International Journal of Law and Information Technology, 2024, **32**, eaae006
https://doi.org/10.1093/ijlit/eaae006
Advance access publication 6 July 2024
Article

OXFORD

Will the real data sovereign please stand up? An EU policy response to sovereignty in data spaces

Mark Ryan[*], Paula Gürtler[†], Artur Bogucki[‡]

ABSTRACT

This paper aims to evaluate the concept of data sovereignty as applied to data spaces, particularly the Common European Data Space (CEDS). The CEDS aims to develop a single European data market through nine domain-specific data spaces: health, industrial and manufacturing, agriculture, finance, mobility, Green Deal, energy, public administration, and skills. It aims to do this by providing a secure and trustworthy technical architecture, a robust data-sharing business model realized through effective governance, and ensuring data sovereignty. Ensuring data sovereignty, however, is challenging when different agents all claim authority over their data within a data space. This paper focuses on three data sovereign agents in the CEDS—individual, organization, and state—to examine how data sovereignty can be implemented in data spaces based on current European Union regulations and whether shortcomings still need to be addressed.

KEYWORDS: common European data space; European strategy for data; data sovereignty; cyberlaw; power; policy.

INTRODUCTION

A European Strategy for Data envisions three core objectives: promoting free data flow, respecting European rules and values, and establishing fair and practical rules for data access and use.[1] The European Union (EU) is implementing new legislative measures to achieve these goals, including a cross-sectoral governance framework, the Data Governance Act[2] for data access, making more high-quality public sector data available for re-use, and the Data Act[3] for horizontal

[*] Mark Ryan, Wageningen Economic Research, Wageningen University & Research, Droevendaalsesteeg 4, 6708 PB, Wageningen, the Netherlands. Tel: +31634230163; Email: mark.ryan@wur.nl;
[†] Paula Gürtler, Centre for European Policy Studies, Brussels, Belgium. Tel: +32(0)22293911; Email: paula.gurtler@ceps.eu
[‡] Artur Bogucki, Centre for European Policy Studies, Brussels, Belgium. Tel: +32(0)22293911; Email: artur.bogucki@ceps.eu

[1] Commission, 'A European Strategy for Data' (Communication) (2020) COM 66 final (European Data Strategy).
[2] Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 [2022] OJ L152/1 (Data Governance Act).
[3] Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonized rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 [2023] OJ L2023/2854 (Data Act).

data sharing. Data spaces have been highlighted as a central component of implementing the Commission's Strategy to overcome barriers to data sharing across organizations by combining necessary tools and infrastructures and addressing trust issues. While the European Data Strategy aims to develop data spaces in nine strategic domain areas such as health, industrial and manufacturing, agriculture, finance, mobility, Green Deal, energy, public administration, and skills, there is, thus far, limited direction on how these spaces should be implemented, governed, and regulated.

The concept of 'data spaces' is relatively new, having been established only 15 years ago in computer science to describe a physical integration of data, where data should be left 'stored at the source'.[4] Data spaces do not require a standard database schema and allow for the coexistence of different types of data with integration 'achieved on a semantic level using shared vocabularies'.[5] Because there is no central place to store data, data exchange occurs directly between participants in this decentralized 'data space'.[6]

Businesses benefit from access to data spaces, as this solution fosters innovative data services conducted cooperatively. It helps break away from the information silos that are often isolated with individual data holders, domains, industries, and countries.[7] The main goal of data spaces is to provide support and functionality for sharing varying data sources in the data ecosystem.[8] While data spaces began as a technical way to support data sharing, data spaces now cover many other domains, such as law, business, governance, and ethics.[9]

The common European data spaces (CEDS) is an EU initiative that aims to provide large-scale collections of data at much lower upfront costs for European businesses,[10] to provide a 'level playing field for data sharing and exchange, leading to less dominance of, and dependency on, large, quasi-monopolistic players'.[11] The nine data spaces of the CEDS aim to ensure that Europeans benefit from data sharing, increase European competitiveness, and protect the data sovereignty of European citizens and businesses.[12] This final goal is the focus of this paper.

While the ambition of data sovereignty might be a worthwhile goal for the CEDS, its precise meaning and implementability is sometimes unclear: '*Data sovereignty* might be seen as a term whose meaning is obvious and self-explanatory, and awareness of alternative meanings is lacking'.[13] While the term 'sovereignty' has traditionally been used to define a monarch or government's

[4] Boris Otto, 'The Evolution of Data Spaces' in Boris Otto, Michael ten Hompel and Stefan Wrobel (eds), *Designing Data Spaces: The Ecosystem Approach to Competitive Advantage* (Springer Nature, Cham, Switzerland 2022) 3.

[5] ibid 7.

[6] Fabian Kirstein and Vincent Bohlen, 'IDS as a Foundation for Open Data Ecosystems' in Boris Otto, Michael ten Hompel and Stefan Wrobel (eds), *Designing Data Spaces: The Ecosystem Approach to Competitive Advantage* (Springer Nature, Cham, Switzerland 2022) 225; Simon Scerri and others, 'Common European Data Spaces: Challenges and Opportunities' in Edward Curry, Simon Scerri and Tuomo Tuikka (eds), *Data Spaces* (Springer Cham, Cham, Switzerland 2022) 337.

[7] Arnaud Braud and others, 'The Road to European Digital Sovereignty with Gaia-X and IDSA' (2021) 35 IEEE Network 4.

[8] A data ecosystem is a complex system of intertwined actors and networks that are involved in, and contribute to, data collection, sharing, and use. These actors and networks can often vary between different sectors. Data spaces are located within larger data ecosystems, but also relate to and can change the dynamic of those ecosystems; Alon Halevy, Michael Franklin and David Maier, 'Principles of Dataspace Systems' Proceedings of the Twenty-Fifth ACM SIGMOD-SIGACT-SIGART Symposium on Principles of Database Systems, 2006.

[9] Edward Curry and Tuomo Tuikka, 'An Organizational Maturity Model for Data Spaces: A Data Sharing Wheel Approach' in Edward Curry, Simon Scerri and Tuomo Tuikka (eds), *Data Spaces* (Springer Cham, Cham, Switzerland 2022) 21.

[10] Cornelia Hedeler and others, 'Dataspaces' in Stefano Ceri and Marco Brambilla (eds), *Search Computing* (Springer 2010) 114; Cornelia Hedeler and others, 'Pay-as-You-Go Mapping Selection in Dataspaces' Proceedings of the 2011 ACM SIGMOD International Conference on Management of Data, 2011; Anish Das Sarma, Xin Luna Dong and Alon Y Halevy, 'Data Modeling in Dataspace Support Platforms' in Alexander T Borgida and others (eds), *Conceptual Modeling: Foundations and Applications* (Springer, Berlin, Germany 2009) 122.

[11] Lars Nagel and Douwe Lycklama, 'How to Build, Run, and Govern Data Spaces' in Boris Otto, Michael ten Hompel and Stefan Wrobel (eds), *Designing Data Spaces: The Ecosystem Approach to Competitive Advantage* (Springer Nature, Cham, Switzerland 2022) 18.

[12] Edward Curry, 'Common European Data Spaces' (Real-time Linked Dataspaces) <http://dataspaces.info/common-european-data-spaces/#page-content> accessed 13 October 2023.

[13] Patrik Hummel and others, 'Data Sovereignty: A Review' (2021) 8 Big Data & Society 2053951720982012. 13.

absolute control over a nation and its territory; how this meaning can be translated into the context of data spaces is unclear. Despite European politicians commonly making references to data sovereignty, it remains sparse in policy documents.[14] It is a popular political concept, despite rarely appearing in legislation and lacking legal definition. However, this trend may indicate that data sovereignty will take on greater significance for data policy in the future, for example, in data spaces, despite an as-yet shallow understanding of what it implies in different contexts and applications. This paper aims to pre-empt this issue by highlighting some of the main challenges of implementing data sovereignty in practice, particularly in data spaces such as the CEDS.

Thus far, very little research has been conducted regarding how data sovereignty applies to data spaces (such as the CEDS) and how it is taken up and implemented in EU legislation. As part of our research for this paper, we analysed 64 articles that focus on data sovereignty in the context of data spaces. One overarching finding from this analysis is that the meaning of data sovereignty is often viewed as uncontroversial and self-explanatory. Nonetheless, data sovereignty was defined in many different ways in the data space literature, implying different understandings and interpretations of its meaning and application. Accurately defining and understanding what data sovereignty means in European data spaces is particularly significant to ensure that stakeholders are not talking past one another or misinterpreting what policy and actions need to be taken in its name.[15] Defining and creating a taxonomy, as well as providing appropriate interpretations of the term, are crucial steps for understanding whether, and how, data sovereignty should be implemented in practice. This involves determining how current regulatory approaches and legislation substantiate enactment of data sovereignty within the context of CEDS. For this purpose, we analysed the 10 European legislative acts for their impact on values commonly identified with data sovereignty of different agents.

The Historical context of EU data governance section of this paper outlines the European data policy landscape and the emergence of the CEDS as a vital ambition for the EU. It explores how the concept of data sovereignty has developed to protect actors and encourage data space uptake. The Defining data sovereignty in data spaces section presents the methodology used in this paper and, based on the literature, claims that data sovereignty in data spaces can be defined by three central characteristics: (i) as a type of control in data spaces; (ii) over the access, use, storage, and sharing of one's data; (iii) by an individual, organization, or state.

While many different values (eg, privacy, security, and ownership) are closely related to or used synonymously with data sovereignty, data sovereignty is a specific *control* over how one's data is shared, stored, accessed, and used (characteristics (i) and (ii) above). While these two characteristics of data sovereignty are relatively uncontroversial, the third characteristic which focuses on the type of agents that can execute sovereignty over data is more problematic. The Challenges of data sovereign agents in CEDS section elaborates on the notions of individual, organizational, and state data sovereignty, and proposes that there are issues with all three types of data sovereignty when the landscape of EU data law is applied and tested against them.

This paper presents the argument that much of European law, especially the General Data Protection Regulation (GDPR),[16] adequately embeds the objectives of protecting individuals sharing data and data sovereignty in the normative core of the legislation but it is not effectively implemented in practice. In addition, there is no clear plan in place regarding how individuals can monetize their data in CEDS. This monetization of personal data was discussed in the data

[14] For example, in Commission 'Commission staff working document on Common European Data Spaces' (Staff Working Document) SWD (2022) 45 final and COM (2020) 66 final

[15] Hummel and others (n 13).

[16] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC [2016] OJ L119/1 (General Data Protection Regulation)' (GDPR)

strategy, which suggested that they would appear in the Data Act (but have not). Without the additional aspect of data monetization, we will propose that it is unclear what the added value of data sovereignty is compared with rights under the GDPR.

Secondly, we argue that applying data sovereignty to organizations in the data space is an idealistic and naive promise. Current policy is often overly restrictive regarding what an organization can do with their data (namely organizational data sovereignty), and there is vagueness around involuntary data-sharing requirements in both the Data Strategy and the Data Act. Furthermore, the data sovereignty of organizations is undermined in the first sectoral proposal from the CEDS, namely the European Health Data Space (EHDS) because it imposes substantial procedural risks and limitations on business data, such as the limited ability to opt out of data sharing arrangements in times of 'exceptional need'.[17]

Thirdly, in the context of state data sovereignty, this paper claims that the data sovereignty of states is a delegation of control to the EU on the assumption that the EU can manage and control the CEDS. It is very unclear whether the EU will function as a centralized authority over the CEDS or what level of control it will have over this process. The lack of clarity is exemplified in the EHDS case, where the EU is the regulator of the data space, and the Member States are the administrators and decision-makers on data access in specific cases. Additional complexities apply in the case of cross-border health databases, where, in exceptional cases, the sovereignty of one Member State might affect another Member State.

Overall, in this paper, we examine what data sovereignty means in the context of CEDS and whether current EU policy is sufficient for its implementation and protection. The main conceptual and practical challenges lie in making data sovereignty concrete and ensuring that all agents that we would like to be sovereign can be sovereign. While the data sovereignty of individuals appears to be sufficiently enabled by current data privacy regulations, the implementation of the GDPR is lacking to effectively protect the rights of individuals. It is unclear through which mechanisms individual data sovereignty (IDS) and the CEDS would improve enforcement of individual control over data compared to existing regulation. In terms of organizational data sovereignty (ODS), it promises organizations more control over their data. On the other hand, exceptions for public interest in current regulation (like the Data Act) limit ODS to a certain extent. Finally, the complexity of state sovereignty in the European Union and the shared sovereignty over state data policy between Member States and Union institutions illustrates that control over data for any of the three agents (individual, organization, and state) is best understood as malleable and a dynamic relationship between agents that can be leveraged towards specific goals.

HISTORICAL CONTEXT OF EU DATA GOVERNANCE

The increasing importance of data in contemporary society has brought regulatory focus to the implications of data governance on politics, democracy, human rights, security, health, and other areas.[18] Data governance encompasses the methods that various actors, such as states, international organizations, local authorities, and private companies, employ to manage digital data collection, processing, transfer, sharing, and general utilization.[19] A surge in regulation has expanded domestic, regional, and international levels, partly prompted by the call for increased oversight.[20]

[17] Commission, 'Proposal for a Regulation of the European Parliament and the Council on the European Health Data Space' (2022) COM 197 final

[18] Sara E Davies and Clare Wenham, 'Why the COVID-19 Response Needs International Relations' (2020) 96 Int Affairs 1227.

[19] Mira Burri, 'Data Flows and Global Trade Law' in Mira Burri (ed), *Big Data and Global Trade Law* (Cambridge University Press, Cambridge, UK 2021).

[20] Alex Hern, 'Apple Chief Calls for Laws to Tackle "shadow Economy" of Data Firms' (The Guardian, 17 January 2019) <https://www.theguardian.com/technology/2019/jan/17/apple-chief-tim-cook-calls-for-laws-to-tackle-shadow-economy-of-data-firms> accessed 13 October 2023.

Two pivotal instruments, the 1995 Data Protection Directive[21] and the GDPR, marked significant shifts in the EU's data protection governance regime, forming the backbone of the EU's transformation into regulating the digital economy.[22] This evolution, involving EU institutions, Member States, and national data protection authorities (DPAs), is characterized by gradual harmonization, constitutionalization, and agencification at the EU level while allowing for specific national carve-outs. The GDPR remains the only 'EU digital acquis' with any substantial practical history regarding data governance, with the possibility to draw on a few years' worth of European Court of Justice adjudications, national rulings, and legal doctrine. We refer to other EU digital acquis further in this section, providing a historical overview illustrating how data governance evolved from a human rights-centric approach towards competition and innovation policy-centric design.

Despite the shift towards shared standards,[23] divergent approaches to data governance have given rise to power struggles and strained transnational, particularly transatlantic, relationships.[24] In 2013, the European Centre for Political Economy projected that significant disruptions in transatlantic data transfers could diminish the EU GDP by between 0.8% and 1.3%.[25] Competing claims for control have caused multiple interruptions in the transatlantic data transfer regime. On two occasions, in 2015 and again in 2020, the Court of Justice of the European Union (CJEU) invalidated the principal transatlantic data-sharing agreement,[26] leaving thousands of businesses grappling with legal uncertainty.[27] The Snowden and Cambridge Analytica scandals of 2013 and 2018 have further highlighted the need for more effective data governance.[28]

Data protection in the EU

The 1995 Directive established several principles and features in the EU's data protection landscape, marking the beginning of EU data protection. These include data quality requirements, criteria for processing personal data, limitations on data usage, security requirements, a system of notification, protection of special categories of data, and individual rights concerning data processing.[29] The Directive's governance introduced several vital points. The Commission's role was primarily to monitor the Directive's implementation—requiring transposition into national law—without additional rule-making powers. The Directive had potential extraterritorial reach and solidified the network of DPAs, giving them significant power.[30] It introduced a risk-based regulation system, kept enforcement at the national level, and brought a hybrid system of 'regulated self-regulation' through certification and codes of conduct.

The GDPR is the European Union's pivotal governance milestone in data protection. Proposed in 2012 but only adopted in 2016 and effective from 2018, it responded to challenges and

[21] Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L281/31 (1995 Directive).

[22] Anke Sophia Obendiek, 'What Are We Actually Talking About? Conceptualizing Data as a Governable Object in Overlapping Jurisdictions' (2022) 66 Int Stud Quart sqab080.

[23] Anu Bradford, *The Brussels Effect: How the European Union Rules the World* (Oxford Academic, New York 2020).

[24] Henry Farrell and Abraham L Newman, *Of Privacy and Power: The Transatlantic Struggle over Freedom and Security* (Princeton University Press, New Jersey 2019).

[25] Matthias Bauer and others, 'The Economic Importance of Getting Data Protection Right: Protecting Privacy, Transmitting Data, Moving Commerce' (European Centre for International Political Economy (ECIPE) March 2013) 3 <https://www.uschamber.com/assets/archived/images/documents/files/020508_EconomicImportance_Final_Revised_lr.pdf> accessed 13 October 2023.

[26] Case C-362/14 *Maximillian Schrems v Data Protection Commissioner* (Schrems I) [2015] ECLI:EU:C:2015:650 and Case C-311/18 *Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems* (Schrems II) [2020] ECLI:EU:C:2020:559.

[27] Obendiek (n 22).

[28] Nikhil Kalyanpur and Abraham L Newman, 'The MNC-Coalition Paradox: Issue Salience, Foreign Firms and the General Data Protection Regulation' (2019) 57 JCMS 448.

[29] Michael Birnhack, 'The EU Data Protection Directive: An Engine of a Global Regime' (16 September 2008) <https://papers.ssrn.com/abstract=1268744> accessed 13 October 2023.

[30] Spiros Simitis, 'From the Market to the Polis: The EU Directive on the Protection of Personal Data Symposium: Data Protection Law and the European Union's Directive' (1994) 80 Iowa LR 445.

developments that rendered the 1995 Directive inadequate.[31] Three key drivers influenced the GDPR's conception. Firstly, the EU underwent treaty changes that enhanced the importance of data protection. Amending the Lisbon Treaty[32] played a crucial role, recognizing data protection as an essential right in the EU. Changes were meant to integrate the Charter of Fundamental Rights of the European Union (CFREU)[33] into EU law, which cemented data protection's constitutional underpinning.[34] Secondly, economic and technological shifts, especially the growing prevalence of the internet, pressured the EU to update its governance model to meet contemporary demands.[35] Lastly, issues stemming from the 1995 Directive, such as fragmentation and ineffectiveness, required attention.[36]

Notably, the GDPR introduced several key features. It transitioned from a directive to a regulation, directly binding its principles across the EU. It established data protection as a fundamental right,[37] extended its reach beyond EU borders,[38] and imposed higher, uniform sanctions for rule breaches.[39] The GDPR also strengthened DPAs, introduced Data Protection Impact Assessments, mandated the appointment of Data Protection Officers (DPOs), and maintained the committee for evaluating third-country data protection frameworks.[40]

Although the primary focus of the GDPR is on safeguarding individual rights (as emphasized in multiple sources[41]), it was also designed as a crucial element of a Digital Single Market driven by enhanced horizontal data flows.[42] The EU's 2017 strategy for establishing a Data Economy[43] acknowledged the GDPR as 'the cornerstone for the uninhibited flow of personal data within the EU'.

The digital single market and the emergence of data spaces

Enhancing horizontal data flows emerged as a crucial factor for the Digital Single Market project. Creating a European data ecosystem within the single market necessitated harmonized rules for data management and flowed across the EU. The Digital Single Market strategy[44] and the strategy for fostering a European Data Economy sought to lessen constraints on data movement, including protectionist actions like localization mandates.

The 2018 Regulation on a Framework for the Free Flow of Nonpersonal Data[45] eliminated several obstacles to data flow, primarily by prohibiting data localization and vendor lock-in. The

[31] Kalyanpur and Newman (n 28); David Landau, 'Abusive Constitutionalism' (3 April 2013) <https://papers.ssrn.com/abstract=2244629> accessed 13 October 2023; Moritz Laurer and Timo Seidl, 'Regulating the European Data-Driven Economy: A Case Study on the General Data Protection Regulation' (2021) 13 Policy Internet 257.

[32] Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community [2007] OJ C306/1.

[33] Charter of Fundamental Rights of the European Union [2010] OJ C83/389

[34] Koen Lenaerts and others (eds), *EU Constitutional Law* (Oxford University Press, Oxford 2022).

[35] Jenna Lindqvist, 'New Challenges to Personal Data Processing Agreements: Is the GDPR Fit to Deal with Contract, Accountability and Liability in a World of the Internet of Things?' (2018) 26 Int J Law Inform Technol 45.

[36] Alessandro Mantelero and others, 'The Common EU Approach to Personal Data and Cybersecurity Regulation' (2020) 28 Int J Law Inform Technol 297.

[37] Kalyanpur and Newman (n 28); Laurer and Seidl (n 31).

[38] Laima Jančiūtė, 'EU Data Protection and "TreatyBase Games": When Fundamental Rights Are Wearing Marketmaking Clothes' in Serge Gutwirth and others (eds), *Data Protection and Privacy: The Age of Intelligent Machines* (Hart Publishing 2017).

[39] Julia Hörnle, 'Juggling More than Three Balls at Once: Multilevel Jurisdictional Challenges in EU Data Protection Regulation' (2019) 27 Int J Law Inform Technol 142.

[40] Thomas Streinz, 'The Evolution of European Data Law' (18 January 2021) <https://papers.ssrn.com/abstract=3762971> accessed 13 October 2023.

[41] Nihit Goyal, Michael Howlett and Araz Taeihagh, 'Why and How Does the Regulation of Emerging Technologies Occur? Explaining the Adoption of the EU General Data Protection Regulation Using the Multiple Streams Framework' (2021) 15 Regulat Govern 1020; Kalyanpur and Newman (n 28); Laurer and Seidl (n 31).

[42] Maja Brkan, 'Do Algorithms Rule the World? Algorithmic Decision-Making and Data Protection in the Framework of the GDPR and Beyond' (2019) 27 Int J Law Inform Technol 91.

[43] Commission, 'Building a European Data Economy' (2017) COM 9 final.

[44] Commission, 'A Digital Single Market Strategy for Europe' (2015) COM 192 final.

[45] Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of nonpersonal data [2018] OJ L303/59 (Regulation on the free flow of non-personal data).

Open Data Directive[46], which was implemented after the 2018 Regulation, sought to make data more accessible and promote the reutilization of public sector information. This directive mandates that public sector entities make data available with minimal restrictions, except in some instances, such as those involving intellectual property rights or exclusive agreements.[47]

The Open Data Directive, as a preparatory step towards the European Data Strategy, was intended to make data sources more accessible and fortify EU businesses against sizable non-EU competitors. This protection from non-EU competitors would be achieved by promoting equitable competition and straightforward market entry. The Directive concentrated on lowering market access hurdles for small and medium-sized enterprises (SMEs) and mitigating the disproportionate first-mover advantage favouring big corporations.[48]

The Open Data Directive was proceeded by the Data Governance Act proposal (DGA) of 2020. The DGA aims to address public sector data not included in the Open Data Directive due to specific protections, such as intellectual property rights, commercial or statistical confidentiality, or data protection limitations.[49] The Act also seeks to simplify data sharing by establishing standardized rules for data exchanges.[50] Its objectives are to enhance data access, decrease data procurement costs for businesses, ease the transfer of nonpersonal data between companies, and enable the sharing of personal data through designated intermediaries. It also defines the obligations of data intermediary service providers, or data brokers, that are key for data sharing on a larger scale.[51]

The DGA was created with the conviction that, according to DGA Recital 2, the 'data economy should be organized in a way that allows businesses, particularly micro-enterprises, SMEs, and startups, to flourish, ensuring neutral access to data, portability, and interoperability, while avoiding the consequences of lock-in'. The aim was to establish an even playing field in the data economy, where a competitive advantage is gained from the quality of services offered rather than businesses' data volume. The DGA also oversees the flow of nonpersonal data to non-EU countries, enabling the EU to make adequacy decisions. Instead of encouraging data to flow outward, the EU has based its policy on the Schrems II ruling, curtailing the outward flow of personal data. Similarly, the DGA restricts the outward flow of industrial data—a position so conspicuous that Commissioner Vestager had to deny that the DGA was a protectionist measure during a press conference discussing the policy.[52]

This push for an even playing field is also reflected in the Data Strategy's recognition that 'a handful of Big Tech companies possess a significant portion of the world's data, 'limiting the chances for EU-based 'data-driven businesses to emerge, grow, and innovate'.[53] The Data Strategy sought to lay the groundwork for the EU's future competitiveness by constructing a European data space and allowing EU businesses to benefit from the powerful Single Market when it comes to the data-enabled economy.[54]

[46] Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information [2019] OJ L172/56 (Open Data Directive).

[47] Vincenzo Iaia, 'The Remodelled Intersection between Copyright and Antitrust Law to Straighten the Bargaining Power Asymmetries in the Digital Platform Economy' (2021) 29 Int J Law Inform Technol 169.

[48] European Commission, 'Open Data' (Shaping Europe's Digital Future) <https://digital-strategy.ec.europa.eu/en/policies/psi-open-data> accessed 13 October 2023.

[49] Natasha Lomas, 'EU Lawmakers Agree Data Reuse Rules to Foster AI and R&D' (TechCrunch, 1 December 2021) <https://techcrunch.com/2021/12/01/data-governance-act-provisional-agreement/?guccounter=2> accessed 13 October 2023.

[50] Andrés Chomczyk Penedo and Pablo Trigo Kramcsák, 'Can the European Financial Data Space Remove Bias in Financial AI Development? Opportunities and Regulatory Challenges' (2023) Int J Law Inform Technol eaad020.

[51] Shivangi Mishra, 'The Dark Industry of Data Brokers: Need for Regulation?' (2021) 29 Inter J Law Informat Technol 395.

[52] Lomas (n 50).

[53] COM (2020) 66 final 3.

[54] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC [2022] OJ L277/1 (The Digital Services Act) (DSA) and the Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 [2022] OJ L265/1 (Digital Markets Act) (DMA) are integral to the broader initiative of establishing a Digital Single Market. These policies aim to enhance the competitive

Another crucial step towards the emergence of data spaces is the Data Act, which has the overarching goal of fostering a fair data-driven economy.[55] As Internal Market Commissioner Breton stated, the Data Act aims to 'ensure that industrial data is shared, stored and processed in full respect of European rules. It will form the cornerstone of a strong, innovative, and sovereign European digital economy'.[56] Beyond merely amplifying data flows, the Data Act also directly impacts consumer protection and competition. By granting users the ability to access data generated by digital products, such as Internet of Things devices and software, and allowing them to share them with third parties—while simultaneously prohibiting tech giants from doing the same with third-party data—the Act enhances competition in digital markets and challenges established market positions. It is a complementary measure to previous regulations and is celebrated as 'a significant stride towards establishing a single European data market'.[57] It concentrates on machine-generated data and sets forth standards for data sharing and (re-) utilization by specifying who can derive value from data and in what manner, as per DGA Recital 45. The Data Act empowers users, rather than just technology providers, to access data generated by technologies they operate and convey it to third parties offering aftermarket services. Additionally, the Data Act encourages data flow by imposing portability requirements that make it easier to switch cloud providers.

These policies and activities are secondary to the goal of a single European data market, ultimately culminating and being realized through the CEDS (the fourth pillar of the European Data Strategy). The nine domain-specific data spaces are health, industrial and manufacturing, agriculture, finance, mobility, Green Deal, energy, public administration, and skills.[58] While it is not the first attempt at creating data spaces (there is also the International Data Space[59] and GAIA-X[60]), the CEDS focuses on data spaces in a European context to pursue a single European data market.[61]

Alongside a digital single market, EU politicians have simultaneously promoted the goal of (technological, digital, and data) sovereignty in response to dependency on technology providers at national and Union levels. For example, Commission President Ursula von der Leyen accentuated the need for investment in 'European tech sovereignty'[62] and French President E. Macron emphasized the importance of sovereignty at the European level, linking it to regulatory frameworks, the protection of liberties, and using data for economic growth as a cornerstone of European digital policy[63]. Thierry Breton, then European Commissioner for Internal

position of EU businesses in relation to non-EU businesses when it comes to data access and usage. By imposing transparency requirements and other regulations on larger platforms, which primarily impact non-EU businesses, these policies help tilt the balance in favor of EU businesses.

55 Council of the European Union, 'Data Act: Council Adopts New Law on Fair Access to and Use of Data' (Press Release, 27 November 2023) <https://www.consilium.europa.eu/en/press/press-releases/2023/11/27/data-act-council-adopts-new-law-on-fair-access-to-and-use-of-data/> accessed 11 December 2023.

56 European Commission, 'Data Act: Commission Proposes Measures for a Fair and Innovative Data Economy' (Press Release, 23 February 2022) <https://ec.europa.eu/commission/presscorner/detail/en/ip_22_1113> accessed 11 December 2023.

57 Margrethe Vestager, 'Speech by Executive Vice-President Vestager on the Data Act' (European Commission, 23 February 2022) <https://ec.europa.eu/commission/presscorner/detail/%20en/speech_22_1312> accessed 13 October 2023.

58 Curry (n 12).

59 The International Data Space Association (since 2015) is a worldwide alliance of companies and research organizations that aims to develop a standardized reference architecture for data-sharing. Matthias Jarke, Boris Otto and Sudha Ram, 'Data Sovereignty and Data Space Ecosystems' (2019) 61 Bus Inform Syst Eng 549.

60 Johannes Lohmöller and others, On the Need for Strong Sovereignty in Data Ecosystems (2022) Proceedings of the First International Workshop on Data Ecosystems (DEco'22); Christoph Mertens and others, 'A Framework for Big Data Sovereignty: The European Industrial Data Space (EIDS)' in Edward Curry, Simon Scerri and Tuomo Tuikka (eds), *Data Spaces* (Springer Cham, Cham, Switzerland 2022); Vítor Pedreira, Daniel Barros and Pedro Pinto, 'A Review of Attacks, Vulnerabilities, and Defenses in Industry 4.0 with New Challenges on Data Sovereignty Ahead.' (2021) 21 Sensors (MDPI, Basel, Switzerland); Ana I Torre-Bastida and others, 'Technological Perspective of Data Governance in Data Space Ecosystems' in Edward Curry, Simon Scerri and Tuomo Tuikka (eds), *Data Spaces* (Springer Cham, Cham, Switzerland 2022).

61 Edward Curry, Simon Scerri and Tuomo Tuikka (eds). *Data Space* (Springer Cham, Cham, Switzerland 2022); Scerri and others (n 6).

62 Ursula von der Leyen 'Shaping Europe's digital future' (European Commission, 19 February 2020) https://ec.europa.eu/commission/presscorner/detail/es/ac_20_260> accessed on 17 April 2024.

63 Emannuel Macron 'President sets out vision for European sovereignty – Speech by M. Emmanuel Macron, President of the Republic, at the Nexus Institute' (Ambassade de France au Ryaume-Uni, The Hague, 11 April 2023) < https://uk.ambafrance.org/President-sets-out-vision-for-European-sovereignty> accessed on 17 April 2024.

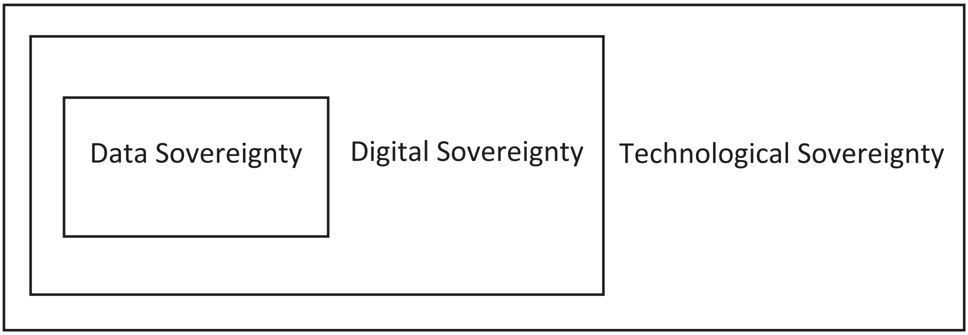

Figure 1: The embeddedness of sovereignty concepts.

Market, proposed several initiatives to bolster European digital sovereignty. Data sovereignty is also promoted as a goal of European data spaces. It is often seen as a subset of technological sovereignty,[64] as described by Hellmeier and von Scherenberg[65] (see Fig. 1).

As shown in Fig. 1, data sovereignty is not separate from the EU's goal of technological sovereignty but is instead a deeply embedded component of this goal. This paper focuses on data sovereignty (as opposed to digital or technological) as it is the type of sovereignty most mentioned in data space projects (such as the IDS and GAIA-X), data space literature, and CEDS.[66]

DEFINING DATA SOVEREIGNTY IN DATA SPACES

Data sovereignty (rather than, for instance, 'digital' or 'cyber' sovereignty) is the preferred term in the context of data spaces and the CEDS.[67] To effectively define data sovereignty in the context of data spaces, this paper examines 64 articles focusing on data sovereignty, specifically within the data space literature (Section Conclusion). The 64 selected articles represent the relatively small number of publications that discuss data spaces and data sovereignty together. The data set of 64 articles is comprised of 33 chapters from the edited collection *Designing Data Spaces: The Ecosystem Approach to Competitive Advantage* by Otto, B., ten Hompel, M., & Wrobel, S.[68]; 16 book chapters from the edited collection *Data Spaces: Design, Deployment and Future Directions* by Curry, E., Scerri, S., & Tuikka, T.[69]; and another 15 articles identified by Scopus searches (with 'data sovereignty' and 'data spaces' as keywords). Several other key texts that have been written in recent years on data sovereignty more generally, both support and contrast with our findings from the data space literature (for example, an article by Hummel et al.[70] was used to contrast definitions of data sovereignty in data space literature with general literature on data sovereignty).

Sovereignty stems from the word sovereign, defined as either a noun or an adjective. The noun sovereign refers to a supreme ruler of a state, typically associated with a monarch with supreme power over their kingdom. The adjective sovereign refers to the possession and exercise of that supreme power. The word sovereign originated from a middle-English word, combining the old

[64] The European Commission only explicitly mentions 'technological sovereignty' (2022) COM 66 final.
[65] Malte Hellmeier and Franziska von Scherenberg, 'A Delimitation of Data Sovereignty from Digital and Technological Sovereignty' (2023) Proceedings of the 31st European Conference on Information Systems.
[66] Duisberg A, 'Legal Aspects of IDS: Data Sovereignty—What Does It Imply?' in Boris Otto, Michael ten Hompel and Stefan Wrobel (eds), *Designing Data Spaces* (Springer Nature, Cham, Switzerland 2022) 61; Nagel and Lycklama (n 11).
[67] See *Hellmeier and van Scherenberger* (n 66).
[68] Boris Otto, Michael ten Hompel and Stefan Wrobel (eds), *Designing Data Spaces: The Ecosystem Approach to Competitive Advantage* (Springer Nature, Cham, Switzerland 2022) v.
[69] Curry, Scerri and Tuikka (n 62).
[70] Hummel and others (n 13).

French word *soverain* (above or supreme) with the English word *reign* (to rule), meaning to rule or reign above supremely. Essentially, sovereignty is 'the sovereign's right to act freely or without interference within a given sphere of action'.[71]

Sovereignty is typically applied in the context of *state* sovereignty,[72] emerging as a concept around the start of the sixteenth century when sovereign monarchs ruled over states and controlled actions therein.[73] In the modern era, the definition veered toward parliamentary sovereignty,[74] whereby sovereignty was increasingly associated with a state's power, rather than a monarch's, to govern itself independently concerning its 'physical territories and domestic affairs'.[75]

The concept of state sovereignty was still affected in the 20th century following several vital events and treaties. For instance, the Hague Conferences of 1899 and 1907 curtailed the right of sovereign states to 'engage in military actions on their own terms'[76]; the League of Nations of the Permanent Court of International Justice was established in 1922 to work as a legal authority that could act to impede the actions of sovereign states[77]. The European Convention on Human Rights[78] and the European Court of Human Rights were established after World War II to unify overarching rights, limiting individual countries' state sovereignty.[79]

Historically, based on the now classic case Costa v E.N.E.L.[80], the EU has been viewed by the Court of Justice of the European Union (CJEU) as an independent legal entity. Such a perspective perceives the EU as a self-sufficient system of norms. This view extends to the EU's legislative, adjudicative, regulatory, and enforcement roles. Although the co-existence of the EU and its Member States' legal orders is complex, it does not diminish the sovereignty of either. It only indicates a demarcation of competence and jurisdiction. In simplified terms, based on EU Treaties, Member States transpose a fraction of their sovereign competencies to the transnational organization bound by the contract (treaties) between the countries forming the organization. Sovereignty, traditionally anchored at the nation-state level, has been well incorporated in Europe, especially considering the powers conferred upon the EU by its Member States. This sovereignty is not compromised by the EU's commitment to human rights, democracy, and the rule of law.

Despite the long history of sovereignty in politics, the combination of *data* and *sovereignty* is relatively new and as a result, it is not always clear what it entails. While sovereignty is the power or authority over a territory, data is information about an individual, group, things, activities, and places. Data can represent personal information, such as a name, date of birth, and nationality. However, data can also refer to more abstract behavioural patterns, such as the likelihood that one will choose a particular brand of juice. It can come from a wide array of domains (agriculture, transportation, and healthcare), activities (stock prices, crime rates, and literacy levels), subjects (individual, group, national, and international), and formats (video, audio, and sensor data). Data can often be repurposed and shared without risking being depleted or losing value.[81] It is highly contextual, about many different people/groups, and can be reused for various purposes.

[71] Pärtel Piirimäe, 'The Westphalian Myth and the Idea of External Sovereignty' in Hent Kalmo and Quentin Skinner (eds), *Sovereignty in Fragments: The Past, Present and Future of a Contested Concept* (Cambridge University Press, Cambridge 2010) 64.

[72] United Nations, 'Charter of the United Nations' (1945) United Nations, San Fransisco 3.

[73] Quentin Skinner, 'The Sovereign State: A Genealogy' in Hent Kalmo and Quentin Skinner (eds), *Sovereignty in Fragments: The Past, Present and Future of a Contested Concept* (Cambridge University Press, Cambridge 2010) 26.

[74] James Tully, *Strange Multiplicity: Constitutionalism in an Age of Diversity* (Cambridge University Press, Cambridge 1995).

[75] Marie Baezner and Patrice Robin, 'Cyber Sovereignty and Data Sovereignty' (2018) CSS Cyberdefense Trend 2 Analyses.

[76] Skinner (n 74) 43.

[77] ibid.

[78] Convention for the Protection of Human Rights and Fundamental Freedoms [1950] (European Convention on Human Rights) (ECHR).

[79] Skinner (n 74) 43.

[80] Case 6/64 *Flaminio Costa v E.N.E.L.* [1964] ECLI:EU:C:1964:66.

[81] Susan Ariel Aaronson, 'Transatlantic Priorities: Data Governance' (2021) 56 Intereconomics 59.

Data sovereignty has emerged to ensure stakeholders are not exploited in the competition for this data.[82] It refers to how an agent can set the parameters around how their data is used.[83] Data sovereignty protects how one's data is used[84] and is a 'basic prerequisite for the cooperation or connection of previously separate value chains and networks'.[85] It is the 'freedom to take independent decisions and the request for fair conditions' for one's data.[86] As shall be explored further in this paper, these definitions are noticeably abstract and do not go into detail about how data sovereignty may be exercised in practice or what legal instruments need to be implemented to protect one's data sovereignty.

Despite this, there are three main characteristics of data sovereignty commonly found within the literature: the values that underpin data sovereignty, the data processes involved, and the data sovereign agent. First, the values that underpin data sovereignty in data spaces need to be explicit.[87] One needs to identify what values are being upheld in data spaces to ensure participants can share data safely and confidently.[88] Therefore, the first question that needs to be asked is: Which value(s) are most important for data sovereignty as they are applied to *data spaces*, such as CEDS?

Second, the types of *data processes* that data sovereignty refers to should be clarified. While traditional definitions of sovereignty refer to absolute power over territorial land, sovereignty has a different meaning when applied to data. The data space literature has varying understandings about what actions must be taken towards data sovereignty in CEDS.

Third, we need to know which *agent(s)* data sovereignty applies to (eg, individuals, organizations, or the state) in European data spaces, as this could lead to drastically different outcomes. For example, if referring to individuals, implementing data sovereignty would focus on privacy, non-discrimination, the right to be forgotten, and laws to protect citizens.[89] Intellectual property rights, business modelling, and governance are likely more relevant for organizations. If related to state data sovereignty, actions must be taken to ensure that multinationals do not harm state security.[90]

The following subsections will examine the three components of data sovereignty described here to understand how it applies to data spaces, particularly the CEDS, and whether current EU policy is sufficient for implementing and protecting data sovereign actors.

Values of data sovereignty and the centrality of control

Hummel et al. identifies several specific values commonly associated with data sovereignty, such as control and power, security and non-maleficence, deliberation, representation and inclusion, privacy, ownership, and transparency.[91] Data sovereignty is an overarching or umbrella concept incorporating several different values. The traditional understanding of state sovereignty is also often classified as a 'cluster concept',[92] which includes related concepts such as autonomy (of citizens), justice (within the state), and security (of the state). Similarly, in the data space literature, data sovereignty is also defined concerning contrasting values (see Table 1).

[82] Hummel and others (n 13).
[83] Heinrich Pettenpohl, Markus Spiekermann and Jan Ruben Both, 'International Data Spaces in a Nutshell' in Boris Otto, Michael ten Hompel and Stefan Wrobel (eds), *Designing Data Spaces: The Ecosystem Approach to Competitive Advantage* (Springer Nature 2022) 29.
[84] Kirstein and Bohlen (n 6).
[85] Michael Ten Hompel and Michael Schmidt, 'Silicon Economy: Logistics as the Natural Data Ecosystem' in Boris Otto, Michael ten Hompel and Stefan Wrobel (eds), *Designing Data Spaces: The Ecosystem Approach to Competitive Advantage* (Springer Nature 2022) 263, 269.
[86] Thomas Usländer and Andreas Teuscher, 'Industrial Data Spaces' in Boris Otto, Michael ten Hompel and Stefan Wrobel (eds), *Designing Data Spaces: The Ecosystem Approach to Competitive Advantage* (Springer Nature 2022) 315.
[87] Otto (n 4).
[88] Jan Jürjens and others, 'Tokenomics: Decentralized Incentivization in the Context of Data Spaces' in Boris Otto, Michael ten Hompel and Stefan Wrobel (eds), *Designing Data Spaces: The Ecosystem Approach to Competitive Advantage* (Springer Nature, Cham, Switzerland 2022) 92.
[89] Robert Herian, 'Blockchain, GDPR, and Fantasies of Data Sovereignty' (2020) 12 Law, Innovation Technol 156.
[90] Kristina Irion, 'Government Cloud Computing and National Data Sovereignty' (2012) 4 Policy Internet 40.
[91] Hummel and others (n 13).
[92] Joe Shaw, *Sovereignty at the Boundaries of the Polity* (ARENA 2002).

Table 1 Values commonly associated with data sovereignty in the data space literature

Values commonly associated with data sovereignty in the data space literature
1. Data ownership[93]
2. Transparency[94]
3. Privacy[95]
4. Control/power/authority[96]

While other values such as fairness,[97] non-discrimination,[98] empowerment,[99] autonomy,[100] and consent[101] are also associated with data ownership, they are only occasionally linked to data sovereignty in data spaces (referenced in passing or the link unclear). Therefore, they have not been included in the analysis of values that typically define data sovereignty in the context of data spaces.

Some values in Table 1—and their relationship to data sovereignty in data spaces—are problematic, particularly data ownership.[102] For example, one of the main reasons for using the data sovereignty concept is to get away from the problematic concept of data ownership.[103] Data ownership and the allotment of specific exclusive rights to data may impede 'the development of the data economy'.[104] It would also require the enforcement of contract law in the data space, which is notoriously difficult.[105] Data sovereignty 'excludes the transfer of ownership rights to any central entities or providers'.[106] Policymakers, practitioners, and academics state that exclusive data ownership rights will not promote economic growth[107] and could hinder data-driven innovation.[108] Furthermore, the concept of data ownership appears strikingly incompatible with the principles of the civil law institutions of property and ownership as established in doctrine. This makes it susceptible to practical inefficiency due to the theoretical intricacies of its assumptions.[109]

[93] Yuri Demchenko and others, 'Defining Platform Research Infrastructure as a Service (PRIaaS) for Future Scientific Data Infrastructure' in Boris Otto, Michael ten Hompel and Stefan Wrobel (eds), *Designing Data Spaces: The Ecosystem Approach to Competitive Advantage* (Springer Nature, Cham, Switzerland 2022); Scerri and others (n 6).

[94] Wieland Holfelder, Andreas Mayer and Thomas Baumgart, 'Sovereign Cloud Technologies for Scalable Data Spaces' in Boris Otto, Michael ten Hompel and Stefan Wrobel (eds), *Designing Data Spaces: The Ecosystem Approach to Competitive Advantage* (Springer Nature, Cham, Switzerland 2022) 419; Nagel and Lycklama (n 11); Vassil Vassilev and others, 'AI-Based Hybrid Data Platforms' in Edward Curry, Simon Scerri and Tuomo Tuikka (eds), *Data Spaces* (Springer Cham, Cham, Switzerland 2022).

[95] ibid; Silvia Gabrielli and others, 'KRAKEN: A Secure, Trusted, Regulatory-Compliant, and Privacy-Preserving Data Sharing Platform' in Edward Curry, Simon Scerri and Tuomo Tuikka (eds), *Data Spaces* (Springer Cham, Cham, Switzerland 2022).

[96] Ulrich Ahle and Juan Jose Hierro, 'FIWARE for Data Spaces' in Boris Otto, Michael ten Hompel and Stefan Wrobel (eds), *Designing Data Spaces: The Ecosystem Approach to Competitive Advantage* (Springer Nature, Cham, Switzerland 2022) 395; Demchenko and others (n 95); Duisberg (n 67); Holfelder, Mayer and Baumgart (n 96); Jarke M and Quix C, 'Federated Data Integration in Data Spaces' in Boris Otto, Michael ten Hompel and Stefan Wrobel (eds), Designing Data Spaces: The Ecosystem Approach to Competitive Advantage (Springer Nature, Cham, Switzerland 2022) 181; Christoph Schlueter Langdon and Karsten Schweichhart, 'Data Spaces: First Applications in Mobility and Industry' in Boris Otto, Michael ten Hompel and Stefan Wrobel (eds), *Designing Data Spaces: The Ecosystem Approach to Competitive Advantage* (Springer Nature, Cham, Switzerland 2022) 493; Douwe Lycklama, 'Data Space Functionality' in Boris Otto, Michael ten Hompel and Stefan Wrobel (eds), *Designing Data Spaces: The Ecosystem Approach to Competitive Advantage* (Springer Nature, Cham, Switzerland 2022); Nagel and Lycklama (n 11); Sebastian Pretzsch, Holger Drees and Lutz Rittershaus, 'Mobility Data Space' in Boris Otto, Michael ten Hompel and Stefan Wrobel (eds), *Designing Data Spaces: The Ecosystem Approach to Competitive Advantage* (Springer Nature, Cham, Switzerland 2022) 343; Fabrice Tocco and Laurent Lafaye, 'Data Platform Solutions' in Boris Otto, Michael ten Hompel and Stefan Wrobel (eds), *Designing Data Spaces: The Ecosystem Approach to Competitive Advantage* (Springer Nature, Cham, Switzerland 2022) 383; Usländer and Teuscher (n 88) 313.

[97] Boris Otto, Michael ten Hompel and Stefan Wrobel (n 69)

[98] Otto (n 4).

[99] Christian Jung and others, 'Data Usage Control' in Boris Otto, Michael ten Hompel and Stefan Wrobel (eds), *Designing Data Spaces: The Ecosystem Approach to Competitive Advantage* (Springer Nature, Cham, Switzerland 2022) 129.

[100] Usländer and Teuscher (n 88).

[101] Lycklama (n 98); Torre-Bastida and others (n 61).

[102] Michael Birnhack and Tal Morse, 'Digital Remains: Property or Privacy?' (2022) 30 Int J Law Inform Technol 280.

[103] Ten Hompel and Schmidt (n 87) 263.

[104] Duisberg (n 67).

[105] ibid.

[106] Ten Hompel and Schmidt (n 87) 273.

[107] Ignacio Cofone, 'Beyond Data Ownership' (2021) 43 Cardozo L Rev 501.

[108] Jianxi Luo, 'Data-Driven Innovation: What Is It?' (2023) 70 IEEE Trans Eng Manage 784.

[109] Anastasios Dosis and Wilfried Sand-Zantman, 'The Ownership of Data' (2023) 39 J Law, Econ, Organiz 615; Cofone (n 109).

Within the data space literature, data sovereignty is often defined as providing other benefits and values, such as privacy and transparency.[110] Sometimes, these values are defined as essential outcomes of, or *additional* values alongside, data sovereignty rather than necessarily core characteristics *of* data sovereignty.[111] In other instances, privacy is mentioned in the same context as data sovereignty as something to be upheld, with little explanation around how these concepts relate or interact.[112] Despite the relatively low levels of incorporating privacy within data sovereignty (in data spaces) definitions, its significance to the data sovereign individuals is paramount (this will be further discussed in Section Individual data sovereignty in CEDS). For now, privacy can be understood as a closely related and relevant concept to data sovereignty but not as a *core* characteristic of the definition of data sovereignty itself.

There was one value that was consistently defined as part of the core meaning of data sovereignty in the data space literature: authority/power/control (terms used interchangeably throughout the literature and meant in the same way; namely, control over what is done with one's data. The remainder of the paper will refer to the control of data). The value of control is fundamental to both traditional definitions of state sovereignty[113] and definitions of data sovereignty outside of the data space literature.[114] All are seen as fundamentally underpinned by power[115]: 'Sovereignty was surely born out of a desire to understand and explain power, but also to claim, legitimize and challenge power'.[116] In the context of data spaces, data sovereignty is used to explain the control over what is done with one's data. Control is fundamentally tied to and underpins definitions of data sovereignty in the data space literature. Once again, in practical and legal terms, it is not yet clear at this stage how this sovereign type of control would be implemented in the context of data spaces, and what it would imply for specific data rights holders.

Definition 1: Data sovereignty in data spaces is control by an agent over a particular process over one's data.

Data sovereignty and control over the processing of one's data

If we understand data sovereignty as a type of control over data, what type of process is subjected to this control? The most common one in the literature is control over who has *access* to one's data. However, some claim that 'access control alone is insufficient, as data sovereignty would end once the flow of data between participants took place after access has been legitimately granted'.[117] While control over access to one's data is undoubtedly an essential component of control, it requires supplementation with other processes concerning one's data, such as control over the *usage* of one's data. The control over one's data could be implemented by granting certain restrictions and usage policies relating to access to one's data: 'Such a policy could be, for instance, the permission to use a dataset for one week, with the obligation to delete it after that time'.[118]The 'right to be forgotten', a policy established and implemented by the GDPR, covers some of this ground of ensuring control over one's data.[119] However, the 'right to be forgotten' concerns only one dimension, namely, the right to have one's private

110 Holfelder, Mayer and Baumgart (n 96).
111 Nagel and Lycklama (n 11).
112 Vassilev and others (n 96).
113 Hent Kalmo and Quentin Skinner, 'Introduction: A Concept in Fragments' in Hent Kalmo and Quentin Skinner (eds), *Sovereignty in Fragments: The Past, Present and Future of a Contested Concept* (Cambridge University Press 2010) 1.
114 Hummel and other (n 13).
115 Denis Baranger, 'The Apparition of Sovereignty' in Hent Kalmo and Quentin Skinner (eds), *Sovereignty in Fragments: The Past, Present and Future of a Contested Concept* (Cambridge University Press, Cambridge 2010) 47.
116 Martti Koskenniemi, '12 Conclusion: Vocabularies of Sovereignty–Powers of a Paradox' in Hent Kalmo and Quentin Skinner (eds), *Sovereignty in Fragments: the Past, Present and Future of a Contested Concept* (Cambridge University Press, Cambridge 2010) 223.
117 Lohmöller and others (n 61) 3.
118 ibid.
119 Aislinn O'Connell, 'The Right to Be Forgotten, by Paul Lambert' (2020) 28 Int J L Inform Technol 88.

Table 2. Data sovereignty in data spaces is a type of control over.

Data sovereignty in data spaces is a t ype of control over:
1. Data access[121]
2. Data usage[122]
3. Data-sharing[123]
4. Data storage[124]

information be removed from Internet searches and directories (permanent restriction against anyone accessing it) in particular circumstances, representing only one component of the control over access to one's data (of data sovereignty). Other components, for instance, could refer to temporary access, permanent restrictions against access toward some (as opposed to all), or access under certain conditions, specific locations, or for certain timespans only.[120] While the 'right to be forgotten' is undoubtedly a necessary policy for ensuring data sovereignty, it is insufficient.

Therefore, while data access and usage control are significant to any definition of data sovereignty, so is control over who and how one's data can be shared and stored. Overall, one may refer to data sovereignty in data spaces as a type of control over one's data concerning how it is accessed, used, shared, and stored, as reflected in the definitions found in the literature on data sovereignty in data spaces (see Table 2).

The first two processes are often translated into rules for access and use in EU legislation. These rules determine how businesses leverage data to generate value. Access rules specify what data can be gathered, including personal information from individuals, and how it can be shared or transferred among entities in horizontal data exchanges. On the other hand, use rules can indirectly impact data flow, as regulations such as consumer protection can increase the cost of data processing, thereby decreasing the profitability of some data extraction endeavours.

These rules can affect different actors in varying ways, influencing their capacity to extract and utilize data. Strict data and consumer protection measures may reduce the market dominance of influential players, promote competition, and create opportunities for rivals, including local ones.[125] Data storage is not as crucial in data spaces because data is 'stored at the source'.[126] Data spaces do not have a central data storage place, and data exchange occurs directly between participants.[127]

[120] Pieter TJ Wolters, 'The Territorial Effect of the Right to Be Forgotten after *Google v CNIL*' (2021) 29 Int J Law Inform Technol 57.

[121] Ahle and Hierro (n 98); Fabian Biegel and Nemrude Verzano, 'From Linear Supply Chains to Open Supply Ecosystems' in Boris Otto, Michael ten Hompel and Stefan Wrobel (eds), *Designing Data Spaces: The Ecosystem Approach to Competitive Advantage* (Springer Nature, Cham, Switzerland 2022) 485; Gouriet M and others, 'The Energy Data Space: The Path to a European Approach for Energy', in Boris Otto, Michael ten Hompel and Stefan Wrobel (eds), *Designing Data Spaces: The Ecosystem Approach to Competitive Advantage* (Springer Nature, Cham, Switzerland 2022); Holfelder, Mayer and Baumgart (n 96); Nagel and Lycklama (n 11); Tocco and Lafaye (n 98); Usländer and Teuscher (n 88).

[122] Ahle and Hierro (n 98); Demchenko and others (n 95); Duisberg (n 67); Holfelder, Mayer and Baumgart (n 96); Jarke and Quix (n 98); Langdon and Schweichhart (n 98); Lycklama (n 98); Nagel and Lycklama (n 11); Pretzsch, Drees and Rittershaus (n 98); Tocco and Lafaye (n 98); Usländer and Teuscher (n 88).

[123] Biegel and Verzano (n 123); Duisberg (n 67); Lycklama (n 98); Otto (n 4).

[124] Biegel and Verzano (n 123); Holfelder, Mayer and Baumgart (n 96); Otto (n 4).

[125] Aaronson (n 83); Inge Graef, Martin Husovec and Nadezhda Purtova, 'Data Portability and Data Control: Lessons for an Emerging Concept in EU Law' (2018) 19 German L J 1359; Crispin Niebel, 'The Impact of the General Data Protection Regulation on Innovation and the Global Political Economy' (2021) 40 Comp L Security Rev 105523, p. 12.

[126] Otto (n 4) 7.

[127] Kirstein and Bohlen (n 6); Scerri and others (n 6).

Data sovereignty in data spaces is a type of control over the access, use, sharing, and storage of one's data. However, whose data we are talking about is still unclear. For example, Hummel et al.[128] found that data sovereignty has been applied to protect the data of countries, indigenous populations, users/consumers, citizens, societies, patients, and organizations (private, governmental, and non-governmental). However, which agents are relevant to data sovereignty in European data spaces is sometimes unclear.

Definition 2: Data sovereignty in data spaces is controlled by an agent over access, use, storage, and sharing of one's data.

Data sovereign agents in data spaces

In the past few decades, the term sovereignty has been used in various contexts, including 'bodily sovereignty'[129], 'food sovereignty'[130], and 'data sovereignty'[131]. As well as across a broad spectrum of contexts, it has also been used concerning a range of actors. Hummel and others[132] extensive literature review of different types of data and digital sovereignty identified eleven types of possible sovereign agents: countries, indigenous populations, user/consumer, private-sector organizations, governmental organizations, non-governmental organizations, expert/professional, societies, patients, citizen, and intergovernmental organizations. Data sovereign agents in the data space literature are typically limited to individuals, organizations, and states. The following section will focus on the challenges of applying data sovereignty to these three agents in the context of CEDS. However, for now, we incorporate these three agents into a working definition of data sovereignty in data spaces:

Definition 3: Data sovereignty in data spaces is control by an individual, organization, or state over the access, use, storage, and sharing of their data.

Overall, the three identified core characteristics of data sovereignty in this section are already visible in current and prospective data policies. The first two characteristics of data sovereignty (values and processes) in data spaces differ across Europe's prevailing data and technology policy frameworks. For example, privacy is strongly emphasized in the GDPR. In contrast, most policy documents emphasize control over data and the processes necessitating control over data (access, use, sharing, and storage). These two main characteristics can be seen in Table 3.

Table 3 highlights that while the first two characteristics of data sovereignty can be identified within the law, it is still unclear how different actors in the data-sharing chain are, or can be, sovereign over their data in data spaces. As a result, it may become difficult to protect data sovereignty in data spaces when it is still unclear *which* agents' data sovereignty should be protected in the data space or how to implement sovereignty using the current data policy (as illustrated in Table 3).

The following section focuses on the third characteristic of data sovereignty—the agents claiming sovereignty in the data space. Conceptually, the values and processes of data sovereignty apply to whichever agent has a legitimate claim to control the access and use of specific data. However, this may lead to tensions between individual, organizational, and state control

[128] Hummel and others (n 13).

[129] Philippa Levine, 'Sovereignty and Sexuality: Transnational Perspectives on Colonial Age of Consent Legislation', *Beyond Sovereignty* (Springer, New York 2007); Leigh A Trueblood, 'Female Genital Mutilation: A Discussion of International Human Rights Instruments, Cultural Sovereignty and Dominance Theory' (1999) 28 Denv J Int'l L Pol'y 437; Alex Wilson, 'Our Coming in Stories: Cree Identity, Body Sovereignty and Gender Self-Determination' (2015) 1 J Global Indigeneity 4.

[130] Via Campesina, 'Food Sovereignty' (2003) 9 Foodfirst Backgrouder 4 <https://archive.foodfirst.org/wp-content/uploads/2013/12/BK9_4-Fall-2003-Vol-9-4-Food-Sovereignty.pdf> accessed on 17 April 2024; Raj Patel, 'Food Sovereignty' (2009) 36 J Peasant Stud 663; Michel Pimbert, *Towards Food Sovereignty* (International Institute for Environment and Development London 2009); Hannah Wittman, 'Food Sovereignty: A New Rights Framework for Food and Nature?' (2011) 2 Environ Soc 87.

[131] Hummel and others (n 13).

[132] Ibid.

Table 3. Historical overview of the data governance evolution in the EU and its relation to data sovereignty processes and values.

EU legislation	Adopted	Which elements of data governance does it introduce?	Data processes	Values of data sovereignty
1995 Directive	1995	This Directive consists of rules and individual rights concerning the processing of personal data. It limits data usage, data quality, security requirements, and the protection of special categories of data.	Access, usage, storage	Privacy, transparency, control
General Data Protection Regulation (GDPR)	2016	Personal data protection as a fundamental right; sanctions for rule breaches on privacy, transparency, and access rights; *the right to be forgotten (article 17) gives individual privacy precedence over economic and public* interests in accessing specific data; data protection rights travel with the data.	Access, sharing, usage, storage	Transparency, privacy, authority/ control
Regulation on the free flow of non-personal data	2018	Easing non-personal data flow between EU countries and IT systems; allowing public authorities access to their data even in another EU country; and prohibiting data localization and vendor lock-in.	Access, sharing, storage	Privacy, control
Open Data Directive	2019	This Directive focuses on increased accessibility of public data, reutilization of public sector information, and exceptions for some instances, eg, intellectual property.	Access, usage, sharing	Transparency, authority
Data Governance Act (DGA)	2022	(Neutral) data access; decrease data procurement costs for businesses; formalized portability and interoperability requirements; standardized rules for data exchanges and intermediation services; sectoral data spaces; enabling the EU to make adequate decisions on data flows to third countries.	Access, usage, sharing	Transparency, privacy, control
Digital Services Act (DSA)	2022	This Act focuses on consumer protection, the European Digital Single Market (DSM), and an equal playing field between service providers.	Usage, sharing	Transparency, control
Digital Markets Act (DMA)	2022	This Act focuses on consumer protection, the European DSM, competition between Market Players, and obligations for gatekeepers not to abuse their position.	Access, storage	Transparency, control
Data Act	2023	Standardized rules for data exchanges enhance data access and portability for users (not just technology providers), ease the transfer of nonpersonal data between companies, and make it easy to switch cloud providers.	Access, usage, sharing	Transparency, privacy, control

Table 3. Continued

EU legislation	Adopted	Which elements of data governance does it introduce?	Data processes	Values of data sovereignty
E-Evidence[133]	2023	Allow law enforcement to obtain stored electronic evidence located in another state.	Access	Privacy
AI Act (Proposal)[134]	N/A	Utilizing industrial data to drive AI development.	Access, usage	

over data as these agents might hold overlapping claims to the protected entity–data. To identify whether the current data policy is sufficient to establish institutions capable of implementing and protecting data sovereignty for these agents or if further steps need to be taken, we will take the working definition of data sovereignty based on the findings from Sections Individual data sovereignty in CEDS, Organizational Data Sovereignty in CEDS, and State data sovereignty in CEDS.

CHALLENGES OF DATA SOVEREIGN AGENTS IN CEDS

The previous section outlined a working definition of data sovereignty in the context of data spaces, such as the CEDS. Current definitions of data sovereignty in the data space literature converge on several points and loosely define it as a type of control over how one's data is stored, shared, accessed, and used. A more challenging issue is identifying how different agents can be sovereign in data spaces. We have identified three possible data sovereign agents from the data space literature: the individual, organizations, and the state. This section focuses on these three agents to highlight potential issues for each in the context of EU data spaces and current limitations in EU data policy to protect the data sovereignty of these agents.

3.i. Individual data sovereignty in CEDS

The individual is one possible agent in data spaces.[135] Within the literature on data spaces, data sovereignty has been defined as 'the capability of a legal entity or natural person to determine and execute usage rights when it comes to their data'.[136] However, as there is no legal definition for data sovereignty, it is difficult to identify what is meant by usage rights in this context, and what their practical role might be in implementing data sovereignty. Furthermore, the definition of usage rights overlaps significantly with definitions of legal capacity. Therefore, usage rights are determined (to a certain extent) by the procedural ability to execute such rights. Other definitions classify data sovereignty similarly but emphasize the individual's self-determination towards their data.[137] Therefore, giving 'human users' control, or individual data sovereignty

[133] Regulation (EU) 2023/1543 of the European Parliament and of the Council of 12 July 2023 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings [2023] OJ L191/118.

[134] Commission 'Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonized Rules on Artificial Intelligence (Artificial Intelligence Act (AI Act)) and Amending Certain Union Legislative Acts' COM (2021) 206 final.

[135] Gouriet and others (n 123); Ralf Kalmar and others, 'Agricultural Data Space' in Boris Otto, Michael ten Hompel and Stefan Wrobel (eds), *Designing Data Spaces: The Ecosystem Approach to Competitive Advantage* (Springer Nature, Cham, Switzerland 2022) 279; Christoph Lange, Jörg Langkau and Sebastian Bader, 'The IDS Information Model: A Semantic Vocabulary for Sovereign Data Exchange' in Boris Otto, Michael ten Hompel and Stefan Wrobel (eds), *Designing Data Spaces: The Ecosystem Approach to Competitive Advantage* (Springer Nature, Cham, Switzerland 2022) 111; Nagel and Lycklama (n 11); Otto (n 4).

[136] Otto (n 4) 5.

[137] Jarke, Otto and Ram (n 60); Pettenpohl, Spiekermann and Both (n 85).

(IDS), over their data is prevalent within the data space literature.[138] However, because data sovereignty is primarily discussed in policy documents, it is often referred to in abstract terms. Consequently, the lack of a legal definition poses significant challenges in establishing a formal and practical understanding of what this institution entails on a systemic level and in practical terms.

IDS is the control individuals have over what is done with their data.[139] Most of the objectives in data spaces are focused on ensuring fair data flow between businesses, promoting data-driven growth, and ensuring that businesses follow GDPR and European data legislation.[140] IDS is often associated with two goals: protecting individuals (eg, their privacy and safety)[141] and providing fair compensation when their data is accessed, shared, or used.[142] These goals could be seen as a division between protecting individuals from harm caused by the misuse of their data on the one hand and allowing them to benefit from sharing their data on the other. For example, businesses must abide by the GDPR when processing and transferring data within the data space. Individuals should also benefit from better products and services because of better data-sharing.[143] As a result, there is often a strong emphasis on developing and implementing user-friendly data spaces and abiding by data protection laws.[144]

The overlap between privacy regulation and enhanced control over data (ie, data sovereignty) appears promising. At the same time, harm prevention has already been implemented in various legislation (through anti-discrimination, right to be forgotten, privacy, and data protection laws, as discussed here and in Section Historical context of EU data governance). It is, however, less clear how individuals can *benefit* from sharing their data use (eg, through monetizing their data in the data space). This sometimes results in tension between the twin aims of protecting individuals and allowing them to benefit from sharing their data. Though not explicitly included in CEDS proposals, some scholars are excited that the CEDS potentially 'incentivizes individuals to share their data, introducing C2B business models that allow them to remain in control of their data while directly receiving fair monetary or economic benefits'.[145] However, it is unclear how this incentivization would or should occur, what is considered fair monetary compensation, and how users can protect themselves and their data from exploitation. In the first concrete data space proposal – the Proposal for a European Health Data Space (EHDS)—such monetization schemes for individual data subjects are not included.

Traditionally, large tech companies are granted permission to use individuals' data in exchange for free services, popularly described as the 'freemium' model.[146] The Big Five[147] tech companies have significantly benefitted from this model, but consumers are becoming increasingly wary about giving away their data in this way.[148] As a result, there has been a growing interest in 'Personal Data Spaces', which may grant individuals greater control over what is done with their data. Personal data spaces may also provide the end-user with greater transparency over how their data is used (ie, their data sovereignty) while directly rewarding them for the use of their data.[149] However, personal data is already protected as a fundamental right in the Treaty

138 Lange, Langkau and Bader (n 137).
139 Judy Bowen and Annika Hinze, 'Participatory Data Design: Managing Data Sovereignty in IoT Solutions' (2022) Interacting Comput iwac031.
140 Scerri and others (n 6).
141 Gabrielli and others (n 97).
142 Curry, Scerri and Tuikka (n 62).
143 Scerri and others (n 6).
144 Edward Curry and others, 'Data Sharing Spaces: The BDVA Perspective', *Designing Data Spaces* (Springer, Cham 2022).
145 Scerri and others (n 6) 350.
146 Curry, Scerri and Tuikka (n 62).
147 Microsoft, Meta, Google, Amazon, and Apple.
148 Curry, Scerri and Tuikka (n 62).
149 ibid.

on the Functioning of the European Union[150] (TFEU) arts 2 and 16, in the CFREU arts 7 and 8, as well as by the privacy framework of GDPR, which grants multiple privacy-related rights and stipulates the further processing of personal data.

There are several issues with the Personal Data Space model. For example, the quantity and quality of available data remains relatively limited and focuses mainly on social media content.[151] There are also several ethical challenges, such as ensuring that individuals (and their data) are not misused, abused, and exploited in the process of sharing data in the personal data space. If there is a split between industrial and personal data spaces[152], this may create challenges around data portability and interoperability between the two types of data spaces, thus making many of the potential benefits of data spaces more challenging to realize.[153] Some commentators point out that this monetization of personal data may allow for increased exploitation by large tech companies, not less, where data monetization and personal data spaces are created by data-driven businesses to gain greater control over individuals' data.[154] They are maintained by data subjects trying to exert greater control over their data under the assumption that it is already being used by these companies free of charge.[155]

Additionally, because the CEDS will be fundamentally grounded in the GDPR, it is debatable how much further the data sovereignty concept will bring individuals greater control over their data. To reiterate the main requirements of the GDPR, it 'requires companies dealing with European consumers to (1) *increase transparency*, (2) *provide users with granular control for data access and sharing*, and (3) guarantee consumers a set of fundamental individual digital rights (including *the right to rectification, erasure, and data portability and to restrict processing*) [our emphasis added]'.[156]

The CEDS makes limited reference to personal data spaces, how individuals may monetize their data, or if it intends to incorporate data monetization for the individual in practice. Much of its emphasis is still on *protecting* the end-user rather than how they can *benefit* from their data. In the EU, personal data is treated as *res extra commercium* and is thus excluded from the free market.[157] Individuals will benefit from better access to cross-sectoral services, more effective developments in European industries, and professional opportunities in a thriving European landscape rather than necessarily a direct economic benefit from data use.[158] While the European Strategy for Data explicitly mentions personal data spaces, it does not detail how they should be implemented or what form they should take. Instead, it states they will be further discussed in the Data Act.[159] It appears that the focus of the Data Act is on *industrial data spaces,* which appear to be the focus of the CEDS as well.

With all these issues in mind, it is not easy to see how IDS can be applied in the context of CEDS. Much of the requirements of IDS are already well-established within the GDPR, raising the risks of duplicating normative assumptions. The push toward personal data spaces and data monetization is practically complex, ethically questionable, and of dubious economic value for those whose data are being shared. Rather than the abstract and impractical notion of IDS, individuals may be sufficiently protected under current privacy protection laws and practices.

[150] Consolidated version of the Treaty on the Functioning of the European Union (TFEU) [2007] OJ C202/1.
[151] Curry, Scerri and Tuikka (n 62).
[152] Amin Anjomshoaa and others, 'Data Platforms for Data Spaces' in Edward Curry, Simon Scerri and Tuomo Tuikka (eds), *Data Spaces* (Springer Cham, Cham, Switzerland 2022).
[153] Curry, Scerri and Tuikka (n 62).
[154] Herian (n 91).
[155] ibid.
[156] Curry and others (n 146) 7.
[157] Václav Janeček and Gianclaudio Malgieri, 'Commerce in data and the dynamically limited alienability rule' (2020) 21:5 *German L J* 924-943.
[158] Scerri and others (n 6).
[159] Reg (EU) 2023/2854—the Data Act—does indeed apply to personal data sets, as well. A separate legal research would be necessary to elaborate on the co-application of Reg (EU) 2016/679and Reg (EU) 2023/2854.

However, the potential practical limitations of an ambitious legislation like the GDPR for current privacy protection must be considered. The fifth anniversary of the GDPR has sparked a wave of critical reflection, with most commentaries praising its ambition and the trend toward individual control over their data while also pointing out significant enforcement challenges via the Data Protection Agencies (DPA).[160] For example, DPAs are have been found to 'generally fail to give data subjects a clear picture of what to expect from the submission of a complaint'.[161] People who have filed complaints against companies infringing upon their rights have had to wait months or even years to be remedied for the violation, mainly if the case concerned cross-border data flows. Hence, despite the focus on equipping individuals with legal tools to protect their data, procedural pitfalls have rendered the provisions of substantiative GDPR, to a large degree, moot.

Technological tools could significantly ease compliance challenges for both the GDPR and IDS. Unfortunately, research findings suggest that technical challenges pervade data space implementation, particularly in access and usage control.[162] While many methods can already be used to control who can gain access to data, one of the outstanding challenges lies in technical control over enforcing data usage policy on the data-consuming side.[163] In simpler terms, an individual might be able to select trusted parties to share their data with, but they do not have the appropriate tools to guarantee how these trusted parties use the data. Experts predict it will be several years before the first solutions to this problem become available.[164]

Though personal data spaces have not been given explicit policy attention, the proposed European Health Data Space (EHDS) deals with sharing and re-using personal health data. While IDS appears to be covered rather comprehensively by the GDPR in the case of personal health data, the EHDS proposal further highlights the potential procedural limits of IDS ambitions. The EHDS proposal defines rules for the primary use of electronic health data (EHD) to improve the care delivery to a single patient across healthcare providers[165] and the secondary use of EHD to make this data available for research, innovation, and better policymaking.

Individual data subjects can make their electronic health records available for secondary use by opting in or out of such a data-sharing agreement. However, the EHDS proposal does not yet foresee fine-grained control by individuals who can access their data once it is included in the EHDS database. Individuals provide blanket consent for secondary use purposes. Researchers and policymakers can request access to this data by applying through a Health Data Access Body (HDAB) that manages a databank on available data sets with the authority to grant or deny access (a closer analysis of the governance mechanisms is provided in the next section).

Concerning IDS, another aspect of the EHDS proposal stands out. Article 38 makes explicit that the exception from GDPR Article 14 applies so that HDABs shall not be obliged 'to provide the specific information under Article 14 of Regulation (EU) 2016/679 to each natural person concerning the use of their data for projects subject to a data permit'. Article 14 of GDPR grants

160 Gloria G Fuster and others, 'The right to lodge a data protection complaint: OK, but then what?–An Empirical Study of Current Practices under the GDPR' (Access Now, July 2022) <https://www.accessnow.org/wp-content/uploads/2022/07/GDPR-Complaint-study.pdf> accessed 13 October 2023; Estelle Massé and others, 'Five Years Under the EU GDPR–Becoming an Enforcement Success' (Access Now, May 2023) <https://www.accessnow.org/wp-content/uploads/2023/05/GDPR-5-Year-report-2023.pdf> accessed 13 October 2023.

161 Fuster and others (n 162) 4.

162 Malte Hellmeier and others, 'Implementing Data Sovereignty: Requirements & Challenges from Practice' (2023) Proceedings of the 18th International Conference on Availability, Reliability and Security.

163 ibid.

164 ibid. 9.

165 While the details of the electronic health records and data sharing platform myhealth@EU that facilitate primary use of EHD, that is, making electronic health records available to other health care providers of the same patient, are still uncertain, data subjects shall have the ability to limit the visibility of parts of their medical records, depending on the care provider. For example, one might grant their psychiatrist access to their mental health records, but not their dentist. While there is agreement between Parliament and Commission that patients should be empowered to limit visibility of some of their medical history, a question remains whether the healthcare professionals should be able to see that the patient has made a restriction on access.

the data subject the right to be provided with information where personal data has not been obtained from the data subject, that is, transparency. Article 14(5) specifies an exception in case of disproportionate effort, which applies to the secondary use of health data in the EHDS. Instead, the EHDS proposal includes transparency provisions so that the HDAB shall provide public information on all the data permits issued and make the results of research projects accessible online. These obligations are less comprehensive than those under the GDPR. Aligning the EHDS proposal with the GDPR remains an ongoing challenge for the EHDS regulation.

Overall, legislators are still committed to the EHDS to retain privacy and data protection for the individual data subject, making their data available for secondary use. However, the ambitions of the proposed EHDS regulation also illustrate the practical limits of the GDPR and IDS. IDS in data sharing for primary use of data can be supported more quickly than for large, aggregated data sets. For primary use of their health data, individuals share medical records with their health professionals, with whom they have a personal relationship. Meanwhile, for secondary use purposes, health data is aggregated and shared with a large group of stakeholders. The EHDS proposal also lacks any mention of monetization of the health data made available by individuals, indicating a lack of interest in moving beyond the privacy focus of IDS in the specific case of personal health data.

Organisational data sovereignty in CEDS

The potential benefit of the data economy in the EU exceeds 550 billion euros, and the value of this data must be distributed among businesses rather than centred in the hands of a small, powerful elite.[166] The CEDS aims to facilitate more significant opportunities for SMEs and start-ups to benefit from data sharing rather than only the large techcompanies.[167] Data spaces aim to provide a 'level playing field for data sharing and exchange, leading to less dominance of, and dependency on, large, quasi-monopolistic players'.[168] While a great aspiration, it is still unclear how providing data spaces to existing data intermediaries without forcing agents with dominant market shares to open their data bases or become part of the data space would work in practice.

Organizational data sovereignty (ODS) promises the fair distribution of benefits and control over one's data resources while emphasizing data creation value[169] and increased economic efficiency for data-driven businesses.[170] ODS states that organizations should have 'self-determination' and control over how their data is accessed, used, shared, and stored.[171] The organization can define usage restrictions over their data before they share it with others.[172] Data sovereignty is essential for developing data-driven businesses within and across different organizations.[173] Much of the data space literature assumes that if data sovereignty is formally foreseen, this may increase trust in the data space, increasing the use of data spaces and the proposed resultant benefits of data-sharing.[174] Ensuring ODS in European data spaces is thus thought to lead to organizations placing a greater level of trust in the process and the data space

166 Otto (n 4).
167 ibid.
168 Nagel and Lycklama (n 11) 18.
169 ibid
170 Volker Berkhout and others, 'Energy Data Space' in Boris Otto, Michael ten Hompel and Stefan Wrobel (eds), *Designing Data Spaces: The Ecosystem Approach to Competitive Advantage* (Springer Nature, Cham, Switzerland 2022).
171 Pettenpohl, Spiekermann and Both (n 85).
172 ibid.
173 Jung and others (n 101); Ten Hompel and Schmidt (n 87).
174 Anjomshoaa and others (n 154); Curry, Scerri and Tuikka (n 62); Curry and Tuikka (n 9); Gouriet and others (n 123); Dirk Hecker, Angelika Voss and Stefan Wrobel, 'Data Ecosystems: A New Dimension of Value Creation Using AI and Machine Learning' in Boris Otto, Michael ten Hompel and Stefan Wrobel (eds), *Designing Data Spaces: The Ecosystem Approach to Competitive Advantage* (Springer Nature, Cham, Switzerland 2022) 211; Ten Hompel and Schmidt (n 87); Vassilev and others (n 96).

itself, encouraging them to make use of the data space and thus creating more significant levels of use and data-sharing, benefiting them, other organizations, and the market as a whole.[175]

The European Data Strategy attempts to establish a European data economy that encourages the flow of public and private data sets in a context where businesses are not yet enthusiastic about data sharing.[176] In the official communication of the Commission, the key obstacles to B2B data sharing are a lack of economic incentives and trust between competitors.[177] Overcoming a lack of economic incentive is a significant obstacle: For the first-mover among the data holders, there is little economic incentive to make their datasets available to competitors if they cannot access their data in return. Lack of trust may play a secondary role: If competitors lack trust in the CEDS, organizations will be sceptical about their proposed sovereignty in the data space, creating even more hesitation to share data with competitors.

While ensuring ODS in CEDS is a desirable goal (if organizations have control over their data, they will trust the process and be more likely to share data), it is undermined by the current restrictive and unclear data-sharing policy. For example, researchers have repeatedly found that data altruism and B2G data sharing are exceptionally challenging to motivate.[178] While the European Data Strategy states that 'The general principle shall be to facilitate voluntary data sharing,' the Commission acknowledges that 'specific circumstances' may require making access compulsory to address market failures and overcome initial obstacles, such as the 'first-mover' disadvantage in data sharing among competitors.[179]

The vagueness regarding involuntary data-sharing is also a component of the Data Act. Concerning ODS, Chapter V Article 14 of the Data Act defines an 'obligation to make data available based on exceptional need'. This definition states that 'upon request, a data holder shall make data available to a public sector body or to a Union institution, agency or body demonstrating an exceptional need to use the data requested'. In this light, Article 15 provides a qualification of 'exceptional need', which applies in case of public emergency of prevention of a public emergency, or when the 'lack of available data prevents the public sector body or Union institution, agency or body from fulfilling a specific task in the public interest that has been explicitly provided by law'. Practical possibilities of applying those definitions in the contexts of ODS and the whole EU's digital acquis remain to be seen. However, the tenor concerning ODS suggests that ODS does not take priority over public interest as a goal for EU policymakers.

Since a comprehensive proposal for the CEDS is still missing, a closer analysis of the sectoral proposal for the EHDS can provide circumstantial insights into the EU's approach to ODS and whether ODS is a goal of EU policymaking in CEDS. In examining the proposal regarding ODS, it is helpful to understand the governance of the EHDS in the light of the Data Governance Act (DGA), given that the EHDS is the first sectoral application of the DGA.

Where the DGA defines data intermediaries, the EHDS establishes Health Data Access Bodies (HDABs) in all Member States. The HDABs are at the centre of the EHDS's governance structure. They are public agencies that, like (possibly private) data intermediation service

[175] Ahle and Hierro (n 98); Anjomshoaa and others (n 154); Demchenko and others (n 95); Gabrielli and others (n 97); Monika Huber and others, 'Building Trust in Data Spaces' in Boris Otto, Michael ten Hompel and Stefan Wrobel (eds), *Designing Data Spaces: The Ecosystem Approach to Competitive Advantage* (Springer Nature, Cham, Switzerland 2022) 147; Jung and others (n 101); Nagel and Lycklama (n 11); Otto (n 4); Otto, ten Hompel and Wrobel (n 69); Pettenpohl, Spiekermann and Both (n 85); Pretzsch, Drees and Rittershaus (n 98); Magnus Redeker and others, 'A Digital Twin Platform for Industrie 4.0', *Data Spaces* (Springer Cham, Cham, Switzerland 2022); Vassilev and others (n 96).

[176] Marcin Zieliński, 'Business-to-Business Data Sharing within the EU Digital Market (2019–2021): Categorization of Data and Actors Involved in Data Sharing Operations' (2023) *Business-to-Business Data Sharing within the EU Digital Market (2019-2021): Categorization of Data and Actors Involved in Data Sharing Operations: Zieliński, Marcin* [Sl]: SSRN.

[177] COM (2020) 66 final 7.

[178] Jukka Ruohonen and Sini Mickelsson, 'Reflections on the Data Governance Act' (2023) 2.1 Digital Society 10; Mahsa Shabani, 'The Data Governance Act and the EU's Move Towards Facilitating Data Sharing' (2021) 17.3 Mol Syst Biol e10229.

[179] COM (2020) 66 final.

providers under the DGA, are non-profit. EHDS governance is to be supported by the EHDS Board (to be chaired by the Commission) and a core platform to facilitate cross-border sharing of EHD, namely HealthData@EU.

The electronic health data holders in the EU, which range from public to private organizations, must notify the respective HDAB about their relevant data sets. This data intermediary then publishes the data sets in a public online register. Potential data users can access this information by applying for access to these data sets with the HDAB. The final decision-making authority (according to the various provisions and protections defined in the regulation) lies with the data intermediary, not the data holder. The HDAB under the EHDS also has the power to administer penalty fees for data holders reluctant to comply with the regulation at any of these steps. However, at the time of writing it is unclear whether such strictly controlled access to data can be enforced and how compliance with dataset notifications can be monitored. There may be procedural limitations and risks in enforcing the EHDS.

All of this indicates that, at least in the specific case of the EHDS, strict ODS does not appear to be the singular policy goal. It appears desirable as it enables the data economy, but not when it might conflict with state interest, like in the case of public health emergencies. It is reasonable to assume that focusing on public health as a public good is a priority and unique to the EHDS. The other sectoral data spaces of the CEDS may leave more room for organizations to exercise control over their data sharing, but this remains to be seen as the EHDS is still the first of its kind.

State data sovereignty in CEDS

State sovereignty is commonly understood as the authority of a state to govern itself through its institutions, including by expressing political intent through law. Unless otherwise specified, the law is understood as authoritative statements containing rules of conduct, backed by coercive force, exercised at the national level by a legitimately constituted (democratic) nation-state. It is further constituted in the supranational context by binding commitments voluntarily entered into between sovereign states (typified by public international law). Many states rely on data to provide suitable amenities and services to improve the welfare of citizens.[180] Thus, having sovereign power over domestic affairs data is a core interest of states. Furthermore, protecting state and citizen information is one of the fundamental criteria for ensuring the self-rule and freedom of that state and its citizens.[181]

State data sovereignty (SDS) implies sovereign power within state jurisdiction to govern how data on domestic affairs is shared, stored, and used.[182] It means self-governing data at the state level without forceful external interference. Such interference could compromise cybersecurity and national security, which could, in turn, lead to extreme political destabilization. Thus, a lack of control over state-relevant data may reduce state self-determination and undermine internal cohesion.

While states may rely on data sovereignty to exercise state sovereignty, states are also reliant on data sovereignty to ensure state sovereignty.[183] A lack of state sovereignty may lead to a greater risk of digital criminality and threats due to a lack of repercussions or turmoil within the state. In other words, where there is dysfunctional state sovereignty, there may be a concurrent increase in digital crime, online fraud, and data breaches.[184]

180 Irion (n 92).
181 Andrew D Mitchell and Theodore Samlidis, 'Cloud Services and Government Digital Sovereignty in Australia and Beyond' (2021) 29 Int J Law Inform Technol 364.
182 Baezner and Robin (n 76).
183 ibid.
184 Stephen D Krasner, 'The Durability of Organized Hypocrisy' in Hent Kalmo and Quentin Skinner (eds), *Sovereignty in Fragments: The Past, Present and Future of a Contested Concept* (Cambridge University Press, Cambridge 2010) 96.

Within the context of the CEDS, one particularity of SDS requires clarification–the sovereignty of states in the EU. Traditionally, one of the main characteristics of sovereignty has been its centralization of executive power. However, an aspect of the emergence of the EU 'has been the increasing sense of the "fragmentation" of traditional social wholes in a way that has made it impossible to identify any single point of power as the holder of "sovereignty"'.[185] How could SDS be realized in a fragmented situation like the EU's CEDS?

To begin with, a state's participation in the EU is not necessarily a 'giving away' of sovereignty, but rather, a delegation of power to the EU, as these powers can 'always be recovered by a renegotiation, by a denunciation of the treaties, or by a new constitutional amendment'.[186] Each Member State amended its constitution to allow them to join the EU. The Member States did so voluntarily, often based on a democratic mandate such as a referendum. Member States can leave the organization if they choose to, as evidenced by the UK's recent withdrawal. Such formal action would revoke the powers and sovereignty delegated to the EU and its institutions: 'On this footing, it can be claimed that there is here no loss of sovereignty, but simply a process of conferral of power by way of delegation under the constitution of each state'.[187]

In the data context, the EU regulates data based on the conferred competencies in the Treaty on the Functioning of the European Union (TFEU) Art 26 and 114, which state the mandate for internal market regulation, a predominant competence of the EU. In the context of data spaces, if Member States are giving away some competencies to the EU to manage and control the CEDS (and the data shared within it), then it is expected that the EU will implement these delegated competencies that affect SDS. However, it is unclear if, or how, the European Commission or a different EU institution will function as a centralized authority over the CEDS.

Again, we can turn to the EHDS as a potential case of how the CEDS might shape SDS. The legal basis for the EU's competence on the EHDS has become possible with recent shifts in health policy. The current proposal of the EHDS foresees a delegation of power based on Article 3(6) TFEU, which establishes that the EU may act within the competencies conferred on it in the Treaties to achieve goals and enforce its principles. However, there have not been specific norms in Article 4(1) that provide an explicit legal basis to confer competence on the matter of health data to the EU because health-related matters have traditionally been limited to the Member States, as the EU was understood to act according to the power-conferring norms of the treaties.[188] Most recently, due to the COVID-19 pandemic-related perturbations, the understanding of competence norms and sovereignty related to public health policy shifted partially towards the EU, giving it a more prominent role.[189]

The legal bases for the EU to take a lead on the EHDS initiative and thereby intervene in Member States' digital policy are Article 16 and Article 114 of the TFEU. The former article regards the protection of personal data, and the latter allows the EU to regulate those elements of private law that create obstacles to trade in the internal market. The EHDS thus utilizes internal market and privacy competence-conferring norms to justify the intervention into the data governance of Member States on their domestic affairs related to health. Overall, then, the delegation of a certain level of SDS to the EU is based on the TFEU.

While the EU is competent to regulate the EHDS, Member States maintain the power to make specific data permit decisions via the national HDAB's public bodies. As the administrative

[185] Koskenniemi (n 118).
[186] Michel Troper, 'The Survival of Sovereignty' in Hent Kalmo and Quentin Skinner (eds), *Sovereignty in Fragments: The Past, Present and Future of a Contested Concept* (Cambridge University Press, Cambridge 2010) 143.
[187] Neil MacCormick, 'Sovereignty and After' in Hent Kalmo and Quentin Skinner (eds), *Sovereignty in Fragments: The Past, Present and Future of a Contested Concept* (Cambridge University Press, Cambridge 2010) 165.
[188] Kai P Purnhagen and others, 'More Competences than You Knew? The Web of Health Competence for European Union Action in Response to the COVID-19 Outbreak' (2020) 11 Eur J Risk Regulat 297.
[189] Mary Guy, 'Towards a European Health Union: What Role for Member States?' (2020) 11 Eur J Risk Regulat 757.

body, the HDAB decides on data permit applications and facilitates data sharing, which is a core aspect of SDS. According to the national governance structure, Member States can establish multiple HDABs but must determine one national contact point. However, they are mandated to collaborate at the EU level through the EHDS Board.

The Member States are still sovereign as they make the administrative decisions on specific data permit applications. These decisions *de facto* determine the impact of the EHDS. The EU, though, retains the competence to regulate the EHDS and oversee its implementation. This complex relationship will be discussed in more detail below. It must be made clear that the EHDS may be an exceptional case of this relationship. The level of oversight from the EU is based on established precedents for implementing adequate health procedures during COVID-19, which justify intervention in the event of another pandemic. The level and type of SDS in the other domain-specific European data spaces are still unclear as they are in the very early stages of development. However, an analysis of SDS in EHDS may offer insights into how it may materialize in other data spaces.

The crux for SDS in the context of the EHDS may lie in accessing cross-border sources of electronic health data for secondary use (such as registries and databases) as defined in Article 53 of the proposed regulation. Firstly, when there is only one official data holder[190] of a cross-border registry registered in a specific Member State, the competent HDAB is the body of that same Member State. However, suppose this cross-border registry has joint controllers[191] registered in different locations within the EU; this leads to a second situation where the HDAB can be any of the countries where one of the joint controllers is established. A third situation occurs if registries of several Member States are organized in a single network at the Union level, where this network may designate one coordinator, whose location also determines the competent HDAB.

All three situations can impact the SDS of one Member State compared to another because Article 54 (2) of the EHDS proposal suggests that 'a data permit issued by one concerned health data access body may benefit from mutual recognition by the other concerned health data access bodies.' This formulation suggests that decisions on data access applications should be recognized across Member States. In theory, this could mean that the HDAB of one Member State decides on data access to the data held by another Member State. The administrative body of one Member State can thus impact the rights holders in another Member State by allowing for comparative interpretation. It matters where the administrative body is, not the data subject, which implies that only the location of the controller of the registry is essential for determining the competent HDAB. The EHDS proposal does not mention the nationality of the data subject whose data is aggregated in such cross-border registries.

Uncertainty around the impacts of EHDS on SDS is amplified by the reality that the policy decision will lose some of its initial power in the reality of administratively issued permits by the technocratic corpus of health data national administration. Member States can maintain considerable power through the administrative bodies of the HDABs, where decisions on data access are made. Member States that wish to ensure SDS should utilize legal rules and norms towards that end since political orders lose power in favour of legal norms and rules, as court rulings ultimately define the interpretation of the law. Based on the competence norms defined earlier, Member States have considerable power in the context of the EHDS over the data registered with their HDBAs. Essentially, they get to decide who, on what conditions, and for how

[190] In COM (2022) 197 final art 2(2), 'data holder' is defined as 'any natural or legal person … who has the right or obligation, in accordance with this Regulation, . . . , through control of the technical design of a product and related services, the ability to make available, including to register, provide, restrict access or exchange certain data'.

[191] 'Controller' is defined in Reg (EU) 2016/679 art. 4(7) as 'the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data'. Joint Controllership is defined in Reg (EU) 2016/679 art 26(1) as follows: 'Where two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers'.

long someone gets access to health data.[192] As explained above, such decisions can impact data subjects in other Member States and data-holding organizations.

Although the decision to issue data permits under the EHDS proposal is not entirely discretionary (as it is subject to specific predefined purpose-based conditions and criteria under Article 46), it still provides the states with an advantageous position, allowing for full access restriction. Since it is an administrative interaction between an HDAB and the applicant, the balance between the parties involved is far from equal, as the state-appointed HDAB authority holds most of the power. Despite existing provisions in place to preserve the rights and obligations of the non-state parties, predominantly in the form of administrative judiciary, the protection in practice is time and resource-intensive (as the implementation of the GDPR showed), thus favouring states' power over the data sovereignty of individuals or organizations.

CONCLUSION

This paper has evaluated the concept of data sovereignty and how it has been applied to the CEDS providing extensive observations of both *de lege lata* and *de lege ferenda*. The ambition behind this analysis was to bridge the theoretical reflections on how technology challenges legal and regulatory approaches with the dogmatic analysis of how political ideals can be translated into practical legislative frameworks. To achieve satisfactory results, we utilized an interdisciplinary approach that combined methods from law, regulation, as well as ethics, and economics

We began by analysing how the CEDS has emerged as a legislative objective in the EU by looking at the historical development of European data regulation. Our assessment showed that the historical account of data privacy in the EU's policy and legislation aimed at contributing to the smooth functioning of the internal market, protecting individuals' fundamental rights, harmonizing data protection rules across the block, facilitating external data transfers, boost EU activity in the data economy, and positioning EU as a leader in data protection. The emergence of the Common European Data Space (CEDS) as a legislative objective in the European Union can be traced back to the foundational steps taken in data protection. Starting with the EU's early recognition of the importance of data protection by ratifying in 1981 the Convention 108[193] of the Council of Europe on Data Protection, we have seen the groundwork being laid for the CEDS. This document clearly articulated goals related to individual rights, the internal market, and economic gains associated with data protection.

The evolution of these goals continued with the drafting of the Data Protection Directive (DPD) in 1990, which added emphasis on harmonization and facilitating external data transfers—key components for ensuring the free flow of data across borders while maintaining competitive equality. The DPD aimed to address the diverse national approaches that had become an obstacle to the completion of the internal market.

With the legal consolidation brought about by the Treaty of Lisbon in 2007, which made the Charter of Fundamental Rights legally binding, and the introduction of the General Data Protection Regulation (GDPR) in 2016, the EU significantly reinforced its commitment to data protection. These steps prioritized fundamental rights over other considerations and set the stage for a more uniform approach to data protection across EU Member States.

Furthermore, the GDPR and subsequent communications from the EU Commission have consistently highlighted the importance of international data transfers and the need for a

192 (2022) 197 COM final, arts 44–6.
193 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data [1981] ETS No. 108.

harmonized approach to data protection rules. These efforts not only seek to protect individual rights within the EU but also aim to position the EU as a global leader in data protection standards, promoting an international convergence of these standards.

In summary, the emergence of CEDS as a legislative objective in the EU reflects a long-standing and evolving commitment to establish a comprehensive, coherent, and harmonized data protection framework. This framework is designed to safeguard individual rights, facilitate economic activities, and enhance the EU's role in global data governance.

The paper focused on accurately identifying what data sovereignty means in the context of data spaces. It identified three key characteristics of data sovereignty definitions: the agents involved, the type of value that underpins it, and the processes required to realize it. First, it's critical to clearly define the values that underpin data sovereignty in data spaces such as CEDS. This clarity allows participants to share data safely and confidently, making it essential to determine which values are paramount in these settings. Second, while traditional concepts of sovereignty relate to absolute control over territory, data sovereignty translates differently, involving specific processes that need to be clarified. Analysis reveals varied interpretations about the necessary actions for establishing data sovereignty in data spaces, indicating a need to reach a unified understanding. The definition found to be most applicable in the context of data spaces is a type of control by an individual, organization, or state concerning the access, use, storage, and sharing of their data. Third, the agents to which data sovereignty applies—individual, organization, or state—greatly influence the outcomes. For individuals, this could focus on privacy and rights like non-discrimination and the right to be forgotten. For organizations, it involves aspects like intellectual property rights and business modelling. In the case of state data sovereignty, measures must be taken to protect national security against threats from multinational corporations.

The central contribution of the paper lies in bringing together the legislative context and investigating how it facilitates or does not facilitate the implementation of data sovereignty for individuals, organizations, and states. In moving beyond official policy communications and narratives, we find that existing legislation does not necessarily facilitate data sovereignty in the sense defined in the academic literature. Indeed, the legislative framework lacks any explicit definition of data sovereignty. The paper thus investigates the added value of data sovereignty as applied to three agents (individuals, organizations, and states).

We suggest that GDPR sufficiently covers IDS, because it goes beyond privacy protection, but needs to overcome procedural barriers. While privacy is essential for data spaces, it is sometimes unclear why it is defined as part of data sovereignty.[194] One solution may be to distinguish privacy and sovereignty as separate aspects of enhancing the protection of individuals' data.[195] Providing adequate privacy gives users greater power over what they can and cannot do with their data (ie, their data sovereignty). Likewise, giving individuals greater control (ie, their data sovereignty) over what is done with their data affords them better opportunities to protect their privacy.

This paper further draws on the insights from a case study. The EHDS is a significant legislative development aimed at enhancing the sharing and reuse of personal health data within the EU. This initiative primarily addresses the handling of electronic health data for both primary and secondary uses. For primary use, the EHDS facilitates the improvement of care delivery by allowing seamless access to a patient's health records across different healthcare providers. In terms of secondary use, it enables health data to be used for research, innovation, and policy-making, where individuals can opt in or out of making their data available.

194 Hummel and others (n 13); Irion (n 92); Redeker and others (n 177).

195 Scerri and others (n 6).

In the context of IDS, the EHDS proposal somewhat extends the protections offered by GDPR, yet it also highlights the procedural limitations of IDS ambitions. Notably, while IDS is well-covered by GDPR regarding personal health data, the EHDS lacks provisions for fine-grained control by individuals over who can access their data once it is integrated into the EHDS database. This involves a blanket consent mechanism for secondary use, managed through a Health Data Access Body (HDAB). The HDAB oversees data access requests but is not required to provide detailed GDPR Article 14 transparency to data subjects about the use of their data for approved projects. Instead, the EHDS proposal focusses on public transparency about data permits and research results.

In summary, the EHDS is designed to balance privacy and data protection with the broader industry-specific goals of enhancing health care and supporting health-related research and policy development. However, it also reveals the practical challenges of aligning comprehensive data protection standards like those in the GDPR with the operational realities of managing large, complex data systems like the EHDS. The realization of IDS within the EHDS framework shows a commitment to data protection but also underscores the need for ongoing adjustments to better reconcile data protection norms with the practicalities of large-scale data use.

Concerning ODS, the critical challenge of encouraging organizations to share their data could hamper establishing data spaces that enable B2B data flows. ODS in the context of the European Data Strategy, particularly within the proposed CEDS, aims to ensure fair control and benefit distribution from data resources among businesses. The goal is to prevent the concentration of data control in the hands of a few large entities, thereby facilitating greater involvement of and benefit for SMEs and startups through a more equitable data-sharing framework.

The realization of ODS in European data spaces like CEDS is predicated on giving organizations control over how their data is accessed, used, shared, and stored, which is intended to foster trust and encourage wider participation in data sharing. This is seen as essential for the development of a thriving data-driven economy. However, the ambition for comprehensive ODS faces challenges due to a lack of economic incentives for data sharing among competitors and a general mistrust in the fairness of the data-sharing landscape, which can deter organizations from participating.

Further complications arise from the regulatory perspective. The European Commission recognizes that while voluntary data sharing is preferred, specific circumstances might necessitate compulsory sharing to address market failures and encourage initial data-sharing efforts among reluctant stakeholders. The Data Act, for instance, includes provisions that could compel data sharing in exceptional circumstances, such as public emergencies or to fulfil tasks in the public interest. This may override organizational data sovereignty.

This tension between organizational control over data and the public or collective benefits of data accessibility reflects the broader challenge of balancing private rights with public goods within the EU's digital strategy. The implementation of ODS in sector-specific contexts like the EHDS shows that while organizational control is one goal, it may not take precedence over public interests, such as public health emergencies.

While ODS is a key objective within the EU's data strategy to stimulate a dynamic data economy, its realization is nuanced and depends on balancing organizational autonomy with broader societal and economic imperatives.

Finally, SDS requires balancing the existing relations between agents and their practical requirements for data sovereignty. It should mitigate resulting power struggles, which may lead to the undesirable overreach of states, to enable data access for desirable goals while staying in line with characteristic SDS purposes. We argue that SDS within the context of the CEDS and specifically through the EHDS is realized by maintaining a balance between state-level control and broader EU regulations. SDS is primarily about a state's authority to manage and regulate data related to its domestic affairs independently, without external interference. This includes making decisions about data storage, sharing, and use within a state's jurisdiction, which is crucial for maintaining cybersecurity, national security, and political stability.

In the EU, however, states operate under a shared sovereignty model due to their membership in the Union. This shared model does not imply a loss of sovereignty but a delegation of certain powers to the EU, which can theoretically be reclaimed. This is evident in data governance, where the TFEU provides the EU with competencies to regulate the internal market, including data.

The EHDS is an example where the EU's regulatory framework interacts with state sovereignty in data governance. The EHDS allows for data sharing across EU member states but still respects the role of national HDABs in controlling specific data permit decisions. These bodies decide who can access health data, and under what conditions, and are required to operate within both national and EU regulations.

The governance structure ensures that while the EU facilitates and oversees cross-border data sharing for health-related purposes, individual member states retain significant control over the data registered within their jurisdiction. This structure maintains state sovereignty by allowing states to control access to and use of data, even as it supports EU-wide goals such as improved health services and research capabilities.

Overall, SDS in the context of the EHDS—and potentially other European data spaces—is maintained through a nuanced system where states delegate some control to the EU but retain significant sovereign powers, especially in making critical administrative decisions regarding data access and use. This arrangement reflects the complex relationship between state sovereignty and EU governance in managing the balance between individual state interests and collective European goals.

This subordination of all types of sovereignty under SDS leads to the issue of overreach on the side of the state over organizational and individual data sovereigns. Since the SDS seems to be the most potent form of exercising power over data in the context of the EHDS, it is thus purposeful for the strategic goals of the CEDS to involve other types of sovereignty on a similarly relevant and valid footing. One should aim to protect other sovereignty holders based on rules and norms rather than only relying on political will. Therefore, sovereignty in data spaces should not be seen as absolute, as sovereignty has historically been defined, but as shared between individuals, organizations, and states.

Due to the sensitive *sensu largo* nature of health data, the EHDS proposal seems like a suitable example of resolving tensions between different data sovereignty agents while not proclaiming it as a form of absolute data sovereignty for any individual party and appears to also be the possible interpretation under the EHDS proposal as in Recital 1 of the preamble, the legislator states that:

> *[…] in order to improve access to and control by natural persons over their personal electronic health data in the context of healthcare (primary use of electronic health data), as well as for other purposes that would benefit the society such as research, innovation, policy-making, patient safety, personalised medicine, official statistics or regulatory activities (secondary use of electronic health data). In addition, the goal is to improve the functioning of the internal market[…].*[196]

The balancing act between the aims and values upon which the EHDS is established suggests the need for a balance between individuals, organizations, and states to prevent overreach between each type of right. Data sovereignty will only take a practical step toward effective realization

[196] (2022) COM 197 final.

within the CEDS when the rights and obligations, as well as the values and needs of each party, are formally acknowledged and addressed. The practical impact and effectiveness of this proposal depend on the balance of power among all interested parties; it should not disproportionately favour one side, as this could lead to excessive overreach.

In this paper, we learn that data sovereignty is a confluence of factual, socio-political, technical elements, and established formal statements and institutions. Such a broadly defined term tends to be practically unhelpful; as we mentioned, it is not explicitly referenced in digital-related European laws or legislative proposals. The absence of data sovereignty is apparent not only in the main body of legal acts, which consists of rules and norms related to rights and obligations but also in the preamble consisting of recitals, which provide a binding interpretive background for the application of the law. Through our analysis, we have established that it can be understood as an overarching term encompassing multiple meanings, terms, and institutions under a common designation. To render it more practically useful, we have attempted to specify its broad and narrow senses. In the broad sense, data sovereignty can be seen as the aforementioned horizontal term that holds multiple meanings, terms, and established institutions, typically within a broad socio-technical or political context. In the narrow sense, we argue that data sovereignty can be limited to the meanings it acquires in the context of agents holding imperium over data, adhering to the principle that sovereignty is inherently attributable to entities, not objects.

We posit that establishing wide and narrow understandings of data sovereignty facilitates the practical application of this term. Each existing cultural artefact allows for renewed interpretation in response to changes in the status quo. Given that we treat law broadly as a cultural artifact, in line with well-established legal theory, we maintain that legal terminology and institutions concerning individuals' rights and obligations can be updated as interpretative circumstances evolve.

One circumstance particularly relevant to EU law is the change in the legal system, which may stem from new legislation entering the legal framework. Considering the specific structural nature of EU law, which influences its systemic perception, its 'multi-layered' character is crucial. Within this framework, it is possible to distinguish between normative regulations of varying legal force—primary law, secondary law, EU international law, and organizational law concerning EU institutions—as well as the case law of the Court of Justice of the European Union, including both judgments that express legal principles and 'ordinary' judgments. The diverse nature of the components of EU law also relates to the distinction between directly binding acts, acts requiring implementation through national legislation (directives), and 'soft law' acts (recommendations and opinions). This relationship is clearly visible within EU's digital acquis. For example, the Digital Services Act corresponds strongly with the Digital Markets Act and AI Act, while the same can be said for the Data Act and Data Governance Act, with the General Data Protection Regulation (GDPR) serving as the foundation for the entire EU cyber law system.

Thus, we contend that exploring the possibility of data sovereignty is a worthwhile approach that could substantiate changes in the current understanding of norms, as well as inform future regulatory frameworks. First, let us examine the potential implications for the existing cyberlaw system. Data sovereignty should be regarded as a value pertinent to the systemic interpretation of legal norms and rules, encompassing the rights and obligations of entities within either the system of European law or EU cyberlaw. Initially, it is essential to ascertain whether data sovereignty is an integral part of the system under consideration. Our analysis demonstrates that data sovereignty is reflected within the normative structures of EU legal acts; although not explicitly mentioned, this principle can be inferred from the existing institutions and normative assumptions in the preambles of legal acts that form part of the Union's legal framework. Based on the analysis presented in this article, we believe that it can be safely accepted that data sovereignty is both an integral and significant component of this system.

Secondly, it is necessary to evaluate the position of data sovereignty within the hierarchy of the legal system—whether it holds a supreme, equivalent, or subordinate status relative to other legal institutions. This assessment will inevitably vary depending on the context of the specific case at hand. It may be possible to interpret the value of data sovereignty from the preambles of legal acts, thereby assigning it a guiding and predominant role in the application of the law. Conversely, data sovereignty might appear only within the main text of the law among other norms and regulations, which would suggest, at most, an equivalent status. Moreover, it is conceivable to encounter situations where data sovereignty is not clearly or exhaustively indicated by normative clues, due to its broad concept even in a narrowly defined sense. In such cases, data sovereignty can be employed in an interpretative context where it assumes a subordinate relationship.

Even in scenarios where the application of data sovereignty is impractical in a systemic interpretation due to the inability to establish systemic connections or lack of recognition for our classification, it is difficult to disregard the potential role of data sovereignty in a functional interpretation. Given the presence of norms and regulations that may conceptually, purposefully, and technically overlap, data sovereignty provides a context that can functionally unify existing institutions and mitigate contradictions or counterproductivity in realizing established values. This facilitates the effective application of norms with consideration for their intended purposes.

Though the conclusions of this paper are critical, a re-definition of 'sovereignty' in the context of data spaces could be fruitful in reflecting the balance of power between the three types of agents. Such a re-definition is only effective if undertaken and formalized by the Commission. In this light, we propose to utilize data sovereignty as an interpretatory lens to position this normative background in a systemic way. Such adoption would allow for a swift alignment of legislative initiatives with ever evolving digital policy landscape. Systemic interpretations, through the lens of data sovereignty, would allow to normatively align the EU's digital acquis at the early stage of its application, as well as enhance the practical processes of case-by-case applications of legal norms to data problems in CEDS.

Future research should explore such a project by paying particular attention to how data sovereignty can be realized in practice. Specifically, the effectiveness of the GDPR consent regime in the context of IDS is questionable, particularly in how meaningful consent is achieved in practice. We identify the consistent need for the EU to conduct serious research into the robustness of the consent principle, suggesting a potential for the current system to lead to behaviours that undermine the foundational GDPR principles of data protection. Research could explore how manipulative design and the 'privacy paradox' affect genuine consent and what remedial steps might be taken.

Furthermore, in the context of ODS the high levels of non-compliance with EU' digital acquis among companies suggests a need for research into improved guidance and harmonization between national and EU-wide enforcement policies. This includes the effectiveness of the decentralized system of national authorities and the mechanisms in place, such as the consistency mechanism and urgency procedure, to handle divergences in implementation.

Future research should also include examining the impact of competition within the primary market where data is generated on the relationship between IDS and ODS. This aspect is crucial as competition can limit the ability of organizations to maximize profits from protected consumer data, potentially altering the optimal allocation of data rights.

Furthermore, the assumption of dyadic interactions in data transactions (one firm and one consumer) should be considered as a limited understanding of data transactions in reality.

RReal-world data interactions often involve multiple parties, as seen in industries like automotive or social media, where data about behaviour or preferences could be shared among various stakeholders. To address these complexities, future research could explore multi-agent models that more accurately reflect the multifaceted nature of data transactions. This would provide a deeper understanding of how data rights could be optimally allocated in scenarios where multiple entities, including consumers, different types of firms, and public sector have stakes in the data being generated and used.

Overall, these avenues for future research could help craft more nuanced data governance policies that align with the diverse values, interests, and economic roles of all parties involved in promoting a public good.

FUNDING

This paper was funded by the call DIGITAL-2021-PREPACTS-DS-01, agreement number 101083401.

Conflicts of interest: None declared.