

Louvain School of Management

The European Health Data Space

How is the European Union attempting to create a single market for innovation whilst guaranteeing the right to protection of sensitive data?

Author(s): Sophie Delacroix
Supervisor(s): Jean-Christophe Defraigne
Academic year 2025-2026
Dissertation for the Advanced Master in European Business and
Economic Policy
Daytime schedule

DECLARATION

The declaration below is **mandatory and must appear on the first page (after the front page) of your master's thesis.**

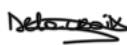
STATEMENTS ON YOUR USE OF GENERATIVE AI

Confirm the following statements:

Statements on responsible use of generative AI	Your answer
The content of my/our master's thesis is my/our original output, even if I/we used generative AI to help prepare it.	☒ Yes ☐ No
I/we master the theories, tools and methods that I/we use for the thesis.	☒ Yes ☐ No
I/we verified that the output presented in the thesis is accurate and valid, and that it contains no hallucination, no false reference, etc.	☒ Yes ☐ No
I/we acknowledge that I/we master the final output and that I am/we are able to explain it and answer questions about it.	☒ Yes ☐ No
I/we made sure not to provide generative AI tools with access to confidential data or information	☒ Yes ☐ No

SIGNATURE

Sign your declaration:

☐ Author last name, first name(s)	Date	Signature
1 DELACROIX SOPHIE	23 / 05 / 2016	
2		

NOTE

For this document, DeepL has been used to propose formulations, but the text is original, except the extracts explicitly mentioned as coming from other sources, which are mentioned in footnotes.

Acknowledgements

I would like to thank my thesis supervisor Mr. Defraigne for his guidance and suggestions throughout the writing of this thesis, as well as for his availability and support during this process.

I would also like to thank my family and friends for their unconditional support and patience during these years of study.

Table of Contents

Introduction	1
Part I — The EHDS: the driving force behind sovereignty and innovation	3
Chapter 1 — From fragmentation to unification: removing barriers to medical innovation	3
Chapter 2 — The HealthData@EU architecture: uniting twenty-seven systems without merging them.....	5
Part II — The challenge of trust: the ethical and legal architecture of protection. 8	
Chapter 1 — A hybrid legal framework: the relationship between the GDPR and the EHDS	8
Part III — European digital sovereignty put to the test by the law.....	12
Chapter 1 — Case law as a battleground: from Schrems to the Health Data Hub.....	12
Chapter 2 — The US cloud at the heart of European healthcare systems: a structural dependency.....	17
<i>1. The EHDS as a structural solution: the residency requirement and its implications</i>	<i>20</i>
Part IV — The American perspective: economic interests and transatlantic tensions	22
Chapter 1 — US stakeholders and the EHDS: between opportunity and resistance...	22
Part V — The European perspective: between shared ambition and national differences	27
Chapter 1 — Twenty-seven Member States, twenty-seven speeds: the European divide over the eHDS	27
General conclusion : The EHDS or Europe’s gamble on trust.....	32
Recap of the central tension and summary of the analysis	32
Direct answer to the research question	32
A critical look: the EHDS – between ambition and fragility	33
Limitations of the study	34
Outlook and prospects	34

Bibliography	36
---------------------------	-----------

Introduction

In the twenty-first century, technology has permeated every aspect of our lives, and the medical field is no exception. The digitisation of health records now enables the longitudinal collection of patients' medical data, opening up unprecedented opportunities for research and care. However, this ease of access raises significant ethical, legal and security issues. Indeed, national platforms such as masanté.be in Belgium aggregate sensitive data, the collection and reuse of which, over time and with technological developments, call into question the validity of the initial consent. (*Bévière-Boyer, 2023*)

It is against this backdrop that the General Data Protection Regulation (GDPR), which came into force in 2018, laid the foundations for a European protection framework. Its fundamental rights (access, the right to be forgotten, portability, and the right to object) have restored citizens' theoretical control over their data. However, the GDPR has paradoxically proved to be a hindrance to medical innovation. By granting Member States considerable leeway for interpretation, notably through Article 9(4), it has led to regulatory fragmentation that makes cross-border data sharing extremely complex. Added to this is the virtual absence of technical interoperability between national hospital systems, a requirement for individual consent to be renewed for each new study, and the lack of a common database at European level, whereas the United States and China possess vast amounts of integrated data, which are the real driving force behind the development of medical artificial intelligence. (*Règlement Général Sur La Protection Des Données, 2016*) (*The European Union General Data Protection Regulation: What It Is and What It Means**, 2019)

The European Health Data Space (EHDS), adopted by Regulation (EU) 2025/327 of 11 February 2025, addresses these four shortcomings. It harmonises rules across Member States, imposes technical interoperability standards on healthcare providers, creates a legal framework for the secondary use of anonymised data, and lays the foundations for a common European database. In doing so, it addresses two converging urgent needs. Firstly, the economic urgency: the Draghi report of September 2024 sounded the alarm over Europe's competitive lag behind the United States and China, noting that a large proportion of European data remains unusable due to a lack of accessibility, which

accelerates the brain drain and capital flight to less restrictive jurisdictions. Secondly, the ethical and security imperative: the healthcare sector is among the targets most exposed to cyberattacks, making systemic data security imperative. (*Drumpt et al., 2025*)

The central question of this work is therefore as follows: how is the European Union striving to create a single market for innovation whilst guaranteeing its citizens' right to the protection of sensitive data? Answering this question requires analysing a fundamental tension: that between the imperative of data availability, necessary for competitiveness and research, and the imperative of privacy protection, a cornerstone of European democratic values.

This study adopts a qualitative approach structured in three parts. The first analyses the architecture of the EHDS and how it seeks to remove barriers to medical innovation whilst building a common infrastructure. The second examines the hybrid legal framework linking the GDPR and the EHDS, focusing on the balance between individual rights and the public interest. The third part, which will be the subject of further development, will address European digital sovereignty in the face of dependence on US infrastructure, transatlantic geopolitical tensions, and the case law that is redefining the boundaries of applicable law.

Part I — The EHDS: the driving force behind sovereignty and innovation

Chapter 1 — From fragmentation to unification: removing barriers to medical innovation

1.1 — The current situation: European data in silos

Article 9 of the GDPR establishes a principle prohibiting the processing of health data, subject to specific exceptions. Paragraph 4, which allows Member States to introduce additional conditions, has led to profound fragmentation across the European landscape. (*Règlement Général Sur La Protection Des Données*, 2016) Two examples illustrate the scale of this disparity. Until the introduction of the EHDS, Germany organised healthcare at the level of its sixteen Länder, each of which required explicit and specific consent for every new study, making any transnational research project administratively complex and daunting. (*OECD*, 2019) In contrast, Estonia has adopted a default opt-out model: data is shared for research purposes unless the citizen explicitly objects, and they can also view the history of access to their information. (*TEHDAS Estonia Country Visit Factsheet*, 2022)

This fragmentation has measurable economic consequences. According to the European Federation of Pharmaceutical Industries and Associations (EFPIA), funding for research and development in Europe has fallen significantly over the past two decades, in contrast to trends in the US and China. (*The Pharmaceutical Industry in Figures*, 2025) (*Clinical Trials*, 2026) Pharmaceutical companies and research institutes are directing their investments towards jurisdictions where access to data is most seamless, causing lasting harm to the European scientific ecosystem. Health data must therefore be viewed for what it is: a non-rival good, whose social value increases with the number of simultaneous uses. As Jones and Tonetti (2020) have shown, the social benefits associated with data increase as it is shared, making its compartmentalisation structurally counterproductive. (*Jones & Tonetti*, 2020)

The comparative advantage that Europe could leverage is precisely the longitudinal nature of its health data. (*Value of Data Report*, 2020) Unlike in the United States, where medical coverage is fragmented and records are scattered across private insurers, European

healthcare systems generate data that often covers the entirety of a patient's life. This temporal depth is invaluable for long-term epidemiological research and for training medical artificial intelligence models free from geographical or demographic biases. It is this asset that the EHDS aims to harness. (*Règlement (UE) 2025/327 du Parlement européen et du Conseil*, 2025)

1.2 — The EHDS response: a model based on the Finnish experience

The EHDS requires each Member State to designate a single body for access to health data, the Health Data Access Body (HDAB), whose model is directly inspired by the Finnish Findata system, which has been operational since 2019–2020. (*Annual Report 2025*, 2026) This one-stop shop centralises requests for access to data from all national healthcare institutions. Researchers no longer need to negotiate separately with each hospital or region: a single request to the national HDAB is sufficient to cover the entire country. (*Services and Instructions*, 2026)

The key principle of this model is ‘view-only’ access. Researchers access the data in a dedicated secure environment, carry out their analyses there, but can only extract their results; this is done after verification by the competent body that these results do not allow for any re-identification. This principle of ‘data access rather than data release’ is a direct response to public concerns about the commercialisation of medical data. The data does not circulate: it is the researcher who comes to it. (*Règlement relatif à l'espace européen des données de santé - Public Health*, 2026)

Chapter 2 — The HealthData@EU architecture: uniting twenty-seven systems without merging them

2.1 — The HealthData@EU platform and the HDAB network

The aim of the EHDS is not to create a centralised repository for all European health data; such centralisation would constitute an unacceptably attractive target for cyberattacks. Rather, the aim is to build a distributed infrastructure, the HealthData@EU platform, which connects national HDABs and enables accredited researchers to locate, request and access data available in the various Member States from a single entry point. (*Règlement (UE) 2025/327 du Parlement européen et du Conseil*, 2025)

In practical terms, a researcher from a university, a public research body or an authorised pharmaceutical company authenticates themselves on the platform using a high level of security, for example via an electronic ID card. They consult the catalogue of available data by country and by category, then submit their request to the relevant HDAB. The HDAB assesses the scientific legitimacy of the project, verifies its compliance with the purposes authorised by the EHDS (research, innovation, public policy development, public health) and explicitly excludes purely commercial purposes (advertising, insurance risk assessment, recruitment decisions). If the request is accepted, the researcher accesses the data in a Secure Processing Environment (SPE), remotely and without the possibility of downloading. The list of granted accesses is published publicly, ensuring the system's transparency. (*HealthData@EU Central Platform - HealthData@EU*, n.d.) (*Directorate-General for Health and Food Safety (European Commission)*, 2026)

Progress in establishing HDABs varies by country. Some already have operational bodies: Findata in Finland, the Health Data Hub in France. (*Un Projet Européen Pour Mieux Soigner, Innover et Prévenir.*, 2025) (*Règlement (UE) 2025/327 du Parlement européen et du Conseil*, 2025) (*Services and Instructions*, 2026) Others have designated their HDAB but have not yet made it fully operational, such as the Belgian Health Data Agency. Finally, others, such as Italy with its highly regionalised healthcare structure, face additional structural challenges. The deadline set by the EHDS for the designation of HDABs is March 2027. (*Murgia et al.*, 2025) (Health Data Agency, n.d.)

2.2 — *Semantic and technical interoperability: a prerequisite*

The networking of national data is only valuable if that data is comparable. To this end, the EHDS imposes a three-fold standard. The SNOMED CT (Systematized Nomenclature of Medicine, Clinical Terms) nomenclature standardises the coding of diseases across all member countries, enabling a French doctor to immediately understand a record written in Italy, or an algorithm to process Hungarian and Spanish data without the need for translation. (*Patient Summary Guideline (Release 3.1)*, 2024) (*La SNOMED CT et le NRC français*, 2026) LOINC (Logical Observation Identifiers Names and Codes) applies the same principle to laboratory test results. (*LOINC*, 2026) (*GUIDELINE on the Electronic Exchange of Health Data under Cross-Border Directive 2011/24/EU Laboratory Results*, 2023) The EEHRxF (European Electronic Health Record Exchange Format) standardises the structure and content of exchangeable medical records, defining the documents that must be systematically accessible in an interoperable format. (*Règlement (UE) 2025/327 du Parlement européen et du Conseil*, 2025) (*What Is EHRxF?*, 2026)

For research, the OMOP (Observational Medical Outcomes Partnership) model requires data to be structured identically across all member countries, facilitating their processing by analytical tools and artificial intelligence. (OHDSI, 2026) (*Omop-Cdm*, 2025) These requirements extend to medical software publishers, who can no longer lock in their customers by making data transfer prohibitively expensive: standardisation mandates effective portability, transforming the theoretical right enshrined in the GDPR into operational reality.

2.3 — *Data security: a trusted architecture*

Data protection within the EHDS is based on several complementary layers of security. Systematic pseudonymisation or anonymisation is carried out by the HDAB prior to any access by a researcher. The ‘trusted third party’ principle strictly separates identity holders from data holders: the organisation that knows who the patient is does not know what they have, and vice versa. An output checking process, combining algorithmic and human checks, ensures that no result extracted from the SPE would allow an individual to

be re-identified through deduction or cross-referencing. (“Package 5,” n.d.)

The regulation also mandates differential privacy: a calibrated statistical disturbance is intentionally introduced into the data, making re-identification through cross-referencing of separate databases impossible. (CNIL, n.d.) (*Differential Privacy | Harvard University Privacy Tools Project*, n.d.) ENISA, the European Union Agency for Cybersecurity, oversees the entire system by applying a ‘zero trust’ policy: every access request is subject to independent verification, including from users who are already authenticated. (*What Is Zero Trust For the Cloud?*, n.d.) (*Règlement (UE) 2025/327 du Parlement européen et du Conseil*, 2025) Finally, and this is a crucial point that will be explored in Part III, the Regulation requires that all data processed under the EHDS be stored within the European Union, as a direct response to the legal risks posed by the US Cloud Act of 2018. (*Cloud Act et RGPD*, 2024) (*Règlement (UE) 2025/327 du Parlement européen et du Conseil*, 2025)

Part II — The challenge of trust: the ethical and legal architecture of protection

Chapter 1 — A hybrid legal framework: the relationship between the GDPR and the EHDS

1.1 — The GDPR, an indispensable foundation

Before analysing what the EHDS brings, it is worth highlighting what it does not call into question. The GDPR remains fully applicable. The EHDS is adopted ‘without prejudice’ to Regulation 2016/679, which it explicitly cites on multiple occasions. It is not a replacement: it is a *lex specialis* that clarifies, in the field of healthcare, the exceptions permitted by Article 9 of the GDPR. (*Règlement Général Sur La Protection Des Données*, 2016) Where the GDPR had created a largely theoretical right to data portability (as each hospital was free to choose its own software, data remained *de facto* non-transferable), the EHDS provides the technical infrastructure it lacked to make this a reality.

1.2 — From individual consent to a legal obligation: a paradigm shift

The most fundamental change brought about by the EHDS concerns the legal basis for data processing for research purposes. The GDPR relied primarily on the patient’s explicit consent (Article 6(1)(a)). This model led to what the medical world calls ‘consent fatigue’: researchers paralysed for months collecting signatures, scientific cohorts skewed by refusals, and the practical impossibility of conducting longitudinal studies spanning decades without having to re-seek consent from thousands of patients. (*Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL*, 2025)

The EHDS marks a fundamental shift. For the secondary use of anonymised data, the Regulation replaces the logic of consent with that of legal obligation (Article 6(1)(c) of the GDPR) and public interest (Article 6(1)(e)). Data holders (hospitals, clinics, software publishers) are now legally obliged to make their data available to the national HDAB. This sharing is no longer a contractual decision or a favour granted: it is a regulatory requirement. (*Règlement (UE) 2025/327 du Parlement européen et du Conseil*, 2025)

This removal of the requirement for individual consent is offset by a three-fold safeguard. Firstly, the data is only accessible after it has been fully anonymised by the HDAB, making it theoretically impossible to link it to an individual. Secondly, an unconditional right to object (opt-out) is maintained: any citizen may at any time prohibit the use of their data for secondary purposes, without having to justify their decision. Thirdly, the authorised purposes are strictly defined: no purely commercial, advertising, insurance or employment-related use may be permitted. Protection no longer relies on a signature at the bottom of a form that is often poorly understood, but on a systemic legal and technical framework. (*Règlement (UE) 2025/327 du Parlement européen et du Conseil*, 2025)

1.3 — Redefining the chain of responsibility

The EHDS also reshapes the structure of legal liability. Under the standard framework of the GDPR, the chain of control is linear: the data controller, usually the hospital or medical practice, defines the purposes of the processing and is accountable for it. With the EHDS and cross-border data flows, this approach is no longer sufficient. In the event of a data breach during an exchange between two Member States, who is liable? The regulation introduces shared liability: if the breach occurs at the level of the European technical infrastructure (MyHealth@EU), liability shifts to the Commission or the Member States managing the national contact points. If the data is inadequately secured at source, the holding hospital remains liable. This clarification is essential to overcome the reluctance of healthcare stakeholders to share data for fear of being held liable for technical errors occurring outside their sphere of control. (*Règlement (UE) 2025/327 du Parlement européen et du Conseil*, 2025)
(*RÈGLEMENT (UE) 2016/ 679 DU PARLEMENT EUROPÉEN ET DU CONSEIL*, 2016)

At the centre of this chain are the HDABs, which act as legal trusted third parties. It is their responsibility to carry out a prior check that any research project complies with the principles of the GDPR (relevance, lawfulness, purpose limitation) before issuing a ‘data permit’. This intermediary role relieves the hospital of the legal complexities involved in assessing scientific projects. Once the permit is granted, responsibility transfers to the researcher for the duration of their access to the SPE. This clear chain of responsibility

forms the foundation of trust essential to the social acceptability of the entire system. (*Règlement (UE) 2025/327 du Parlement européen et du Conseil*, 2025)

1.4 — The sanctions regime: the EHDS as the rule, the GDPR as the enforcement mechanism

Finally, the credibility of the system rests on its enforcement regime. The EHDS has not created a new scale of penalties: it has modelled its own on that of the GDPR. Article 87 of Regulation 2025/327 provides for administrative fines of up to €20 million or 4% of global annual turnover, whichever is higher. This structure is deliberate: the EHDS provides the ‘traffic rules’ (the obligations to share and secure data) whilst the GDPR provides the ‘muscle’, that is to say, the sanctioning power of national data protection authorities. This convergence ensures that the most powerful players, such as large pharmaceutical companies or cloud operators, will not be able to treat the obligations of the EHDS as mere administrative constraints to be circumvented. (*Règlement (UE) 2025/327 du Parlement européen et du Conseil*, 2025) (*Espace Européen Des Données de Santé (EEDS) | EUR-Lex*, 2026) (*European Health Data Space Regulation*, 2025) (Kjeldahl Bjerregaard Bjerrum & Husum, 2025)

The first two parts analysed how the EHDS builds a medical innovation architecture based on a legal and technical balance between data availability and protection. However, this European framework comes up against a geopolitical reality that the regulation itself cannot fully resolve: Europe's dependence on digital infrastructures whose legal sovereignty lies outside the scope of European law.

The third part, to be developed, will address three complementary dimensions. Firstly, the issue of the actual storage of European health data: to what extent do the servers of major US cloud operators (Amazon Web Services, Microsoft Azure, Google Cloud) host data that is, in theory, subject to European law, but in practice exposed to the US Cloud Act of 2018? Secondly, the case law that has gradually reshaped this landscape: from the invalidation of the Safe Harbour by the Court of Justice of the European Union in the Schrems I judgment (2015) to the invalidation of the Privacy Shield in the Schrems II judgment (2020), right through to the landmark cases of the French Health Data Hub, which was forced to leave Microsoft Azure, and Doctolib, whose continued use of AWS was conditionally approved by the Council of State. Thirdly, the positions and interests of US stakeholders (technology companies, the pharmaceutical industry and institutional lobbies such as AmCham EU) in the face of a regulation that is profoundly reshaping the conditions of access to one of the world's richest data markets.

Part III — European digital sovereignty put to the test by the law

Chapter 1 — Case law as a battleground: from Schrems to the Health Data Hub

As we have seen, the GDPR, supplemented by the EHDS, demands absolute security regarding the use and storage of data, all the more so for health data, which is the very essence of our personhood. (*Cloud Defence*, 1016) However, European servers are often not powerful enough to store such large volumes of data, which is why much of the European Union's data is stored on US servers. However, the question arises as to the reliability of these servers in terms of security, partly due to the US Cloud Act. This US legislation, which allows US authorities to access data stored by US-based providers, conflicts with the absolute security required by the GDPR and the EHDS. (*Cloud Act et RGPD*, 2024) This is not a new concern, and there have already been several court rulings on the matter. We will analyse a few of these, including the two Schrems judgments, the 'Health Data Hub' or 'Microsoft Azure' case, and the 'Doctolib' case.

The landmark precedent: the Schrems I judgment (CJEU, 2015)

In 2015, the Court of Justice of the European Union (CJEU), which is the judicial institution of the European Union, ruled against the 'Safe Harbour', an agreement with the United States concerning compliance with data protection standards, in the 'Schrems I' or 'C-362/14' of 6 October 2015. (*Cour de justice de l'Union européenne*, n.d.) (*Affaire C-362/14*, 2015) It was a law student, Maximilian Schrems, who took Facebook Ireland to court in 2013 because the platform was transferring its users' personal data to its parent company based in the United States. However, according to the student, US law did not provide sufficient protection for European citizens and their data. Indeed, at that time, there was an agreement between the United States and the European Union regarding data protection, known as the 'Safe Harbour'. This was a system whereby US companies self-certified their compliance with European data protection requirements. (*The EU-US Safe Harbour Agreement*, 2012) The CJEU then ruled that the student was right to challenge this system because the US authorities still had de facto access to the

data if national security so required, and because a European citizen had no effective legal remedy available in the United States to ascertain the context in which their data was being processed or to object to it; which is in direct contradiction with Articles 7 and 8 of the Charter of Fundamental Rights of the European Union. (*Charte Des Droits Fondamentaux de l'Union Européenne*, 2000)

This ruling is significant because it established that the protection of personal data requires structural safeguards and not merely protection based on the good faith of a third country outside the European Union. Following this ruling, all US companies suddenly found themselves without a legal basis for transferring data to their parent companies. The European Union and the United States therefore attempted to put in place a second agreement, the 'Privacy Shield', in 2016.

The escalation: the Schrems II ruling (CJEU, 2020)

The 'Privacy Shield' was once again a system where companies self-certified their compliance with European data protection requirements, but they had to make a public commitment to the US Department of Commerce, and there were certain key principles to be observed in addition to this in order to address the arguments that had led to the annulment of the 'Safe Harbour'. These key principles were that European citizens had to be informed about the collection of their information, they had to be able to object to the sharing of their data, companies had to take measures to ensure data security against leaks or unauthorised access, and they had to allow citizens to access and amend their data. (*EU-U.S. Privacy Shield*, 2016)

However, Schrems was once again unconvinced of the effectiveness of these measures and challenged the mechanism once more on the grounds that the US authorities could still access this data. The CJEU, in the 'Schrems II' or 'C-311/18' judgment of 16 July 2020, also invalidated the effectiveness of this agreement for the same reasons as the 'Safe Harbour' scheme, namely that US authorities still had access to the data on grounds of national security and that, despite the 'ombudsperson' established within the US Department of State, this still did not provide European citizens with an effective legal remedy, as the 'ombudsperson' was not sufficiently neutral and had no binding authority. (*C-311/18*, 2020)

What does survive from this agreement, however, are the ‘standard contractual clauses’ or ‘SCCs’, which are contractual clauses imposed by the European Commission on European companies wishing to transfer data outside the European Union if the recipient country guarantees a level of security equivalent to that guaranteed by the European Union. (*Standard Contractual Clauses (SCC) - Commission européenne*, 2021) These clauses are subject to a strict condition, namely the ‘transfer impact assessment’ (TIA). (*International Data Transfers | European Data Protection Board*, n.d.) It is an obligation for the data exporter to ensure that the recipient country guarantees an equivalent level of security for data protection. This is therefore virtually impossible to ensure given the ‘Cloud Act’ or ‘Clarifying Lawful Overseas Use of Data Act’ adopted in 2018 by the United States, since this Cloud Act, as explained previously, allows US authorities to demand data stored on servers belonging to US providers.

The Health Data Hub v Microsoft Azure case: the European test case in the healthcare sector

The Schrems II ruling has therefore left the issue of data transfer security entirely unresolved. One instance where this has posed a practical problem is that of the ‘Health Data Hub’. The Health Data Hub is a platform created in France in 2019 to collate all health data and make anonymised data easily accessible for primary and secondary use; it is, in fact, the HDAB chosen by France. (*FAQ in English | Health Data Hub*, n.d.) When it was set up, Microsoft Azure, an American company, was chosen as the hosting provider. (*Microsoft Corporation | Lobbyfacts*, 2025) Following the Schrems II ruling, companies have once again lost the right to transfer data to their parent companies. This obviously applies to Microsoft Azure as well, particularly as Microsoft Azure is an American company and is therefore subject to the Cloud Act. Associations such as the ‘Conseil National du Logiciel Libre’ (CNLL) have therefore taken the matter to the Council of State to challenge this ongoing collaboration, which contravenes the new Schrems II ruling. The CNIL, or ‘Commission nationale de l’informatique et des libertés’, which is the French national data protection authority, concludes that transferring data to Microsoft would therefore be illegal as things stand. The CNIL remains the competent authority, as the national authority, to examine a transfer and prohibit it if security is not guaranteed, in accordance with the Schrems I ruling.

The Council of State heard these arguments but decided not to immediately suspend the use of Microsoft in the midst of a health crisis, justifying this on the basis of Article 49(1)(d) of the GDPR, which allows for an exemption if the public interest so requires. The platform will, however, have to migrate to another hosting provider within a reasonable timeframe. It is in this context that Health Data Hub has decided to switch providers, moving to Scaleway, part of the Iliad group, a French provider. This cloud is less powerful than its American counterparts but has the advantage of compliant with European standards and not subject to the US Cloud Act. As discussed previously, France is one of the designated national HDABs and a source of inspiration for the EHDS. This example demonstrates that, whilst it took France several years to establish a sustainable system compliant with GDPR requirements, the challenge ahead looks daunting for the EHDS, which must bring together the 27 Member States of the European Union.

The Doctolib case: the legal nuance

A similar case, occurring at around the same time, also took place in France; this is the ‘Doctolib’ case. Doctolib is a French platform created to facilitate the booking of appointments between patients and doctors. (*Définition | Doctolib*, 2025) In 2021, during the COVID-19 pandemic, the French government entered into a partnership with the platform to facilitate the booking of appointments for COVID-19 vaccination. Certain associations, drawing a parallel with the Health Data Hub case and given that the Schrems II ruling had already been handed down, challenged this partnership before the French Council of State, highlighting the same privacy concerns as in the Health Data Hub case, since the platform is hosted on ‘Amazon Web Services’ (AWS), an American company subject to the Cloud Act. However, this case law introduces a nuance compared to the cases previously discussed, as the Council of State did not condemn this partnership. It distinguished it from the Health Data Hub case for three main reasons. Firstly, the data stored by Doctolib did not consist of sensitive medical data, as it comprised contact details, names and dates. Secondly, an independent third party was responsible for end-to-end encryption of the data, which prevented AWS and the US authorities from accessing the data directly. And finally, this data was hosted on servers located in France, which contractually obliged AWS to deny access to the US authorities and to inform Doctolib if such a request had been made.

This case therefore introduces a nuance regarding the use of US cloud services. However, in this instance, the hosting provider had been chosen for its efficiency, whilst acknowledging that the data in question was not the most sensitive. In the case of the EHDS, the data will be sensitive medical data and therefore, despite strict contractual clauses or significant precautions such as end-to-end encryption, the question arises as to whether this case law can be applied within the context of the EHDS.

The Data Privacy Framework (2023): solution or respite?

Following the failure of Safe Harbour and the Privacy Shield, the European Union and the United States sought to negotiate a new agreement in order to continue collaborating. Under this agreement, concluded in July 2023, the United States ensures a level of security substantially equivalent to that established by the European Union. It adds two safeguards, notably that US authorities may only access data in a proportionate manner and where genuinely necessary for national security, and that companies collecting data are subject to stricter rules. In addition to this, a redress mechanism for European citizens has been put in place. A European citizen who has doubts about the lawfulness of the processing of such data may first lodge a complaint with the ‘Civil Liberties Officer’ and, if that is not sufficient, may refer the matter to the ‘Data Protection Review Court’. This new agreement therefore provides a legal remedy for European citizens, which was not the case under previous agreements. (*cadre de protection des données UE - États-Unis*, 2023)

Despite these new provisions, companies remain subject to the US Cloud Act. We may therefore question the actual consequences of this agreement.

Looking at these various European court rulings, it is clear that the European Union and the United States are attempting to reach an agreement. The United States wants the European Union to maintain cooperation between their technology companies, whilst the European Union wishes to ensure the security of citizens’ data in accordance with the GDPR. Due to the Cloud Act, finding common ground to comply with the security standards required for the implementation of the EHDS looks set to be a tedious and complex process. The question is whether such an agreement could be reached, or whether the European Union should focus more on creating and developing a European server with a capacity equivalent to that of its US counterparts.

Chapter 2 — The US cloud at the heart of European healthcare systems: a structural dependency

Let us start with the initial paradox: the EHDS requires data to be stored in Europe, but Europe has not built the infrastructure to ensure this itself. AWS, Microsoft Azure and Google Cloud account for around 65–70% of the European cloud market. In the healthcare sector specifically, this dependency is even more pronounced because hospitals and national systems migrated en masse to these platforms between 2015 and 2022, often driven by digital modernisation policies that did not anticipate the legal consequences of Schrems II. This chapter examines the reality of this dependence, the US legal framework that makes it problematic, and European attempts to address it.

Current situation: where is European health data actually stored?

According to Synergy Research Group, a market research firm, AWS, Microsoft and Google are the leading providers of European cloud services, accounting for around 70% of the market. (*European Cloud Providers' Local Market Share Now Holds Steady at 15% | Synergy Research Group, 2025*) Although this does not pertain solely to the healthcare sector, it nevertheless demonstrates a trend in Europe. The EMA, or 'European Medicines Agency', based in Amsterdam, which regulates medicines for European citizens, is a concrete example of this. This European institution is co-developing the EHDS and, in 2024, selected Microsoft Azure as its preferred provider. It justified this choice on the grounds that the American company invests billions annually to ensure cybersecurity, an amount that European companies cannot afford. It has therefore shut down its servers in Europe to switch exclusively to Microsoft. (*European Cloud Providers' Local Market Share Now Holds Steady at 15% | Synergy Research Group, 2025*) (*European Medicines Agency Cloud Strategy Accelerating Innovation and Digitalisation Better Public and Animal Health Outcomes, n.d.*) When it comes to European sovereignty, it is important to understand that the jurisdiction applicable to companies depends, amongst other things, on the nationality of the parent company. In other words, if a European company chooses to collaborate with the European subsidiary of an American company, it will remain subject to the requirements of the US Cloud Act. (*The CLOUD Act, 2022*) This

is why, under the EHDS, US authorities could still have access to European data even though it is stored by US companies on servers in Europe.

Currently, under the EHDS, the various types of health data (genomic, medical, administrative) are treated equally in terms of the security required for their storage. However, the sensitivity of these different types of data is not equivalent. Administrative data is significantly less sensitive than medical data per se. This was, in fact, highlighted by the Doctolib case discussed earlier. Genomic data, on the other hand, is extremely sensitive as it allows a person and their family to be identified and cannot be altered. Some countries, such as China, have special legislation governing such data for national security purposes. (*Mapping China's Tech Giants* | *Australian Strategic Policy Institute*, n.d.) (*AVIS COMMUN AVIS 143 CCNE / AVIS 5 CNPEN*, 2023) Its commercial and scientific value is immense. It is undeniable that the risks associated with storing these different types of data are not equivalent. The question arises as to why they are treated uniformly.

The US Cloud Act: anatomy of a legal threat

Let us now take a closer look at the US Cloud Act, or the ‘Clarifying Lawful Overseas Use of Data Act’, which is the source of most concerns regarding data storage. This act, signed by US President Donald Trump in 2018, authorises US authorities to demand data stored by US companies. Whilst this was already possible via a lengthy diplomatic process, the Cloud Act makes access much quicker. The Cloud Act allows for the conclusion of bilateral agreements with other countries so that they too have access to data stored in the United States, and such an agreement has, for example, already been concluded with the United Kingdom and Australia. (*Salgado*, 2025) However, the United States and the European Union have never managed to sign such an agreement, mainly due to Article 48 of the GDPR. (*Department of Home Affairs Website*, 2022) This provision prohibits the unlawful transfer of data outside the European Union. Although the United States already has access to data stored on US servers under this Act, the European Union cannot easily conclude such an agreement as it would legitimise the Cloud Act and thus the transfer of data. This runs counter to the GDPR and would consequently weaken it. This legal issue has direct consequences for businesses, which may find themselves caught between US and European legislation with no solution. By the same token, the US government has direct access to European citizens’ data under Section 702 of the FISA

Act. (*FISA Section 702*, n.d.) This section authorises the National Security Agency (NSA) to access data without having to request it if this is necessary for foreign intelligence purposes. This is one of the issues contested in the Schrems II ruling. A parallel can be drawn between the situation regarding the Cloud Act and European health data and the case of the TikTok platform in the United States. (*Sissoko-Noblot*, 2025) Indeed, The United States sought to ban the Chinese platform on the grounds that it held the data of millions of Americans and that this was unacceptable, given that China has legislation comparable to the Cloud Act.

However, the Cloud Act allows for challenges to data access if this would cause a ‘material risk of conflict’ with the law of another country, which is the case with European Union law. (*18 U.S. Code § 2703 - Required Disclosure of Customer Communications or Records*, n.d.) But such challenges depend on the goodwill of the company. As for abusive requests, these must be challenged under the standard contractual clauses established following the Schrems II ruling. This remains a contractual commitment, and US law (like any other law) takes precedence over contractual commitments.

European attempts at sovereignty: between ambition and reality

To address the issues arising with these US hyperscalers, France and Germany sought to propose an infrastructure enabling the identification of sovereign European clouds. In 2019, they launched Gaia-X, an infrastructure that allowed different clouds to obtain a label if they complied with GDPR standards. Thus, European businesses and citizens could easily distinguish sovereign European offerings from American offerings created for Europe and appearing to be sovereign. Although the initiative was initially met with enthusiasm, this quickly waned when the public realised that companies such as Amazon and Microsoft were members and could therefore influence the required technical standards. The final blow was the departure of Scaleway, the French cloud provider. (*Pollet*, 2022)

The European Union has begun to develop its own clouds, and there are now several in existence. France, for example, has developed OVHcloud and Scaleway. OVHcloud is a major European provider and is unique in that it manufactures its servers on European soil, which meant it was subject solely to French and European law. However, in

2021, a fire destroyed one of its two data centres, resulting in the loss of thousands of files belonging to corporate clients. (IGEDD, 2022) Such a loss of data is simply not an option for a hospital, for example. Scaleway, meanwhile, is the provider for the Health Data Hub but does not yet have the capabilities equivalent to those of American hyperscalers. This is, in fact, the problem faced by other European providers such as Deutsche Telekom, IONOS, Exoscale and Outscale – companies based in Germany, Switzerland and France. (Gartner | *Delivering Actionable, Objective Insight to Executives and Their Teams*, 2026)

France has therefore decided to trial a system combining the strengths of US hyperscalers and European sovereign clouds. To do this, they are applying the SecNumCloud model to Bleu or S3NS. (*S3NS Annonce La Qualification SecNumCloud de Son Offre Cloud de Confiance PREMI3NS* | Thales Group, 2025) (*Capgemini et Orange sont heureux d'annoncer le lancement des activités commerciales de Bleu, leur future plateforme de « cloud de confiance »*, 2024) (ANSSI, n.d.) How does this work in practice? In effect, businesses have access to the US hyperscalers' cloud, but it is French companies that hold the encryption keys. This could be compared to a franchise. In theory, this means that if the US authorities request access to data stored on these servers, the American hyperscalers would not be able to provide it, as they do not hold the encryption key. (VELLIET, 2023) However, the question companies are still asking is whether the data is truly secure. Indeed, whilst the US hyperscalers do not hold the keys, they are the ones who create the code. (Blancato & Carr, 2024) There could be a vulnerability, exposing European data.

1. The EHDS as a structural solution: the residency requirement and its implications

The EHDS Regulation (2025/327), and in particular Article 87, imposes requirements on all Member States regarding the storage and processing of data. (*Règlement (UE) 2025/327 du Parlement européen et du Conseil*, 2025) It requires that the processing of personal data, as well as the pseudonymisation and anonymisation of such data, be carried out within the territory of the European Union. This requirement is primarily met through the system of accessing data within secure environments, without sending it. However, this article does not require the use of a specific provider; this means that data-processing institutions, such as HDABs or HealthData@EU, may do so using a

non-European provider provided that the latter has a server located within the European Union. This residency requirement gives rise to a new risk of fragmentation: does a Member State that currently stores its data on a server belonging to a US subsidiary, such as Microsoft Azure Ireland, comply with the residency requirement? It will first be necessary to ensure that there is a clause prohibiting transfer outside the European Union, but is that sufficient; does a contractual clause not allow subsidiaries to derogate from the legal obligations to which they are subject, such as the Cloud Act? (*White Paper Demystifying the Debate on the US CLOUD Act vs European/UK Data Sovereignty in the Context of Cloud Services*, 2026) The issue has not yet been resolved by the Commission, which leaves discretion to Member States until secondary legislation is adopted by March 2027. (*Watkins*, 2025) Furthermore, national HDABs are only to be designated by March 2027. However, the residency requirement will take effect as soon as HealthData@EU becomes operational, in other words between 2027 and 2031. (*European Health Data Space Regulation (EHDS) - Public Health*, 2026) The entire roll-out of this infrastructure without clear legislation is forcing Member States to adopt measures now, the impacts of which will extend over time. (*Angeloudi et al.*, 2025)

Part IV — The American perspective: economic interests and transatlantic tensions

Chapter 1 — US stakeholders and the EHDS: between opportunity and resistance

The United States is a large country with many different stakeholders. All must be taken into account when analysing the US perspective on the EHDS, as they do not share the same interests. Technology companies such as Microsoft, Amazon and Google are directly affected by this regulation and have much to lose. But pharmaceutical companies such as Pfizer or Johnson & Johnson could stand to gain in the long term if they are granted access to these databases. And institutional lobbies find themselves caught in the middle. As in the European Union, there is therefore no single American view. We will therefore take a closer look at each of these perspectives.

US tech companies: an existential threat to their European model

The EHDS poses a real threat to major US tech companies such as Amazon, Microsoft and Google. Indeed, the European cloud market is substantial, worth billions of euros, and growing. (*European Cloud Providers' Local Market Share Now Holds Steady at 15% | Synergy Research Group, 2025*) Although the regulation itself does not prohibit the use of US platforms, Article 87 indirectly requires that data be stored and processed within the European Union. The European subsidiaries of these platforms are therefore viable options, but the Schrems II ruling and the Cloud Act do not make it easy for European companies to choose these US platforms. This regulation could therefore cause significant harm to US tech companies within a few years and cause them to lose a considerable share of the European market. These US hyperscalers are consequently fighting back all the way to Brussels, the seat of the European Commission. To this end, they employ lobbyists. Major companies such as Google and Microsoft spend millions of euros on lobbying every year. (*Revealed: Tech Industry Now Spending Record €151 Million on Lobbying the EU | Corporate Europe Observatory, 2025*) These lobbyists use three main arguments. (Norigami & Silva, 2026) Firstly, they argue that a requirement for local data storage is sufficient to guarantee data security and that adding a requirement for a sovereign cloud

would amount to protectionism, which is contrary to the GATS. Secondly, European providers are significantly less capable than US platforms and do not allow for the same of health data. Finally, the lobbies maintain that fragmentation of the cloud market could hinder innovation, which is completely at odds with the objective of the EHDS; that this cloud issue delays innovation and research, thereby directly harming European patients. So far, the Commission has not wavered. (Roussanov & González-Lamuño, 2025) It still does not prohibit US companies from operating within the European Union under the EHDS, but nor has it asserted that the physical location of data within the European Union alone is sufficient to guarantee the necessary security for such data. The issue of legal sovereignty therefore remains unresolved and is putting pressure on US hyperscalers to develop technologies that are legally independent of the US government, such as the S3NS system. Lobbying has therefore not worked as hoped, but this demonstrates that these US companies are trying, as best they can, to defend their interests in the face of this regulation that directly impacts them.

The US pharmaceutical industry: an unexpected ally of the EHDS

For major US pharmaceutical companies, this regulation could, on the contrary, be a potential long-term gain. Companies such as Johnson & Johnson or Pfizer are major consumers of secondary data. Having access to such a database would be a major asset for them. Access would be granted to them in two different ways: either they seek full access by becoming a member of the EHDS under Article 75 of the EHDS Regulation, in which case they will only gain access from 2035 onwards, or they may gain access as early as 2027 under Article 91 of the same regulation, provided they demonstrate that they also grant European researchers access under conditions that are equal to or less restrictive than those of the EHDS. Unlike the EHDS system, in the United States data is fragmented across private insurers and not aggregated. It is for these reasons, among others, that the EFPIA, or ‘European Federation of Pharmaceutical Industries and Associations’, has supported the EHDS in its official positions. (EFPIA Position on EHDS, 2024) EFPIA also represents the European subsidiaries of US groups. Although this could be an advantage for them, they also have several concerns. Firstly, they would like access to this data to be granted to commercial entities as well. (Barton, 2024) When HDABs receive such a request, they have the power to accept or reject it. The regulation is rather vague regarding

access for commercial actors, yet a pharmaceutical company conducts research but also seeks to make a profit. A second concern revolves around intellectual property. (*Efpia Response to the Consultation on Legislative Proposal for a European Health Data Space*, n.d.) Indeed, the regulation does not set out specific rules on the matter, whereas a company could develop its system using public data from various HDABs, which may have issued different clauses regarding whether or not to share results. They also question the reciprocity required for access to HealthData@EU. (*Tschammler et al.*, 2025) This allows access if third countries grant reciprocity after 10 years. However, they consider a decade to be too long a period in the pharmaceutical sector. In this context, lobbying by PhRMA (Pharmaceutical Research and Manufacturers of America) has called for the EHDS to be included in trade discussions with the EU, in the hope of reducing the timeframe before third countries gain access to the EHDS. The final point concerns genomic data. This data is of significant value, and the EU is home to several biobanks. The question is whether this data can be included in the EHDS and thus used by US companies such as Illumina, for whom this would represent real added value, even though the data is difficult to anonymise.

AmCham EU and institutional lobbies: data diplomacy

The third player with its own perspective is the institutional lobbies. AmCham EU, or the American Chamber of Commerce in the EU, based in Brussels, represents over 150 major US companies operating in the European Union. Annually, it allocates a budget of around €1.5 million, in addition to the individual budgets of its members. AmCham EU has various specialist committees working on different pieces of European legislation, which enables the leaders of these committees to meet regularly with European Commissioners. (*American Chamber of Commerce to the European Union | Lobbyfacts*, 2026) Officially, AmCham EU is not an anti-European American lobby. It supports the EHDS in a 2022 public consultation but contests certain provisions which it considers discriminatory towards American companies. (*European Health Data Space*, 2022) The provisions in question are the data localisation requirement, which it considers a protectionist measure contrary to WTO rules; access to data for non-European suppliers after a 10-year period; and clarification of the intellectual property issue. It is calling for a framework ensuring

that models developed using data available via the EHDS infrastructure are protected by intellectual property rights and remain the property of the company that developed them.

The USTR, the Office of the United States Trade Representative, publishes an annual report, the National Trade Estimate Report on Foreign Trade Barriers, in which it details the trade barriers it considers third countries to be imposing on the United States. (*2024 National Trade Estimate Report on FOREIGN TRADE BARRIERS*, 2024) In its first reports following the EHDS proposal, it identified several EHDS provisions as trade barriers. In its 2024 report, however, published under Biden, it removed these provisions from the list because governments have “a sovereign right to adopt measures in pursuit of legitimate public policy objectives”. Then, in 2025, under Trump and a few days before the announcement of the reciprocal tariffs plan, the USTR reinserted these provisions onto the list of trade barriers. (*Comments to USTR on the National Trade Estimate Report on Foreign Trade Barriers*, 2025)

The US Chamber of Commerce is based in Washington and is much more direct and critical of the regulations adopted by the European Union. In its view, the EHDS in its entirety, just like the GDPR, constitutes a barrier to innovation. It also publishes annual reports in which it analyses the cost to US companies of adapting to European standards. Unlike AmCham EU, it is not in direct contact with European Commissioners. Instead, it presents its arguments to the US Congress and the federal government so that they may incorporate these issues into their agenda and ensure they are taken into account in transatlantic negotiations.

The "Brussels Effect" revisited: the EHDS as an exportable model or a fortress?

Anu Bradford developed a theory in 2020: the Brussels Effect. According to this theory, when the European Union adopts a regulation, global companies are forced to adapt to it, as the European Union market is significant and it is not cost-effective to have two different standards within the same company. (Bradford, 2012) This is, for example, what happened with the adoption of the GDPR; large companies such as Apple and Google adopted data protection measures for all their users, not just European ones. The EHDS could therefore potentially have the same effect and set global standards. (Kanninen, 2025) This is a possibility because the European healthcare market is a significant one and global

pharmaceutical companies do not wish to be excluded from it, because certain countries such as Japan are considering creating their own system similar to that of the EHDS, and because the WTO (World Trade Organisation) and the OECD (Organisation for Economic Co-operation and Development) have emphasised the importance of good health governance. (Kubota & Ishibashi, 2025) (OECD, 2023) However, the EHDS is an infrastructure that processes data stored within the European Union; it therefore does not have the same effect on foreign companies as the GDPR does. Furthermore, the United States might react in the opposite way and tighten its standards, which would ultimately lead to global fragmentation in data processing. Finally, China is developing a national system that excludes third countries and is therefore not geared towards collaboration.

The EHDS was launched at a time when transatlantic tensions were already present. The Trump administration has already expressed its dissatisfaction with the regulatory multilateralism that comes with this new regulation. The United States has already threatened retaliation over the fines imposed on companies such as Google. The introduction of the EHDS therefore represents a further point of contention in these transatlantic tensions: the European Union must fear trade retaliation if it wishes to maintain its data security regulations at the highest level. (Greer et al., 2025)

The American perspective cannot, therefore, be summarised by a single viewpoint. Each of the American stakeholders defends its own interests and views the EHDS as either a threat or an opportunity. For major American tech companies, it is more of a threat. As for American pharmaceutical companies, they could stand to gain if the right conditions are put in place for them. And US lobbies do not adopt the same official positions depending on their geographical location. However, these stakeholders share a common stance in refusing to allow the EHDS to become a tool for discrimination. We have also observed that all of this is also a geopolitical issue dependent on the United States' objectives regarding transatlantic relations. The European Union is therefore under pressure and must be aware that its choices will influence transatlantic relations, but that if it wishes to remain true to the primary objective of the EHDS—to guarantee the highest possible level of security for its citizens—it cannot yield to all American demands.

Part V — The European perspective: between shared ambition and national differences

Chapter 1 — Twenty-seven Member States, twenty-seven speeds: the European divide over the eHDS

The EHDS is a European Union initiative to be implemented within the Union. However, the European Union is a political and economic union currently comprising 27 Member States. Each of these Member States has its own laws, its own economy and its own policies. Nor do they share the same technological standards, socio-economic indicators or minimum wage. The member states of the European Union are therefore a very heterogeneous group. This makes the implementation of the EHDS extremely complex. Moreover, their healthcare systems are also very different, and although the EHDS may have drawn inspiration from certain European countries, others are not yet as advanced. The challenge for the EHDS is therefore to implement a single set of regulations, with uniform standards, across a union of countries with very different starting points.

The pioneers: the Nordic countries and Estonia as models

Currently, Nordic countries such as Estonia and Finland are the most advanced in terms of their starting point for implementing the EHDS. Finland has a system similar to the EHDS, called Findata, which has been in place since 2020. (*Finland Country Visit Factsheet*, 2022) Since then, it has proven its worth with over 400 research projects approved in three years and an average processing time for applications of 30 days. The EHDS has therefore adopted certain aspects of Findata's operations, such as the opt-out system. This means that data from all patients is automatically considered available for use, but the patient has the right to request that this not be the case. It has also adopted the data permit system, whereby each country, via its national contact point – a system Finland had already recognised as necessary for Findata's operation – approves researchers' requests for specific data use within a clearly defined framework, and researchers cannot deviate

from this. It also incorporates the secure processing environment system, where researchers conduct their research using the data within a secure space, meaning the data is no longer sent to the researcher. And finally, the principle of publishing the list of data accesses so citizens can keep an eye on who is accessing their data and why, so that researchers can see if a study similar to theirs is already underway and thus potentially facilitate collaborations, and finally so that the HDAB can carry out checks to ensure it is not systematically granting access to the same people. (*Permits - Findata*, n.d.) The concern regarding the transition from Findata to the EHDS is the scale of the system; Finland has a population of around 5.5 million, whereas the EHDS is intended to cover approximately 450 million people.

Then we have countries such as Denmark and Sweden. They do not have a system similar to Findata in place, but Denmark has been recording its citizens' medical data in registers since the 1970s. (*Sweden Country Visit Factsheet*, 2022) (Erlangsen & Fedyszyn, 2015) (Schmidt et al., 2019) This means they have data spanning around fifty years. Having data over such a long period can be vital for certain research. Sweden, for its part, also has several long-term national registers, but in addition to this, it has the legal framework allowing for the cross-referencing of these registers. These two examples demonstrate that centralising data is not at odds with data security; indeed, the figures show a very high level of trust on the part of citizens in these countries towards their national medical institutions.

Finally, there is also Estonia. It has digitised virtually everything related to healthcare. Thus, every medical record has been digitised since 2008 and citizens can access them via their electronic ID card, whilst almost all medical prescriptions are electronic as well. Building on this, Estonia is participating in the initial pilot phases of MyHealth@EU, the digital infrastructure enabling cross-border data exchange. (Estonian E-Health Records, n.d.) (Jõgi et al., 2023)

Ambiguous positions: France and Germany between ambition and resistance

Then there are countries such as Germany and France. Germany is the largest country in the European Union in terms of population, making it a key player regarding the EHDS. However, it remains ambivalent towards the latter. This stems, among other things,

from the experiences of the Gestapo and the Stasi in the last century, during which citizens' personal information was used against them. These events have fostered a mindset that is wary of the dissemination of personal data and opposed to centralisation. Against this backdrop, in 1983 the German Constitutional Court enshrined a right to informational self-determination (*Volkszählungsurteil*). (Simitis, 1984) This right grants German citizens the right to decide what information—which allows conclusions to be drawn about the individual—may be disclosed and how it may be used. This right stems from German constitutional law, which means it is difficult to deviate from it. Furthermore, historically, Germany has been one of the countries most opposed to the regulations the European Union is attempting to introduce. In Germany, healthcare is a matter for the *Länder*, and so each Land has its own IT system. Although the German federal government supports the EHDS and is trying to prepare the country for it, for example through the GDNG (*Gesundheitsdatennutzungsgesetz*) Act adopted in 2023, which lays the initial foundations such as the creation of data access points, the provision of data for secondary use and the establishment of secure environments, several *Länder* oppose the EHDS. (*Gesundheitsdatennutzungsgesetz (GDNG)*, 2024) (The Health Data Use Act, 2024)

France, for its part, has made significant progress regarding digital sovereignty. As previously discussed, it has supported the Gaia-X project, created to develop a trusted digital space, and has already opted for a French cloud provider, Scaleway, for its HDAB Health Data Hub. (Khaski, 2026) (Beurnez, 2026) However, its healthcare system is not uniform, and hospitals in France use a wide variety of software, which complicates interoperability and, consequently, research. Furthermore, the CNIL, the French data protection authority, is highly active and carefully scrutinises healthcare providers' compliance with the GDPR, and it is highly likely that it will do the same regarding the EHDS's compliance with the GDPR. It is more cautious than the Ministry of Health, which is enthusiastic about the EHDS. (*Cloud Souverain Santé : Scaleway Remplace Microsoft*, 2026) (Navarro & Zannotti, 2020)

Member States facing difficulties: the digital divide and political resistance

Other EU countries face greater obstacles. Some Central and Eastern European countries, such as Bulgaria, Romania and even Poland, are far less advanced in the digitisation of their healthcare systems compared to the European average. (Kessissoglou

et al., 2024) (*Digital Decade 2025*, 2025) This delay poses a challenge for the EHDS because, even if they designate an HDAB by March 2027 as required by the regulation, the data available in these countries will clearly be incomplete and likely difficult to interoperate. The European Union is aware of this weakness, which is why it has earmarked EU funds to help countries in this situation develop their digital infrastructure, but development takes time. (*Synthesis Report 2025*, 2025)

Italy is an example of a country where the problem lies in the division of powers. In Italy, healthcare is governed by the regions, each of which has its own system and its own rules. (Murgia et al., 2025) (*The Lancet Regional Health – Europe*, 2025) It is also in this context that designating a single national HDAB by March 2027 is a challenge, as it raises constitutional questions regarding the powers of the central government and the regions. Although the country has been attempting to centralise data since 2012, the process is still not complete after more than a decade. Italy is one example among many of federal or regionalised countries where responsibilities regarding healthcare do not always lie with the state.

Finally, Hungary highlights another issue that relates more to politics and governance. (Jóri, 2012) The European Union, and consequently the EHDS, consider that the data collected complies with the GDPR. Researchers accessing Hungarian data via the EHDS will assume that this data has been collected in accordance with the GDPR. However, Hungary under Viktor Orbán has already been called into question regarding the independence of its institutions and data protection authorities from the government. So although the EHDS regulation provides for a supervisory mechanism by the European Commission, potential sanctions remain limited. In reality, potential sanctions do not apply to the HDAB itself – and therefore not to the government – but to private institutions. The only mechanism against a Member State is the infringement procedure, but this takes place before the Court of Justice of the European Union and generally takes between two and four years. Short-term sanctions are therefore not envisaged; those against the government are subject to the Commission's discretion and require the identification of a breach of a specific article of the regulation. (Barrett, 2024) Can we therefore assume that all Member States apply the same standards of protection?

The Digital Omnibus: towards an internal review of the data protection framework

In November 2025, the European Commission adopted the Omnibus package in response to the Draghi and Letta reports on European competitiveness and the European Union's lag in the field of AI. (*Digital Omnibus Regulation Proposal | Shaping Europe's Digital Future*, 2025) (*An Agile Digital Rulebook for the EU | Shaping Europe's Digital Future*, 2026) Among other things, this package seeks to reform the definition of personal data so that pseudonymised data is no longer classified as personal data if it does not allow for the identification of the person to whom the data belongs. This is a position completely at odds with that of the EHDS adopted a few months earlier, which is based entirely on the definition of personal data provided by the GDPR. In February 2026, the EDPB and the EDPS, two institutions overseeing data protection, published a joint opinion rejecting controversial proposals in this package, including the redefinition of personal data. (*Omnibus Numérique: L'EDPB et Le CEPD Soutiennent La Simplification et La Compétitivité Tout En Soulevant Des Préoccupations Majeures | European Data Protection Board*, 2026) The part of the package concerning data has not yet entered into force and must go back through the trilogue between the Parliament, the Council and the European Commission. This package therefore reflects the internal tension within the European Union, which wishes to maintain its digital sovereignty through the EHDS and the GDPR whilst improving its competitiveness vis-à-vis the United States or China, for example.

The challenge facing the EHDS of applying a single regulation to the differing realities of the 27 Member States is no small one. It is possible to meet this challenge, and several countries demonstrate that the EHDS's objective is achievable, but it is clear that certain digital, technological and political challenges will first need to be overcome. The implementation of the regulation will depend on the cooperation of each Member State, and its success is subject to many conditions.

General conclusion : The EHDS or Europe's gamble on trust

Recap of the central tension and summary of the analysis

As explored throughout the various chapters of this work, the European Union has therefore developed several techniques to reconcile a single market for innovation and medical research with the protection of sensitive data. Initially, the EHDS developed a system for data access and institutional trust whilst guaranteeing the right to object and defining the purposes of data use. However, data security is compromised by dependence on US infrastructure, which is subject to the Cloud Act, contrary to the GDPR. It is in this context that the EHDS requires data to be located within the European Union, but European infrastructure is not yet sufficiently robust to ensure the smooth operation of a system of this scale. Furthermore, this regulation has proved to be a strategic geopolitical tool to be taken into account in relations between the European Union and the United States, whilst remaining aware of certain differences of opinion within the various US institutions.

Direct answer to the research question

Within the European Union, the EU is attempting to create a single market for innovation and medical research by harmonising rules across the various member states to eliminate the fragmentation caused by the laxity of the GDPR. It is also attempting to standardise technical rules so that data accessible from different countries is usable and comparable. Finally, through each country's HDABs, it facilitates access to data for researchers whilst maintaining control to ensure data security and safeguarding the intended purpose of the data's use.

The EHDS guarantees data security through technical standards such as anonymisation and SPE, through the law by requiring data to be stored within the European Union, through the two main regulations—the GDPR and the EHDS—and through transparency by publishing the list of data accessors and the right to object.

The European Union has therefore succeeded in establishing a legal framework with technical standards conducive to data security, but remains exposed to factors beyond its control, such as geopolitical tensions and digital dependency, as well as to the will of

the 27 Member States.

A critical look: the EHDS – between ambition and fragility

The EHDS demonstrates the European Union's ambition and lays the necessary foundations for its successful implementation; it sets out a legal framework, establishes technical standards, and provides funding to accommodate the specific circumstances of the various Member States. However, the success of the EHDS depends on the European Union's consistency. It must remain consistent with the values and principles upon which the regulation is built, but also upon which the Union itself is founded. For this to happen, the surrounding legal framework must stabilise. The EHDS relies on the GDPR and the DPF regarding data transfers, yet these are being undermined by the Omnibus package and transatlantic tensions respectively. The EHDS was built around the GDPR, and the Omnibus Package calls into question a key definition within that regulation. If the new definition is adopted, it leaves the door open to profound challenges regarding the EHDS; will European citizens have sufficient confidence not to refuse en masse to share their pseudonymised personal data, when certain studies show that it remains possible to identify the person behind the data by cross-referencing certain databases? Will an amendment to the EHDS be necessary if this definition is adopted, and more specifically Article 68 of this regulation, which requires authorisation for pseudonymised data, given that the EHDS is so recent? The DPF, for its part, is unstable following the paralysis of the PCLOB, and there remains uncertainty regarding the continuation of the executive order that established it. However, to prevent the legal basis underpinning the EHDS from collapsing easily—for example, through a unilateral decision by the United States—the DPF would need to be consolidated by legislation, for instance.

The whole issue surrounding data transfers to US companies highlights the problem of the lack of a sovereign European cloud. Although the EHDS regulates access to and storage of data, the European Union's actual control remains limited. Since US companies are subject to the Cloud Act, there is nothing to prevent US authorities from accessing this data. There are two solutions to this problem: a sovereign third party holding an encryption key, or a sovereign European cloud. The first solution would allow security requirements to be combined with the performance of US companies, but it would be necessary to ensure that the

US company cannot actually access the data, despite having the encryption key. The ideal solution would therefore be a sovereign European cloud that is as efficient as its US counterparts. At present, they are not as efficient, but it is possible to improve them by providing the right incentives.

Ultimately, the European Union's consistency in addressing these approaches is crucial. Although its objectives are manifold and require further consideration to reconcile them, it cannot lower its standards for protecting its citizens in order to be more economically competitive. It must find innovative solutions that allow these two objectives—both necessary for the proper functioning of the European Union—to be combined. The EHDS embodies the European Union's choice of a society where citizens' well-being is a priority, yet it strips it of the means to ensure it. It must align its choices with its primary objective.

Limitations of the study

This thesis has several limitations. Firstly, it examines only the legal and institutional framework of the EHDS and was unable to examine in depth public perception of this regulation, nor did it examine in depth the reality on the ground in hospitals or among patients. A further study could be conducted regarding the trust placed by citizens in those accessing their data, particularly commercial entities. Finally, this thesis has also focused primarily on relations between the European Union and the United States, but other relationships must be taken into account, such as those with China, for example.

Outlook and prospects

It is also important to emphasise that the EHDS is currently being implemented and that this thesis has examined the current state of affairs. However, the future is uncertain. Maximilian Schrems has already announced his intention to challenge the Data Privacy Framework between the European Union and the United States, which is due to be implemented in 2023 and is one of the pillars of the EHDS. If the outcome is similar to the first two cases, the European Union would have no choice but to develop its own sovereign European cloud.

One of the key products that could emerge from the creation of this single market will be trained medical AI systems. But who will own them, and who will have access to them? These are distinct questions to which the European Union will have to respond without delay.

Furthermore, the EHDS is a gamble on the part of the European Union. If it succeeds, it could become a global model to follow. However, this success is subject to many conditions, such as HealthData@EU being operational, the HDABs functioning, and the entire infrastructure being genuinely useful for medical research. Conversely, if it fails, it will demonstrate a potential incompatibility between the European Union's data protection requirements and innovation. The answers to these questions will only emerge in the coming years, or even decades, once the EHDS has been established and adopted.

Bibliography

I acknowledge using AI to improve the phrasing and formatting of this work.

18 U.S. Code § 2703—Required disclosure of customer communications or records. (n.d.).

LII / Legal Information Institute. Retrieved May 13, 2026, from

<https://www.law.cornell.edu/uscode/text/18/2703>

2024 National Trade Estimate Report on FOREIGN TRADE BARRIERS. (n.d.). Retrieved

May 14, 2026, from <https://ustr.gov/sites/default/files/2024%20NTE%20Report.pdf>

Affaire C-362/14 (Cour de justice September 23, 2015). [https://eur-lex.europa.eu/legal-](https://eur-lex.europa.eu/legal-content/FR/ALL/?uri=CELEX:62014CC0362)

[content/FR/ALL/?uri=CELEX:62014CC0362](https://eur-lex.europa.eu/legal-content/FR/ALL/?uri=CELEX:62014CC0362)

American Chamber of Commerce to the European Union | lobbyfacts. (2026).

<https://www.lobbyfacts.eu/datacard/american-chamber-of-commerce-to-the-european-union?rid=5265780509-97>

An agile Digital Rulebook for the EU | Shaping Europe's digital future. (2026, May 7).

<https://digital-strategy.ec.europa.eu/en/policies/digital-rulebook>

Angeloudi, E., Gillert, J., & Takhar, J. (2025, March 5). European Health Data Space Regulation Published – What's Next? *Healthcare & Life Sciences Blog*.

<https://healthcarelifesciences.bakermckenzie.com/2025/03/05/european-health-data-space-regulation-published-whats-next/>

Annual report 2025. (2026, March 17). Findata. <https://findata.fi/en/about-findata/annual-report-2025/>

ANSSI. (n.d.). *Cloud.* cyber.gouv.fr. Retrieved May 11, 2026, from

<https://cyber.gouv.fr/enjeux-technologiques/cloud/>

AVIS COMMUN AVIS 143 CCNE / AVIS 5 CNPEN. (n.d.). Retrieved April 27, 2026, from https://www.ccne-ethique.fr/sites/default/files/2023-05/CCNE-CNPEN_GT-PDS_avis_final27032023.pdf

Barrett, G. (2024). Rule of Law Chickens Coming Home to Roost. *Verfassungsblog*. <https://doi.org/10.59704/1d158aab48c749aa>

Barton, C. (2024, January 2). *Finalizing the European Health Data Space | Pharmaceutical Technology*. <https://www.pharmtech.com/view/finalizing-the-european-health-data-space>

Beurnez, V. (2026, April 23). *Le Health Data Hub a choisi le Français Scaleway pour héberger les données de santé*. Acteurs Publics. <https://acteurspublics.fr/articles/le-health-data-hub-a-choisi-le-francais-scaleway-pour-heberger-les-donnees-de-sante/>

Bévière-Boyer, B. (2023). Les perspectives éthiques et juridiques du suivi numérique de santé à vie du patient du XXIème siècle: Ethical and legal perspectives on lifelong digital health monitoring of the 21st century patient. *Journal du Droit de la Santé et de l'Assurance - Maladie (JDSAM)*, 36(1), 45–55. <https://doi.org/10.3917/jdsam.231.0045>

Blancato, F. G., & Carr, M. (2024). The trust deficit. EU bargaining for access and control over cloud infrastructures. *Journal of European Public Policy*, 33(3), 936–967. <https://doi.org/10.1080/13501763.2024.2441418>

Bradford, A. (2012). *The Brussels Effect* (SSRN Scholarly Paper No. 2770634). Social Science Research Network. <https://papers.ssrn.com/abstract=2770634>

C-311/18, Case C-311/18 (Cour de justice July 16, 2020). <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62018CJ0311>

Cadre de protection des données UE - États-Unis. (2023, July 10). [Text]. European Commission - European Commission. https://ec.europa.eu/commission/presscorner/detail/en/qanda_23_3752

Capgemini et Orange sont heureux d'annoncer le lancement des activités commerciales de Bleu, leur future plateforme de « cloud de confiance ». (2024, January 15). *Capgemini France*. <https://www.capgemini.com/fr-fr/actualites/communiqués-de-presse/capgemini-et-orange-annoncent-le-lancement-des-activites-commerciales-de-bleu-leur-future-plateforme-de-cloud-de-confiance/>

Charte des droits fondamentaux de l'Union Européenne. (n.d.). Retrieved April 24, 2026, from https://www.europarl.europa.eu/charter/pdf/text_fr.pdf

Clinical Trials. (2026). <https://www.efpia.eu/about-medicines/development-of-medicines/regulations-safety-supply/clinical-trials/>

Cloud Act et RGPD: Quelles implications pour la protection des données des entreprises européennes ? (2024, November 14). <https://www.lexisnexis.com/blogs/fr-juridique/b/droit-des-affaires/posts/cloud-act-et-rgpd-protection-donnees-entreprises-europeennes>

Cloud Defence. (n.d.). Retrieved April 24, 2026, from <https://futureinstitute.tech/assets/doc/FOTICloudDefenceReport26.pdf>

Cloud souverain santé: Scaleway remplace Microsoft. (2026, April 23). https://www.parlons-politique.fr/economie-societe/quand-letat-choisit-un-cloud-souverain-pour-protéger-les-donnees-de-sante-le-basculement-de-microsoft-vers-scaleway_14432/

CNIL. (n.d.). *Confidentialité différentielle*. Retrieved April 21, 2026, from <https://www.cnil.fr/fr/definition/confidentialite-differentielle>

Comments to USTR on the National Trade Estimate Report on Foreign Trade Barriers. (2025, October 29). *Public Citizen*. <https://www.citizen.org/article/comments-to-ustr-on-the-national-trade-estimate-report-on-foreign-trade-barriers/>

Consumers, Health, Agriculture and Food Executive Agency. (2021). *Assessment of the EU*

Member States' rules on health data in the light of GDPR. Publications Office.

<https://doi.org/10.2818/546193>

Cour de justice de l'Union européenne. (n.d.). curia. Retrieved April 24, 2026, from

https://curia.europa.eu/site/jcms/d2_5088/fr/que-fait-la-cjue

Department of Home Affairs Website. (2022). Department of Home Affairs Website.

<https://www.homeaffairs.gov.au>

Differential Privacy | Harvard University Privacy Tools Project. (n.d.). Retrieved April 21,

2026, from <https://privacytools.seas.harvard.edu/differential-privacy>

Digital Decade 2025: eHealth Indicator Study | Shaping Europe's digital future. (2025, June

16). <https://digital-strategy.ec.europa.eu/en/library/digital-decade-2025-ehealth-indicator-study>

Digital Omnibus Regulation Proposal | Shaping Europe's digital future. (2025, November

19). <https://digital-strategy.ec.europa.eu/en/library/digital-omnibus-regulation-proposal>

Directorate-General for Health and Food Safety

(European

Commission). (2026). *HealthData@EU central platform.* Publications Office of the European

Union. <https://data.europa.eu/doi/10.2875/1707164>

Doctolib. (2025, October 2). Futura. [https://www.futura-](https://www.futura-sciences.com/tech/definitions/logiciels-doctolib-27020/)

[sciences.com/tech/definitions/logiciels-doctolib-27020/](https://www.futura-sciences.com/tech/definitions/logiciels-doctolib-27020/)

Drumt, S., Chawla, K., Barbereau, T., Spagnuolo, D., & Burgwal, L. (2025). Secondary use

under the European Health Data Space: Setting the scene and towards a research agenda on

privacy-enhancing technologies. *Frontiers in Digital Health*, 7.

<https://doi.org/10.3389/fdgth.2025.1602101>

EFPIA position on EHDS. (2024, July 24). <https://www.efpia.eu/news-events/the-efpia->

[view/statements-press-releases/efpia-position-on-ehds/](#)

Efpia response to the Consultation on legislative proposal for a european health data space. (n.d.). Retrieved May 13, 2026, from <https://www.efpia.eu/media/676468/efpia-response-to-the-consultation-on-legislative-proposal-for-a-european-health-data-space.pdf>

EHDS. (n.d.). Findata. Retrieved April 21, 2026, from <https://findata.fi/en/services-and-instructions/ehds/>

eHDSI Monitoring Framework (KPIs). (2026, April 18). <https://experience.arcgis.com/experience/77f459be23e545b48f46a79cfaf19423>

Erlangsen, A., & Fedyszyn, I. (2015). Danish nationwide registers for public health and health-related research. *Scandinavian Journal of Public Health*, 43(4), 333–339. <https://doi.org/10.1177/1403494815575193>

Espace européen des données de santé (EEDS) | EUR-Lex. (2026, January 16). <https://eur-lex.europa.eu/FR/legal-content/summary/european-health-data-space-ehds.html>

Estonian e-Health Records. (2024, June 24). e-Estonia. <https://e-estonia.com/solutions/e-health-2/e-health-records/>

Estonian e-Health Records. (n.d.). Retrieved May 14, 2026, from <https://e-estonia.com/solutions/e-health-2/e-health-records/>

EU-U.S. Privacy Shield: Frequently Asked Questions. (2016, July 12). [Text]. European Commission - European Commission. https://ec.europa.eu/commission/presscorner/detail/it/memo_16_2462

European Cloud Providers' Local Market Share Now Holds Steady at 15% | Synergy Research Group. (2025, July 24). <https://www.srgresearch.com/articles/european-cloud-providers-local-market-share-now-holds-steady-at-15>

European Cloud Providers' Local Market Share Now Holds Steady at 15% | Synergy Research Group. (2025, July 24). <https://www.srgresearch.com/articles/european-cloud-providers-local-market-share-now-holds-steady-at-15>

European Commission launches accelerated infringement proceedings against Hungary over the independence of its central bank and data protection authorities as well as over measures affecting the judiciary. (n.d.). [Text]. European Commission - European Commission. Retrieved May 14, 2026, from https://ec.europa.eu/commission/presscorner/detail/en/https://ec.europa.eu/commission/presscorner/detail/en/ip_12_24

European Health Data Space Regulation (EHDS)—Public Health. (2026, March 26). https://health.ec.europa.eu/ehealth-digital-health-and-care/european-health-data-space-regulation-ehds_en

European Health Data Space Regulation: Digital revolution in healthcare - Informative Notes - Knowledge. (2025, March 26). PLMJ Transformative Legal Experts. <https://www.plmj.com/en/knowledge/informative-notes/European-Health-Data-Space-Regulation-digital-revolution-in-healthcare/33864/>

European Health Data Space: An important tool to bridge the digital gap. (2022, May 2). <https://www.amchameu.eu/news/european-health-data-space-important-tool-bridge-digital-gap>

European medicines agency cloud strategy accelerating innovation and digitalisation better public and animal health outcomes. (n.d.). Retrieved April 28, 2026, from https://www.ema.europa.eu/en/documents/other/european-medicines-agency-cloud-strategy-accelerating-innovation-and-digitalisation-better-public-and-animal-health-outcomes_en.pdf

FAQ in English | Health Data Hub. (n.d.). Retrieved April 24, 2026, from <https://www.health-data-hub.fr/page/faq-english>

Finland country visit factsheet. (n.d.). Retrieved May 14, 2026, from <https://tehdas.eu/app/uploads/2023/04/finland-country-visit-factsheet-04-2023.pdf>

FISA Section 702. (n.d.). Retrieved May 13, 2026, from <https://www.intel.gov/foreign-intelligence-surveillance-act/fisa-section-702>

Gartner | *Delivering Actionable, Objective Insight to Executives and Their Teams*. (2026). Gartner. <https://www.gartner.com/en/search>

Gesundheitsdatennutzungsgesetz (GDNG). (2024, March 26). BMG. <https://www.bundesgesundheitsministerium.de/service/gesetze-und-verordnungen/detail/gesundheitsdatennutzungsgesetz>

Greer, S. L., Jarman, H., Kulikoff, R., Panteli, D., van Ginneken, E., & Wismar, M. (2025). The second Trump administration: A policy analysis of challenges and opportunities for European health policymakers. *Health Policy (Amsterdam, Netherlands)*, 158, 105350. <https://doi.org/10.1016/j.healthpol.2025.105350>

GUIDELINE on the electronic exchange of health data under Cross-Border Directive 2011/24/EU Laboratory results. (n.d.). Retrieved April 21, 2026, from https://health.ec.europa.eu/document/download/4e8d82ba-87ca-4123-a8d8-a5d895ae8ecc_en?filename=ehealth_ehn-lab-results-guideline_en.pdf

Health crisis preparedness—European Commission. (n.d.). Retrieved April 20, 2026, from https://commission.europa.eu/topics/public-health/european-health-union/health-crisis-preparedness_en

Health Data Agency. (n.d.). *Faciliter la recherche, l'innovation et les meilleures politiques publiques grâce aux données*. Retrieved May 11, 2026, from https://www.hda.belgium.be/fr/about_us

Health | ENISA. (2025a, September 16). <https://www.enisa.europa.eu/topics/cybersecurity-of-critical-sectors/health>

Health | ENISA. (2025b, September 16). <https://www.enisa.europa.eu/topics/cybersecurity-of-critical-sectors/health>

HealthData@EU Central Platform—HealthData@EU. (n.d.). Retrieved April 21, 2026, from <https://acceptance.data.health.europa.eu/healthdata-central-platform?locale=en>

IGEDD. (2022). *Les enquêtes techniques*. IGEDD. <https://www.igedd.developpement-durable.gouv.fr/les-enquetes-techniques-a3022.html>

Information management | European Medicines Agency (EMA). (2016, October 20). <https://www.ema.europa.eu/en/about-us/how-we-work/information-management>

International data transfers | European Data Protection Board. (n.d.). Retrieved April 24, 2026, from https://www.edpb.europa.eu/sme-data-protection-guide/international-data-transfers_en

Jõgi, R., Timonen, J., Saastamoinen, L., Laius, O., & Volmer, D. (2023). Implementation of European Cross-border Electronic Prescription and Electronic Dispensing Service: Cross-sectional Survey. *Journal of Medical Internet Research*, 25, e42453. <https://doi.org/10.2196/42453>

Jones, C. I., & Tonetti, C. (2020). Nonrivalry and the Economics of Data. *American Economic Review*, 110(9), 2819–2858. <https://doi.org/10.1257/aer.20191330>

Jóri, A. (2012). The End of Independent Data Protection Supervision in Hungary – A Case Study. In S. Gutwirth, R. Leenes, P. de Hert, & Y. Pouillet (Eds.), *European Data Protection: Coming of Age* (pp. 395–406). Springer Netherlands. https://doi.org/10.1007/978-94-007-5170-5_18

Kanninen, T. (2025, March 26). European Health Data Space – Shaping the future of global health data. *EHDS - BC Platforms*. <https://ehds.bcplatforms.com/european-health-data-space-shaping-the-future-of-global-health-data/>

Kessissoglou, I. A., Cosgrove, S. M., Abboud, L. A., Bogaert, P., Peolsson, M., & Calleja, N. (2024). Are EU member states ready for the European Health Data Space? Lessons learnt on the secondary use of health data from the TEHDAS Joint Action. *European Journal of Public Health*, 34(6), 1102–1108. <https://doi.org/10.1093/eurpub/ckae160>

Khaski, J. (2026, April 23). Health Data Hub: Scaleway remplace (enfin) Microsoft. *Maddyness - Le média pour comprendre l'économie de demain*. <https://www.maddyness.com/2026/04/23/health-data-hub-scaleway-remplace-enfin-microsoft/>

Kjeldahl Bjerregaard Bjerrum, E., & Husum, E. (2025, March 17). *Final EHDS Regulation Adopted: Legal Insights for Cross-Border Health Data Management - Chambers and Partners | Researching Outstanding Lawyers Globally | chambers.com*. <https://chambers.com/legal-trends/update-on-the-european-health-data-space>

Kubota, K., & Ishibashi, S. (2025). Advancing real-world data integration in nursing research: A policy perspective on Japan's next-generation medical infrastructure law and the EU EHDS framework. *Japan Journal of Nursing Science*, 23(1), e70037. <https://doi.org/10.1111/jjns.70037>

La SNOMED CT et le NRC français. (2026, March 26). Agence du Numérique en Santé. <https://esante.gouv.fr/produits-services/cgts/snomed-ct>

Le règlement général sur la protection des données. (2018). Consilium. <https://www.consilium.europa.eu/fr/policies/data-protection-regulation/>

Les missions de la CNIL. (n.d.). Retrieved April 24, 2026, from <https://www.cnil.fr/fr/la-cnil/les-missions-de-la-cnil>

LOINC. (2026). LOINC. <https://loinc.org/>

Mapping China's Tech Giants | Australian Strategic Policy Institute. (n.d.). Mapping China's Tech Giants | Australian Strategic Policy Institute. Retrieved April 27, 2026, from <https://chinatechmap.aspi.org.au/>

Microsoft Corporation | lobbyfacts. (2025). <https://www.lobbyfacts.eu/datacard/microsoft-corporation?rid=0801162959-21>

Murgia, Y., Ciampi, M., Gazzarata, R., Sicuranza, M., Cirillo, F., Esposito, C., Maggi, N., Balestra, G., Sacchi, L., & Giacomini, M. (2025, December 8). *The challenges of national health data ecosystems in feeding the European health data space: The Italian example*. <https://www.frontiersin.org/journals/medicine/articles/10.3389/fmed.2025.1644719/full>

Murgia, Y., Gazzarata, R., Ciampi, M., Sicuranza, M., Cirillo, F., Esposito, C., Maggi, N., Balestra, G., Sacchi, L., & Giacomini, M. (2025). The challenges of national health data ecosystems in feeding the European health data space: The Italian example. *Frontiers in Medicine*, 12. <https://doi.org/10.3389/fmed.2025.1644719>

My rights over my health data—Public Health—European Commission. (2026, March 26). https://health.ec.europa.eu/ehealth-digital-health-and-care/my-rights-over-my-health-data_en

Navarro, P., & Zannotti, F. (2020, October 15). *In wake of the Schrems II, CNIL challenges use of Microsoft cloud storage to host public health data lakes (the Health Data Hub case – Part 1)*. Wwww.Hoganlovells.Com. https://www.hoganlovells.com/en/publications/in-wake-of-the-schrems-ii-cnil-challenges-the-use-of-microsoft-cloud-storage-to-host-public-health-data-lakes-the-health-data-hub-case-part-1_1

Norigami, M., & Silva, M. (2026, February 12). How Big Tech lobbying shapes EU tech regulation. *SOMO*. <https://www.somo.nl/how-big-tech-framed-eu-choices/>

OECD. (2019). *Health in the 21st Century: Putting Data to Work for Stronger Health Systems*. OECD Publishing. <https://doi.org/10.1787/e3b23f8e-en>

OECD. (2023). *Health at a Glance 2023: OECD Indicators*. OECD Publishing. <https://doi.org/10.1787/7a7afb35-en>

OHDSI. (2026). *Data Standardization*. <https://www.ohdsi.org/data-standardization/>

Omnibus numérique: L'EDPB et le CEPD soutiennent la simplification et la compétitivité tout en soulevant des préoccupations majeures | European Data Protection Board. (2026, February 11). https://www.edpb.europa.eu/news/news/2026/digital-omnibus-edpb-and-edps-support-simplification-and-competitiveness-while_fr

Omop-cdm. (n.d.). Retrieved April 21, 2026, from <https://www.health-data-hub.fr/sites/default/files/2025-03/omop-cdm.pdf>

Package 5: Sharing data for health. (n.d.). *Tehdas*. Retrieved April 21, 2026, from <https://tehdas.eu/tehdas1/packages/package-5-sharing-data-for-health/packages/package-5-sharing-data-for-health/>

Patient Summary Guideline (release 3.1). (n.d.). Retrieved April 21, 2026, from https://health.ec.europa.eu/system/files/2023-10/ehn_guidelines_patientsummary_en.pdf

Permits—Findata. (n.d.). Retrieved May 14, 2026, from <https://findata.fi/en/permits/>

Pollet, M. (2022, November 18). *Gaia-X déploie enfin ses ailes*. L'Usine Digitale. <https://www.usine-digitale.fr/article/gaia-x-deploie-enfin-ses-ailes.N2068507>

Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL (2025). <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52025PC0837>

Radley-Gardner, O., Beale, H., & Zimmermann, R. (Eds.). (2016). *Fundamental Texts On European Private Law* (2nd ed.). Hart Publishing Ltd.

<https://doi.org/10.5040/9781782258674>

Règlement (UE) 2025/327 du Parlement européen et du Conseil. (2025).

Règlement général sur la protection des données. (2016, April 27). <https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng>

Règlement relatif à l'espace européen des données de santé—Public Health. (2026, March 26). https://health.ec.europa.eu/ehealth-digital-health-and-care/european-health-data-space-regulation-ehds_fr

RÈGLEMENT (UE) 2016/ 679 DU PARLEMENT EUROPÉEN ET DU CONSEIL. (2016).

Revealed: Tech industry now spending record €151 million on lobbying the EU | Corporate Europe Observatory. (2025, October 27). <https://corporateeurope.org/en/2025/10/revealed-tech-industry-now-spending-record-eu151-million-lobbying-eu>

RGPD: De quoi parle-t-on ? (2026, April 18). <https://www.cnil.fr/fr/rgpd-de-quoi-parle-t-on>

Roussanov, A., & González-Lamuño, A. (2025, March 6). *European Health Data Space Regulation Published in the EU Official Journal | Advisories.* Arnold & Porter. <https://www.arnoldporter.com/en/perspectives/advisories/2025/03/european-health-data-space-regulation-published>

RTL Info. (2026, May 14). RTL Info. <http://www.rtl.be/>

S3NS annonce la qualification SecNumCloud de son offre Cloud de Confiance PREMI3NS | Thales Group. (2025, December 19). <https://www.thalesgroup.com/fr/actualites-du-groupe/communiqués-de-presse/s3ns-annonce-la-qualification-secnumcloud-de-son-offre>

Salgado, R. (2025). First Insights Into the U.S.-U.K. CLOUD Act Agreement. *Lawfare*.
<https://www.lawfaremedia.org/article/first-insights-into-the-u.s.-u.k.-cloud-act-agreement>

Schmidt, M., Schmidt, S. A. J., Adelborg, K., Sundbøll, J., Laugesen, K., Ehrenstein, V., & Sørensen, H. T. (2019). The Danish health care system and epidemiological research: From health care contacts to database records. *Clinical Epidemiology*, 11, 563–591.
<https://doi.org/10.2147/CLEP.S179083>

Services and instructions. (2026, February 4). Findata. <https://findata.fi/en/services-and-instructions/>

Simitis, S. (1984). Die informationelle Selbstbestimmung, Grundbedingung einer verfassungskonformen Informationsordnung. *Neue juristische Wochenschrift : NJW, Neue juristische Wochenschrift : NJW. - München : Beck, ISSN 0341-1915, ZDB-ID 200146-9. - Vol. 37.1984, 8, p. 398-405, 37(8), 398.*

Sissoko-Noblot, M. (2025, February 20). L'éphémère suspension de TikTok aux États-Unis, un conflit entre sécurité nationale et liberté d'expression Par Marie Sissoko-Noblot. *JP blog*.
<http://blog.juspoliticum.com/2025/02/20/lephemere-suspension-de-tiktok-aux-etats-unis-un-conflit-entre-securite-nationale-et-liberte-dexpression-par-marie-sissoko-noblot/>

Standard Contractual Clauses (SCC)—Commission européenne. (2021, June 4).
https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_fr

Sweden country visit factsheet. (n.d.). Retrieved May 14, 2026, from
<https://tehdas.eu/app/uploads/2023/03/sweden-country-visit-factsheet-03-2023.pdf>

Synthesis report 2025. (n.d.). Retrieved May 14, 2026, from
https://health.ec.europa.eu/document/download/f1d320de-6157-49fb-ac35-7cbdd4e426a5_en?filename=state_2025_synthesis_report_en.pdf

TEHDAS Estonia country visit factsheet. (n.d.). Retrieved April 20, 2026, from <https://tehdas.eu/app/uploads/2023/03/estonia-country-visit-factsheets-10-2022.pdf>

The CLOUD Act. (n.d.). Retrieved April 27, 2026, from <https://www.eurojust.europa.eu/sites/default/files/assets/the-cloud-act.pdf>

The Draghi report on EU competitiveness. (2024, September 9). https://commission.europa.eu/topics/competitiveness/draghi-report_en

The EU-US Safe Harbour Agreement. (2012, April 20). Epthinktank. <https://epthinktank.eu/2012/04/20/croatias-european-elections-14-april-2013/>

The European Union general data protection regulation: What it is and what it means.* (2019, February 10). <https://www.tandfonline.com/doi/full/10.1080/13600834.2019.1573501#d1e187>

The future of European competitiveness Part B | In-depth analysis and recommendations. (n.d.). Retrieved April 18, 2026, from https://commission.europa.eu/document/download/ec1409c1-d4b4-4882-8bdd-3519f86bbb92_en?filename=The%20future%20of%20European%20competitiveness_%20In-depth%20analysis%20and%20recommendations_0.pdf

The Health Data Use Act: Expanding the infrastructure for health data in Germany | Gleiss Lutz. (2024, February 13). <https://www.gleisslutz.com/en/know-how/health-data-use-act-expanding-infrastructure-health-data-germany>

The Lancet Regional Health – Europe. (2025). The Italian health data system is broken. *The Lancet Regional Health - Europe*, 48, 101206. <https://doi.org/10.1016/j.lanepe.2024.101206>

The pharmaceutical industry in figures. (n.d.). Retrieved April 20, 2026, from <https://www.efpia.eu/media/uj0popel/the-pharmaceutical-industry-in-figures-2025.pdf>

Tschammler, D., van der Merwe, D., & Mobasser, O. (2025, April 17). Preparing for the European Health Data Space—Opportunities and Challenges for Europe’s Digital Future. *Global Privacy & Security Compliance Blog*.

<https://www.globalprivacyblog.com/2025/04/preparing-for-the-european-health-data-space-opportunities-and-challenges-for-europes-digital-future/>

Un projet européen pour mieux soigner, innover et prévenir. (n.d.). Retrieved April 21, 2026, from <https://www.hda.belgium.be/sites/default/files/documents/2025-05/FR%20-%20Article%20EHDS.pdf>

Value of data report. (n.d.). Retrieved April 20, 2026, from https://www.bennettschool.cam.ac.uk/wp-content/uploads/2020/12/Value_of_data_Policy_Implications_Report_26_Feb_ok4noWn.pdf

VELLIET, M. (2023, January 31). *Digital Sovereignty: European Policies, American Dilemmas* | Ifri. <https://www.ifri.org/en/papers/digital-sovereignty-european-policies-american-dilemmas>

Watkins, L. &. (2025, April 17). Preparing for the European Health Data Space—Opportunities and Challenges for Europe’s Digital Future. *Global Privacy & Security Compliance Blog*. <https://www.globalprivacyblog.com/2025/04/preparing-for-the-european-health-data-space-opportunities-and-challenges-for-europes-digital-future/>

What is EHRxF? (2026). <https://ehr-exchange-format.eu/what-is-ehrx/>

What is Zero Trust For the Cloud? (n.d.). Fortinet. Retrieved April 21, 2026, from <https://www.fortinet.com/resources/cyberglossary/zero-trust-for-the-cloud>

White Paper Demystifying the debate on the US CLOUD Act vs European/UK Data Sovereignty in the context of cloud services. (2026, February 3). <https://cms.law/en/bel/legal-updates/white-paper-demystifying-the-debate-on-the-us-cloud-act-vs-european-uk-data->

[sovereignty-in-the-context-of-cloud-services](#)

The European Health Data Space (EHDS), adopted in February 2025, represents a landmark step in the European Union's ambition to build a unified framework for the sharing and reuse of health data across Member States. By establishing harmonised standards for primary and secondary use of health data, the EHDS aims to improve patient care, accelerate medical research, and reinforce European digital sovereignty in the health sector.

This thesis examines the conditions under which the EHDS can effectively fulfil its objectives, with a particular focus on the legal and geopolitical challenges it faces. The analysis covers three interconnected dimensions: the technical and institutional architecture of the regulation, the fragility of the transatlantic data transfer framework on which it partly relies, and the internal tensions within the European Union itself.

The thesis argues that while the EHDS provides a solid legal foundation, its success is far from guaranteed. The instability of the Data Privacy Framework, the paralysis of the PCLOB under the second Trump administration, and the proposed redefinition of personal data under the Digital Omnibus package all represent structural vulnerabilities that could undermine the regulation before it is fully deployed. Ultimately, the EHDS can only succeed if the European Union remains coherent with the values and principles on which it was built ; choosing genuine digital sovereignty over short-term competitiveness, and ensuring that the legislative framework surrounding the regulation does not contradict its own foundations.

UNIVERSITÉ CATHOLIQUE DE LOUVAIN
Louvain School of Management

Place des Doyens, 1 bte L2.01.01, 1348 Louvain-la-Neuve
Boulevard Emile Devreux 6, 6000 Charleroi, Belgique
Chaussée de Binche 151, 7000 Mons, Belgique

www.uclouvain.be/lsm