fix the GDPR's frustration of global biomedical research. Science (1979) 2020;370:40.
[3] Bradford L., Aboy M., Liddell K. COVID-19 contact tracing apps: a stress test for privacy, the GDPR, and data protection regimes. J Law Biosci LSAA034 2020;7.
[4] Callahan A. Medical device surveillance with electronic health records. NPJ Dig Med 2019;2:1.
[5] Cohen IG. The European artificial intelligence strategy: implications and challenges for digital health. Lancet Dig Health 2020;2:e376.
[6] Davies W. The happiness industry: how the government and big business sold us well-being. Verso Books; 2015.
[7] Defourny J, Nyssens M. Social enterprise in Europe: recent trends and developments. Soc Enterp J 2008;4:202.
[8] Defourny J, Nyssens M. Social enterprise in Europe: at the crossroads of market, public policies and third sector. Policy Soc 2010;29:231.
[9] Eichler H-G. Data rich, information poor: can we use electronic health records to create a learning healthcare system for pharmaceuticals? Clin Pharm Therap 2019; 105:912.
[10] 'European Data, Law is impeding studies on diabetes and Alzheimer's, researchers warn' https://www.science.org/content/article/european-data-law-impeding-studies-diabetes-and-alzheimer-s-researchers-warn accessed 21 September 2023.
[11] European Commission, A European strategy for data (Communication) COM (2020) final https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0066 accessed 17th Apr 2023.
[12] European Commission, Communication from the commission to the European parliament, the Council, the European economic and social committee and the committee of the regions, A European strategy for data https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0066.COM (2020) 66 final, accessed 17 Apr 2023.
[13] European Commission, Data Governance Act Explained https://digital-strategy.ec.europa.eu/en/policies/data-governance-act-explained accessed 17th January 2023.
[14] European Commission. Staff working document on data spaces. 2023. https://digital-strategy.ec.europa.eu/en/library/staff-working-document-data-space accessed 17th Apr.
[15] Gordon WJ, Stern AD. Challenges and opportunities in software-driven medical devices. Nat Biomed Eng 2019;3:493.
[16] Hall JA. Transparency of genetic testing services for "health, wellness and lifestyle": analysis of online prepurchase information for UK consumers. Eur J Hum Genet 2017;25:908.
[17] Hansen W.J. and others, 'Assessment of the EU Member States' Rules on Health Data in the Light of GDPR'.
[18] Hasan E. Chapter 29 - Examples from administrative claims data and electronic health records. In: Cynthia J. Girman, Mary Elizabeth Ritchey, editors. Pragmatic randomized clinical trials. Academic Press; 2021. https://www.sciencedirect.com/science/article/pii/B9780128176634000027 accessed 28 February 2023.
[19] Hoofnagle CJ, Van Der Sloot B, Borgesius FZ. The European Union general data protection regulation: what it is and what it means. Inf Commun Technol Law 2019;28:65.
[20] Jabri S. Artificial intelligence and healthcare: products and procedures. In: Wischmeyer Thomas, Rademacher Timo, editors. Regulating artificial intelligence. Springer International Publishing; 2020. doi:10.1007/978-3-030-32361-5_14. accessed 15 February 2023.
[21] Kalokairinou L, Borry P, Howard HC. Regulating the advertising of genetic tests in Europe: a balancing act. J Med Genet 2017;54:651.
[22] Kamara I. and De Hert P., 'Understanding the balancing act behind the legitimate interest of the controller ground: a pragmatic approach' (8 August 2018) https://papers.ssrn.com/abstract=3228369 accessed 20 September 2023.
[23] Kiseleva A., 'AI as a medical device: is it enough to ensure performance transparency and accountability in healthcare?' (8 November 2019) https://papers.ssrn.com/abstract=3504829 accessed 14 September 2022.
[24] Kiseleva A., Kotzinos D., De Hert P. 'Transparency of AI in healthcare as a multilayered system of accountabilities: between legal requirements and technical limitations'. Front Artif Intell 2022;5. https://www.frontiersin.org/articles/10.3389/frai.2022.879603 accessed 14 September 2023.
[25] Kramcsák PT. Can legitimate interest be an appropriate lawful basis for processing artificial intelligence training datasets? Comput Law Sec Rev 2023;48:105765.
[26] Marcus J.S. 'The European health data space'. SSRN Electron J 2022. https://www.ssrn.com/abstract=4300393 accessed 27 January 2023.
[27] Martin-Sanchez FJ. Secondary use and analysis of big data collected for patient care. Yearb Med Inform 2017;26:28.
[28] McLennan S. Practices and attitudes of bavarian stakeholders regarding the secondary use of health data for research purposes during the COVID-19 pandemic: qualitative interview study. J Med Internet Res 2022;24:e38754.
[29] McLennan S, Celi LA, Buyx A. COVID-19: putting the general data protection regulation to the test. JMIR Public Health Surveill 2020;6:e19279.
[30] Mourby M. Governance of academic research data under the GDPR—Lessons from the UK. Int Data Privacy Law 2019;9:192.
[31] Niemiec E. Will the EU medical device regulation help to improve the safety and performance of medical, 8. AI devices? Dig Health; 2022. 20552076221089079.
[32] O'Connor S. Secondary data analysis in nursing research: a contemporary discussion. Clin Nurs Res 2020;29:279.
[33] Quinn P. The anonymisation of research data—A pyric victory for privacy that should not be pushed too hard by the EU data protection framework? Eur J Health Law 2017;24:347.
[34] Quinn P. Research under the GDPR - a level playing field for public and private sector research? Life Sci Soc Policy 2021;17:4.
[35] Quinn P. Research under the GDPR - a level playing field for public and private sector research? Life Sci Soc Policy 2021;17:4.
[36] Quinn P, Quinn L. Big genetic data and its big data protection challenges. Comput Law Sec Rev 2018;34:1000.
[37] Rajaram A. Training medical students and residents in the use of electronic health records: a systematic review of the literature. J Am Med Inform Assoc: JAMIA 2020;27:175.
[38] Schreyögg J. Defining the "Health Benefit Basket" in nine European countries. Eur J Health Econ 2005;6:2.
[39] Tacconelli E. Challenges of data sharing in European Covid-19 projects: a learning opportunity for advancing pandemic preparedness and response. Lancet Reg Health - Eur 2022;21:100467.
[40] Vlahou A. Data sharing under the general data protection regulation. Hypertension 2021;77:1029.
[41] Vukovic J. Enablers and barriers to the secondary use of health data in Europe: general data protection regulation perspective. Arch Public Health 2022;80:115.
[42] Yan M. Mobile apps for healthy living: factors influencing continuance intention for health apps. Technol Forecast Soc Change 2021;166:120644.