Solidarity at the intersection of data sharing and data protection: A normative analysis

Esin Küçük, Essex Law School

Elif Mendos Kuşkonmaz, Essex Law School

Accepted for publication in Maastricht Journal of European and Comparative Law.

Solidarity at the intersection of data sharing and data protection: A normative analysis

This article explores the evolving role of the principle of solidarity in shaping EU data sharing policies amidst global crises, with a specific focus on the implications of the Data Governance Act. During a period marked by significant health emergencies, the necessity of data sharing has emerged as a paramount goal within the EU legislative framework. This analysis investigates the interplay between solidarity and the dual goals of data sharing and data protection. It focuses on how solidarity influences data governance and the implementation of new data sharing frameworks, specifically in areas such as interpreting 'general interest', balancing competing interests, and mitigating harm. The article argues that solidarity not only can support data sharing by underscoring its societal benefits but also safeguard these benefits from being overshadowed by economic aims. In scenarios of conflict, solidarity can maintain that data sharing, while addressing general interests, remains closely tied to mitigating societal vulnerabilities. Additionally, solidarity can substantiate harm mitigation claims when data sharing results in damages. Therefore, solidarity is not just a supportive force for data sharing initiatives but a nuanced tool that aligns with societal needs, promising a balanced approach to the competing priorities of data protection and data sharing.

1. Introduction

The EU has navigated a turbulent period that has vividly underlined the indispensable role of solidarity in managing emergent situations. This period has not merely precipitated a profound re-evaluation of the principles of solidarity in established domains such as asylum and monetary union, but also extended its pertinence to new sectors, particularly those involving data governance and digital technologies. The health crisis, in particular, has showcased the critical importance of data in managing emergencies, both in making crucial decisions about restrictions on freedoms and in driving innovations through health data utilisation. This realisation has intensified efforts to strengthen data availability and accessibility, setting the stage for innovative data-sharing paradigms designed to optimise collective benefits derived from data cultivation.

Most notably, newly introduced Data Governance Act (DGA),[1] which is of central interest to us, aims to maximise data sharing for the general interest of public. It seeks to achieve this firstly by requiring public sector bodies to make certain types of protected data available for re-use, while ensuring the confidentiality of personal data through anonymisation and of commercially sensitive information through modification, aggregation, and secure handling.[2] Secondly, the DGA seeks to encourage the pooling of personal and commercial data through voluntary contributions, a process known as 'data altruism'. The legislative definition of data altruism is "the voluntary sharing of data on the basis of the consent of data subjects to process personal data pertaining to them, or permissions of data holders to allow the use of their non-personal data without seeking or receiving a reward that goes beyond compensation

[1] Regulation (EU) 2022/868 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act) [2022] OJ L 152.

[2] Articles 3-14, DGA. Data eligible for sharing, as defined under Article 3(1), includes data that is commercially sensitive, statistically confidential, protected by intellectual property rights, and personal data.

related to the costs that they incur where they make their data available for objectives of general interest as provided for in national law".[3] General interest grounds, which goes beyond narrow public interest of national security, are exemplified as "healthcare, combating climate change, improving mobility, facilitating the development, production and dissemination of official statistics, improving the provision of public services, public policy making or scientific research purposes in the general interest".[4] Notably, the sharing of data concerns under data altruism does not only concern non-personal data but also personal data to which the data subject consent to share.[5] Thus, fundamentally aiming to utilise and promote data sharing within established constraints, the DGA contrast with the General Data Protection Regulation (GDPR),[6] whose primary goal is to ensure data protection but also permits use of personal data for public interest grounds.[7]

This article examines the evolving prominence of data sharing as a primary objective within the EU legislative framework, addressing how the legal principle of solidarity underpins data sharing and how it can influence the implementation of law on data governance, a question that has not yet been explored.[8] The objective of the article is three-fold: First, to show the central role the data sharing assumes in data governance against data protection, which has been a primary objective of data governance. We assert that the data sharing as a primary objective is built on the function of data in serving diverse interests in the society. Second, we aim to explain how the principle of solidarity relates to law on data sharing. We contend that data sharing, when aimed to serve societal needs and necessitating some level of sacrifice from the data subject, is fundamentally driven by the principle of solidarity. The data governance framework of the EU, both in voluntary and mandatory forms, encompasses data sharing that is underpinned with solidarity. Third, based on this conclusion, we seek reflect on how the nexus between data sharing and solidarity matters, by exploring the ways in which a solidarity-based interpretation can inform both the reading and implementation of the relevant legislative frameworks. We conclude that the significance of a solidarity-based approach to implementing data sharing laws resides in its capacity to offer a value-driven framework that ensures fair distribution of the costs and benefits of data sharing. This approach not only is crucial for achieving a delicate balance between the dual objectives of data protection and data sharing when they conflict, but it also deeply resonates with the foundational principles of the EU's constitutional order.

---

[3] Article 1(c), DGA.

[4] Ibid.

[5] Article 25, DGA.

[6] Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L 119.

[7] Ibid, Article 6(1)(e).

[8] There is a growing body of literature analysing the emerging law concerning data governance from a legal perspective, though primarily focusing on its compatibility with the existing data protection legal framework. I. Graef, R. Gellert and M. Husovec, 'Towards a Holistic Regulatory Approach for the European Data Economy: Why the Illusive Notion of Non-Personal Data Is Counterproductive to Data Innovation', 44 *European Law Review* (2019), p. 605; C. Kruesz and F. Zopf, 'The Concept of Data Altruism of the Draft DGA and the GDPR: Inconsistencies and Why a Regulatory Sandbox Model May Facilitate Data Sharing in the EU', 7 *European Data Protection Law Review* (2021), p. 569; G. Comandè and G. Schneider, 'It's Time: Leveraging the GDPR to Shift the Balance Towards Research-Friendly EU Data Spaces' 59 *Common Market Law Review* (2022), p. 739; Y. Miadzvetskaya, 'Data Governance Act: On International Transfers of Non-Personal Data and GDPR Mimesis', 9(1) *European Data Protection Law Review* (2023), p. 25.

The structure of this article unfolds as follows: Section 2 provides an overview of how data governance has evolved within the EU, illustrating how data sharing has emerged as a central and legitimate goal alongside data protection. Section 3 investigates data sharing under DGA with a view to explaining how and to what extent this concept embodies the principle of solidarity. Section 4 explores the ways in which solidarity, as a legal principle, can inform the implementation of the new data governance regime and reflects on the added value of solidarity-based approach in data sharing. Section 5 concludes.

2. Evolving paradigms in EU Data Governance: Data sharing as a primary objective

Data sharing has not traditionally been a fundamental goal of data governance. On the contrary, the primary goal of EU data governance has centred on the protection of personal data, which inherently restricted opportunities for data sharing. Although protecting personal data remains a critical priority, the significance of data sharing has increasingly come to the fore. In this discussion, we aim to explain the shift in the orientation of data governance within the EU, which now strives to balance the dual objectives of data protection and facilitating data sharing.

The initial phase of data governance the focus of data management has been the protection of personal data. 1970s and 1980s were predominantly occupied with attempts to govern or, more precisely, limit state collection of personal data.[9] Influenced by the Council of Europe initiatives on the topic,[10] the EU legislation on data governance concentrated primarily on controlling the risks of digitalisation and the safeguarding of personal data. The EU approached the question of personal data protection regulation as that of fundamental rights, initially with the Data Protection Directive,[11] to be succeeded by the GDPR. Today, along with other sector-specific legislation,[12] the GDPR sets out rules for the collection, processing, and safeguarding of personal data while also defining precise roles and responsibilities for data controllers and processors. More importantly, protecting personal data is recognised as a fundamental right in addition to the right to privacy in the Charter of Fundamental Rights by the Court of Justice of the EU (CJEU).[13] The Court has invariably acknowledged the

[9] F. W. Hondius, *Emerging Data Protection in Europe* (North Holland Publishing Company, 1975); C. Bennett, *Regulating Privacy: Data Protection and Public Policy in Europe and the United States* (Cornell University Press, 1992). See also Y. Marique and E. Slautsky, 'Freedom of Information in France: Law and Practice' in D.C. Dragos, P. Kovač, and A.T. Marseille (eds) *The Laws of Transparency in Action; Governance and Public Management* (Palgrave, 2019), p. 73 (explaining how the monumental scandals in France in the early 1970s triggered the first legislative efforts to limit the collection of personal data).

[10] Convention for the Protection of Individuals with Regard to the Processing of Personal Data (ETS No. 108), available at: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108; G. Hornung and C. Schnabel, 'Data Protection in Germany I: The Population Census Decision and the Right to Informational Self-Determination', 25(1) *Computer Law & Security Review* (2009), p. 84; G. González Fuster, *The Emergence of Personal Data Protection as a Fundamental Right of the EU* (Springer, 2014).

[11] Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L 281.

[12] Directive (EU) 2016/680 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA OJ L119/1; Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) OJ L 201/37.

[13] Article 8, EU Charter. See also Case C-203/15 *Tele2 Sverige AB v Post –ochtelestyrelsen and Secretary of State for the Home Department v Tom Watson and Others*, EU:C:2016:970, para 124.

significance of data protection rights under the Charter, interpreting its importance relative to other Charter rights and contrasting its application at the national level.[14] This was particularly evident in the landmark case of *Digital Rights Ireland*, wherein the CJEU annulled the Data Retention Directive[15] on the grounds of its undue interference with the Charter's provisions.[16] Despite some complications remains,[17] with these development, personal data protection acquired a robust fundamental rights approach protected by the EU constitutional order.

For a long time, most controversial issue in EU data governance has been the Member States' demands for data access for law enforcement reasons, in particular in the context of irregular migration and crime prevention. In fact, the annulled Digital Data Retention Act was one part of a set of a legislative framework which allow access to personal data on public security grounds. The legislative framework involves, the Advanced Passenger Information Directive, under which carriers were required to relay data pertaining to passengers originating from non-EU countries.[18] There also has been a noticeable escalation in governmental intervention regarding the collection and utilisation of personal data from air travellers within the EU. This expansion of scope is particularly aimed at the prevention of serious criminal activities and acts of terrorism. In this context, the Passenger Name Record Directive was introduced,[19] which serves to regulate the processing of passenger data not only on flights entering or exiting the EU but also on those traversing within its borders.

It would be wrong to assume that the tension over data access has been resolved. Member States continue to demand access to personal data for public safety purposes, with a recent example being the proposal for a new Security Package aimed at facilitating lawful access to encrypted digital data to combat serious and organized crime.[20] However, beyond these security considerations, the discourse over data access has taken a new turn as the demand for data now extends beyond mere public security grounds. As technology advances, the same data sought for public safety is also propelling economic transformations, heralding a new phase in EU data governance where data demands not only address security concerns but also fuel the burgeoning data economy. Since the early 1990s, technological advancement has led to a significant increase in data-driven companies, so much so that a distinct data economy has

[14] O. Lynskey, 'Article 8: The Right to Data Protection' in M. Bobek and J. Prassl, *The EU Charter of Fundamental Rights in the Member States* (Hart Publishing, 2020), p. 355.

[15] Directive 2006/24/EC on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC [2006] OJ L105.

[16] Joined Cases C 293/12 and C-594/12 *Digital Rights Ireland and Others*, EU:C:2014:238.

[17] On difficulties with reconciling fundamental rights protection of personal data and internal market incentives, see M. Finck, 'The Maturation of European Data Law: From Fundamental Rights to Economic Rights' in J. Adams-Prassl (ed.) *The Internal Market Ideal: Essays in Honour of Stephen Weatherhill* (Oxford University Press, 2024), pp. 39-58.

[18] Council Directive 2004/82/EC on the obligation of carriers to communicate passenger data [2004] OJ L 261, Article 1.

[19] Council Directive 2016/681 on the use of passenger name record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime [2016] OJ L 119.

[20] Swedish Delegation, Non-paper on a New SecEUrity Package, 5 June 2024, available at: https://www.statewatch.org/news/2024/july/. In 2023, the EU established the High-Level Expert Group on Access to Data for Law Enforcement. This group was tasked with exploring the challenges law enforcement officers encounter in accessing data and developing potential solutions to these issues. For more information, see: EU Home Affairs.

emerged.[21] Advancement in digital technology and infrastructure allowed the collection of strategic data in mass, which has been crucial in cultivating a robust data economy.[22] Overtime, the foundation of the digital economy has shifted from merely delivering services to incorporating the operationalisation of data generated by these services.[23] In turn, this data has pushed the advancement of new digital technologies and innovations, providing a competitive edge to companies that own significant data resources.[24] These developments have enabled data-driven companies not only to create entirely new categories of products and services but also to forge a unique economic field, where data is actively collected, manufactured, and traded establishing it as a valuable capital.[25] Given the strategic value of data, its production is now a key driver of profitability in the digital economy,[26] fostering a thriving data-centric economic sector.

In response to the economic benefits of better cultivation of data, since 2014, the European Commission has redirected its regulatory focus to leverage the strategic potential of data and stimulate data-driven economy.[27] In its 2017 Communication, the Commission stressed the problem of underutilisation and inadequate sharing of non-personal data, particularly in the context of innovation, as a substantive policy concern.[28] This issue has precipitated the enactment of legislation to ensure free flow of non-personal data and regulate the conditions under which data localisation may be permitted within the EU.[29] It is important to highlight that the focus of data sharing in this new context of data sharing was to promote data economy is non-personal data.[30]

More recently, the rationale for data sharing has expanded further to encompass pressing societal needs. Particularly in response to the COVID-19 pandemic, societal value of

[21] On the growing role of information as a commodity and the growing 'information industry', see D. Schiller, *How to Think about Information* (University of Illinois Press, 2007), pp. 36-37.

[22] OECD, Enhancing Access to and Sharing of Data: Reconciling Risks and Benefits for Data Re-use across Societies, (OECD Publishing, 2019) (suggesting that enhancing access to and reuse of data could yield significant social and economic benefits, potentially contributing up to 1.5% of GDP from publicly held data alone. When including privately held data, the potential economic impact could range from 1% to 2.5% of GDP).

[23] On the ways in which data is collected and utilised by the retailers, L. Einav and J. Levin, 'The Data Revolution and Economic Analysis', *Innovation Policy and the Economy* (2014), pp. 2-3, 5.

[24] For an analysis of how data collection and analysis can drive innovation, refer to A. Goldfarb and C. Tucker, 'Privacy and Innovation', *Innovation Policy and the Economy* (2012), pp. 67-69.

[25] J. Sadowski, 'When Data Is Capital: Datafication, Accumulation, and Extraction, *Big Data & Society* (2019), p. 1 (identifying data as a unique form of 'capital' and associating the imperative of data collection with the continuous cycle of capital accumulation).

[26] OECD, *Data-Driven Innovation* (OECD Publishing, 2015) 29 (indicating that businesses that focus on data-driven innovation and analytics tend to experience productivity growth rates that are 5% to 10% higher than those that do not invest in these areas).

[27] European Commission, Communication from the Commission to the European Parliament, the Council and the European Economic and Social Committee and the Committee of the Regions, Towards a thriving data-driven economy, COM/2014/0442 final.

[28] European Commission, Building a European Data Economy, COM(2017) 9 final, 13.

[29] Regulation (EU) 2018/1807 on a framework for the free flow of non-personal data in the European Union [2018] OJ L 303.

[30] T. Tombal and I. Graef, 'The Regulation of Access to Personal and Non-Personal Data in the EU: From Bits and Pieces to a System?' in V. van der Sloot, S. van Schendel, *The Boundaries of Data* (Amsterdam University Press, 2024) pp. 198-199 (defining non-personal data as i) data that has never been personal data in the first place; ii) anonymised personal data that no longer allows identification of the data subject).

data has received heightened recognition not only in the digital and medical innovations, but also in terms of informed decision making in the public sector. Today, the relevance of data spans multiple sectors, including scientific research, health, energy, and environmental sectors, where the demand for data access continues to surge, highlighting its relevance and importance in serving the 'public good'.[31] In this new phase, the focus has been shifted to sharing data- by making it more available and accessible- for the benefit of 'general interest' which includes its commercial and public interests at large.

Another factor that significantly increase the value of data is the pursuit of digital sovereignty, aimed at mitigating digital dependency on external jurisdictions.[32] The research indicates that countries across the world have highly unequal digital capabilities, and most European countries depend on digital technologies controlled by foreign entities.[33] Dependency on certain technologies for public administration is widespread, as only a few global companies, based in a handful of countries, meet the criteria to supply governments with the necessary technologies at prices that align with the uniform public procurement rules, which often prioritises the most affordable option.[34] Against this backdrop, there is an increased effort by jurisdictions, including the EU, to enhance their digital sovereignty while asserting control over their data, which is considered raw material for digital technologies.[35] For the EU, there is also a strong impetus to uphold European core values, particularly in response to numerous international data protection scandals that have compelled the EU legislature to intervene.[36]

The increasing surge for data driven by increasing economic and societal value of data, led the EU to develop 2020 European Digital Strategy that aims to create a European Data Space.[37] In line with the strategy of promoting data sharing, apart from DGA, the EU has introduced a number of legislative instruments, including Open Data Directive,[38] the Digital Markets Act[39] and the Digital Services Act[40], the DGA, and most recently the Data Act (DA).[41]

---

[31] The World Bank, 'World Development Report 2021', pp. 54-62, available at: https://wdr2021.worldbank.org/the-report/.

[32] D.W. Arner, G.G. Castellano & E.K. Selga, 'The Transnational Data Governance Problem', 37 *Berkeley Tech Law Journal* (2022), pp. 623, 660.

[33] M. Mayer and Y. Lu, 'Digital Autonomy? Measuring the Global Digital Dependence Structure' (2023), pp. 10-17, available at SSRN: http://dx.doi.org/10.2139/ssrn.4404826.

[34] R. Ávila Pinto, 'Digital Sovereignty or Digital Colonialism?', 15 *Sur International Journal on Human Rights*, (2018) p. 20.

[35] In specific to the EU, see European Parliament, 'Digital Sovereignty for Europe', EPRS Ideas Paper, July 2020. See also, H. Roberts et. al., 'Safeguarding European Values with Digital Sovereignty: An Analysis of Statements and Policies' 10 *Internet Policy Rev* (2021), p. 1.

[36] E. Celeste, 'Digital Sovereignty in the EU: Challenges and Future Perspectives', in F. Fabbrini, E. Celeste and J. Quinn (eds), *Data Protection Beyond Borders: Transatlantic Perspectives on Extraterritoriality and Sovereignty* (Hart Publishing, 2021), pp. 219, 220.

[37] European Commission, A European strategy for data, COM(2020) 66 final.

[38] 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 L *172*.

[39] Regulation (EU) 2022/1925 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act) [2022] OJ L 265.

[40] Regulation (EU) 2022/2065 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act) [2022] OJ L 277.

[41] Articles 3(1) and 4(1), Regulation (EU) 2023/2854 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act) [2023] OJ L 2023/2854.

The evolving framework is strategically designed to optimise data accessibility and maximise the benefits of effectively cultivating data, not only in economic terms for business but also as a society, in general, across the EU.

The intensified focus on optimal utilisation of data introduces a new paradigm in EU data governance which is characterised by central role attributed to data sharing. Although safeguarded under Article 8 of the EU Charter for Fundamental Rights, data protection is not an absolute right, and the same provision allows for the use of personal data for legitimate purposes. In parallel, the GDPR, has already set a framework in order to sustain data sharing for the purposes of public interest, and scientific research.[42] The dual objective of data protection and facilitating data sharing on legitimate grounds is indeed embedded within the GDPR.[43] In fact, based on the existing framework, the added value of data altruism scheme under DGA has been questioned.[44] The added value of the Data Governance Act lies in the introduction of data sharing not just as a legitimate but as a primary goal, which is based on the idea of benefiting general interest of the society at large. It is crucial to acknowledge the operational differences between the DGA and the GDPR, where the former emphasises data sharing, while the latter focuses more rigorously on data protection.[45] Therefore, the current EU data governance framework strives to balance these dual objectives, where we posit that solidarity can play a critical role.

3. Nexus between data sharing and solidarity

Although a detailed exploration of solidarity as a legal concept is beyond the scope of this discussion, understanding the connection we argue exists between data sharing and solidarity, necessitates a brief explanation of its normative force and meaning.

Solidarity is a constitutional principle that is strongly rooted in EU Treaties.[46] Reflecting the significance accorded to constitutional provisions, the fundamental role of solidarity in EU legal order has been acknowledged by the CJEU. In judicial proceedings, it functions both as a protective 'shield', supporting Union acts that introduce new obligations of solidarity,[47] and as a 'sword', providing a standard for the legality of both EU and national acts in constitutional reviews.[48] Notably, the General Court acknowledges 'solidarity between the Member States' as a general principle of EU law.[49] Moreover, the Court of Justice categorises it as a fundamental principle of EU law,[50] which arguably allows the use of this principle beyond inter-state relationships. The overarching nature of solidarity is particularly crucial for

[42] Article 6, GDPR.

[43] H.C.H. Hoffman and L. Mustert, 'Five Years of GDPR – Lessons for Procedures, Agencies and Powers', in H. Matsumi *et al.* (eds.) *Data Protection and Privacy* (Hart Publishing, 2024), p. 10.

[44] Ibid, para 159.

[45] For an in-depth analysis of the varying normative considerations embedded within these acts, and to explore the distinctions in their emphasis on data protection, refer to, see Y. Miadzvetskaya, 'Data Governance Act: On International Transfers of Non-Personal Data and GDPR Mimesis' (2023) 9(1) *European Data Protection Law Review*, p. 25.

[46] TEU, Articles 2, 3, 4(3); TFEU, Articles 80, 122, 194, 222.

[47] Joined Cases C-643/15 and C-647/15 *Slovak Republic and Hungary v Council,* EU:C:2017:631, paras. 251-53; Case C-646/16 *Jafari*, EU:C:2017:586, para 88.

[48] Case T-883/16 *Republic of Poland v European Commission*, EU:T:2019:567, para 83.

[49] Ibid, para 69.

[50] Case C-848/19 P *Germany v Commission*, EU:C:2021:598, para 38.

the purposes of our analysis here. This is because it renders the principle normatively significant in fields where it is not explicitly mandated as a constitutional obligation, including data governance and digital transformation.

As far as its meaning is concerned, solidarity can be best understood as a hybrid principle, which is both underpinned with instrumental and value-based reasoning. In the Court's jurisprudence, it is mostly understood in an instrumental manner. This means sacrificing short-term self-interest for common goals to achieve benefits for all in the long term, a concept that is pervasive in EU jurisprudence.[51] It serves to substantiate demands for sacrifices for the benefits that are gained from the attainment of common objectives. Thus, it is characterised by not only supporting others by forfeiting self-interest, but also contribution towards common goals from all benefits. As the architecture of EU constitutionalism has been predominantly shaped around economic objectives, the term 'solidarity' has evolved into a central motif in legitimising the demands of the process of economic integration and addressing the challenges that arise with it. The functional imperatives associated with establishing an economic union, such as a single market, the absence of internal borders, and a unified currency, necessitate a foundational level of solidarity. Therefore, the concept has anchored itself at the heart of functional integration.[52] It is largely built on an instrumental rationale that a commitment to economic integration aimed at collective well-being and prosperity often requires the immediate sacrifices of individual member states for the attainment of common objectives.

Value-driven forms of solidarity, such as social solidarity, also exists under EU law, though lagging behind.[53] The EU primary law, though not presenting an explicit obligation, includes provisions that reflect a value-based understanding of solidarity. For instance, in the preamble of the TEU, solidarity extends beyond a mere principle to become a declarative force, with the Member States committing to a renewed phase of European integration. This commitment involves a deepening of solidarity among their peoples, mindful of their historical, cultural, and traditional contexts. Similarly, the preamble of the Charter of Fundamental Rights encapsulates 'indivisible and universal values' at the heart of the EU values, notably including solidarity. The preamble of TFEU further reinforces this, expressing the Member States' intent to confirm the solidarity binding Europe and its overseas territories and to promote their prosperity in alignment with the principles of the Charter of the United Nations. These provisions embody a concept of solidarity based on values, focusing not merely on accepting sacrifices for the common good, but rather on supporting others to address their needs and vulnerabilities. It is true that the normative force of these provisions is limited. Nevertheless, the significance of these provisions lies not only in providing guidance to legislators but also in their normative impact, as they permit interpretations of the legislation that further these objectives.

Leaving aside the driving forces behind it, solidarity as a legal principle embodies two key characteristics: it requires a level of sacrifice from the contributor and aims to assist others. Both characteristics are evident within the EU data governance framework's approach to data

[51] For instance, Case 276/80 *Ferriera Padana SpA v. Commission*, EU:C:1982:57, paras 30-32.

[52] T. Isiksel, *Europe's Functional Constitution* (Oxford University Press, 2016) p. 87. On the link with the concepts of solidarity and constitutional federalism, see E. Gill-Pedro, 'Solidarity Through the Lens of Functional Constitutionalism', 6 *Nordic Journal of European Law* (2023), pp. 119-120.

[53] This is despite the Court's advancement on social solidarity between the EU citizens, Case C-184/99 Grzelczyk, *EU*:C:2001:458.

sharing. First, data sharing as envisaged under DGA, whether voluntary or mandatory, involves some level of sacrifice for contributor, which is characteristic of a solidaristic action. While data itself is not a consumable commodity that diminishes when shared, sharing can still entail sacrifices for the data owner. This process inherently carries risks for the data subject or owner, primarily the potential for data to be accessed by unauthorized parties or used for unauthorised purposes. As far as data altruism is concerned, the Member States are entrusted with the obligation to establish national policies relating to the organisational and technical arrangements for data altruism.[54] Data shared under this scheme is to be collected and managed by trusted 'data altruism organisations' that act as repositories for data, voluntarily shared for altruistic purposes on a non-profit basis.[55] These organisations bear specific responsibilities towards data subjects and data holders. Data altruism organisations must inform data owners about the general interest objectives for which the data is processed, ensure the data is not used for unauthorised purposes, and maintain a high level of data security.[56] Furthermore, these organisations are obliged to notify data holders of any unauthorised transfer, access, or use of the non-personal data they have shared.[57] These safeguards, aiming to minimise the likelihood and impact of such breaches, highlight the potential vulnerabilities that come with sharing data.

Second, data sharing is driven by the goal of supporting others, which is the second characteristic of solidaristic action. Defined as 'general interest' under the DGA, the objectives of data sharing can include "healthcare, combating climate change, improving mobility, facilitating the development, production and dissemination of official statistics, improving the provision of public services, public policy making or scientific research purposes in the general interest".[58] We discuss the term later more in detail,[59] suffice to say here that it is intentionally defined open ended, and with a view to maximise the potential societal benefits of data use. Adopting a broader approach, one can argue that the term general interest extents to the distribution of value from data among stakeholders, bolsters innovation, and enhances competition, all of which benefit society, if not directly, indirectly in a longer term. Although drawn broadly, it is important that solidarity conditions the utilisation of data for general interest of society, as it recognises individuals' essential role in achieving general interests so that individual sacrifice is driven towards a societal purpose instead of relating to a carte blanche purpose for which data can be reutilised. In this way, solidarity is reflected within the idea of making collective contributions for the societal good.

It is useful to underline that data altruism envisages a voluntary type of contribution,[60] though data sharing designed under EU data governance can be on mandatory basis, where

[54] Article 16, DGA.

[55] Articles 17-18 and Article 23, DGA.

[56] Article 21, DGA.

[57] Ibid.

[58] Article 12(16), DGA. ["data altruism means the voluntary sharing of data on the basis of the consent of data subjects to process personal data pertaining to them, or permissions of data holders to allow the use of their non-personal data without seeking or receiving a reward that goes beyond compensation related to the costs that they incur where they make their data available for objectives of general interest as provided for in national law, where applicable, such as healthcare, combating climate change, improving mobility, facilitating the development, production and dissemination of official statistics, improving the provision of public services, public policy making or scientific research purposes in the general interest."].

[59] For further discussion of the concept, see below, Section 4.1.

[60] J. Mazur and M. Słok-Wódkowska, 'Access to Information and Data in International Law How to Find a Path Forward from Human Rights-Oriented and Market-Oriented Approach?' 91 *Nordic Journal of International Law* (2022), p. 310 (the authors argue for an obligatory data sharing framework to promote data sharing, specifically

solidarity can be a relevant concept. A broad interpretation of solidarity, encompassing mandatory contributions such as social welfare systems and mandatory vaccinations, more accurately reflects the concept's normative nature as it is applied in both EU and international human rights law.[61] For clarity, solidarity does not substantiate all of those data sharing obligation. Rather, access to data demands may as well be resulting from other legitimate interests. For example, the Data Act aims to ensure that data generated by connected devices and services is accessible to users, both consumers and businesses.[62] The core principle that underpins the data sharing in this context is to empower data holders with control over their data, which is grounded in the concept of privacy. This understanding of solidarity as sacrificing for common good resonates with the data sharing scheme under EU *acquis communautaire*, to the extent that it seeks to promote sharing of both personal and commercial data for the broader goals for the benefit of society at large, contributing to the collective well-being and support of broader societal goals.

Yet, solidarity support mandatory forms of data sharing when such demands stem from the pursuit of the mitigating a societal vulnerability. Although this is not outlined in the DGA, data sharing also takes mandatory forms in limited situations of general interest. The Data Act, for instance, includes provisions for public sector bodies to access private sector data during public emergencies or to fulfil legal mandates, in order to safeguard public interests.[63] One can argue that the underlying rationale of this commercial data sharing demand is solidarity with the broader public who will benefit from the use of this data. Likewise, under Article 6, the GDPR, allows for the use of personal data for the purposes of public interest.[64] Although obtaining consent is typically the primary legal foundation for data processing under the GDPR, there are instances where data can be processed without it, particularly when such processing aligns with significant public interests.[65] This includes situations where data processing is critical for humanitarian purposes, such as "monitoring epidemics and their spread or in situations of humanitarian emergencies, in particular in situations of natural and man-made disasters".[66] Thus, solidarity may support data sharing, be it may voluntary or mandatory, provided that it serves to societal interests.

Having analysed how solidarity relates to and underpins the envisaged data sharing, we will next examine how interpretations of data sharing can be influenced by adopting a solidarity-based approach. We will explore the key implications of this perspective by focusing on three areas, given the limited space available. It is worth noting that the relevance of solidarity extends beyond these areas, arguably encompassing aspects such as consent.

---

from large technological companies as data holders they capitalise on the competitive benefits of the data in the existing digital economy).

[61] Case law concerning mandatory types of solidarity is discussed in Section 4.3. In contrast, see B. Prainsack and A. Buyx, *Solidarity in Biomedicine and Beyond* (Cambridge University Press, 2017), p. 45, who adopt a narrow understanding of solidarity, limiting it to instances of voluntary support for others. The authors reserve the term for situations where there is an external expression of connection, characterized by sympathy or understanding between contributors.

[62] Articles 3(1) and 4(1), DGA.

[63] Articles 5(9), Article 6(9)(10).

[64] Article 6, GDPR.

[65] Article 6, GDPR. For the examination of these grounds, see E.S. Dove, J. Chen 'Should consent for data processing be privileged in health research? A comparative legal analysis', *International Data Privacy Law* (2022), pp. 120–31.

[66] GDPR, Recital 46.

4. Solidarity based reading of data sharing

4.1. Defining 'general interest'

The hallmark of data sharing under data altruism is its orientation towards the 'general interest'. It is described broadly rather than defined precisely. Within the framework of the EU Charter of Fundamental Rights, the 'general interest recognised by the Union' provides a legitimate foundation for actions that might otherwise be perceived as infringements of these rights.[67] For example, the general interest of the EU encompasses objectives pursued within the Common Foreign Security Area, as outlined in Article 21(2) of the TEU, including supporting democracy, the rule of law, human rights, preserve peace, prevent conflicts and strengthen international security, and the sustainable development of developing countries with the primary aim of eradicating poverty.[68] The broad application of this concept was highlighted in an early case where the transparency in the usage of European funds was recognised as a general interest.[69]

In the context of the DGA, however, the concept of 'general interest' as a new dimension. It is not solely confined to the 'general interest of the EU'; instead, it is to be defined by the Member States. Under the DGA, the determination of what constitutes the general interest rests with the Member States, who are responsible for implementing the Regulation. Data altruism organisations are required to specify the objectives of general interest they aim to support when collecting data.[70] At this point, it is useful to consider the closely related concept of 'public interest', also defined by Member States. This notion is frequently invoked within the single market to justify derogations from the economic freedoms established in EU law.[71] While not explicitly defined in EU law, 'public interest' is exemplified in various legislations.[72] Definition of public interest as "the aggregate of citizen entitlements that the state is charged to safeguard' captures the essence of this concept highlighting how public interest is inherently connected to state policies and actions at various levels.[73]

Although there is significant overlap, within the context of the DGA, the concept of general interest is arguably more expansive, covering situations that benefit the public even when not framed or pursued as public policy within a given Member State. For instance, data sharing requests for research purposes illustrate this broader interpretation. Apart from the broader interpretation aligning with the primary objective of maximising data use, textual

[67] Article 52 (1), EU Charter of Fundamental Rights.

[68] Case T-256/11 *Ezz and Others v. Council*, EU:T:2014:93, para. 199. See also, Case T-262/15 *Kisilev v. Council*, EU:T:2017:392, paras. 80-83.

[69] Joined Cases C–92/09 and C–93/09 *Volker und Markus Schecke and Eifert*, EU:C:2010:662, para. 71.

[70] Article 19)4)(h), DGA.

[71] Article 36, TFEU.

[72] For example, Directive 2006/123/EC of the European Parliament and of the Council of 12 December 2006 on services in the internal market, Article 4(8) (including public policy; public security; public safety; public health; preserving the financial equilibrium of the social security system; the protection of consumers, recipients of services and workers; fairness of trade transactions; combating fraud; the protection of the environment and the urban environment; the health of animals; intellectual property; the conservation of the national historic and artistic heritage; social policy objectives and cultural policy objectives). Examples are further elaborated in Recital 40.

[73] T. Tridimas, Wreaking the Wrongs, Balancing Rights and the Public Interest the EU Way, *Columbia Journal of European Law* (2023), p. 189.

support for this argument can be found in how the GDPR frames purpose limitations, including scientific or historical research purposes and statistical purposes separately along with public interest as legitimate grounds to process personal data.[74] In fact, the DGA lists a larger spectrum of objectives as an example, including but also going beyond public interest grounds, such as 'healthcare, combating climate change, improving mobility, facilitating the development, production and dissemination of official statistics, improving the provision of public services, public policy making or scientific research purposes'.[75] The Act reiterates these exemplary purposes also in its Recital, indicating also that technological advancement is considered as general interest, by suggesting that the Regulation is intended to foster the creation of large data pools via data altruism, which will support data analytics and machine learning throughout the Union.[76] What is worth underlining is that technologic and digital advancement is part of what the DGA considers as a general interest.

There is no doubt that the DGA intents general interest to be an inclusive and dynamic concept. Nevertheless, there is considerable discretion the Member States can exercise in deciding where its counters can be drawn. That is where solidarity could inform the interpretation of what amounts to general interest. For instance, from a more conservative perspective, general interest can be read to mean 'common' interest of the Union, whereas a more liberal reading may include data sharing that concerns particularly one Member States or a segment of a population. This is of particular importance in situations where shared data provided by one Member State serves to specific Member State and its regional benefits, rather than the EU in general. Another context, where the authorises may need to address is how distance the benefit should be. As to the term 'interest', in a strict sense, 'interest' might suggest immediate and direct benefits arising from data usage. However, a more expansive view may consider 'interest' in a flexible manner, encompassing not only indirect and long-term benefits but also those benefits that, while not quantifiable, are still identifiable. Even if the data use benefits a region of the EU rather than the EU as a whole, or liberal interpretation of general interest, emphasising collaboration and knowledge sharing that extends beyond immediate or localised benefits.

Intuitively, one might argue that solidarity always necessitates a broad understanding of general interest, with a view to ensuring that the shared data cultivation is maximised. This is arguably true in most of the cases outlined above, especially when data sharing concerns commercial data, and it promises to create substantial public value. Moreover, solidarity may require a broader interpretation when the interests are specific to one region, data sharing might not directly benefit the state where the data was made accessible by public authorities or is likely to benefit future generations rather than current population.

However, there are occasions when solidarity might necessitate a more constrained interpretation of the general interest. Consider, for instance, data sharing initiatives aimed at technological developments. While a broad reading of the term 'general' would encompass commercial interests, a stricter approach would seek to ensure that more direct societal welfare also exists. Likewise, in case of a privately commissioned research that does not serve a clear public interest. The inclusion of applied and privately funded research and technological development and data analytics in the list of general interest is problematised by the European Data Protection Board and the European Data Protection Supervisor, criticised the DGA in its

[74] Article 5(b), GDPR.

[75] Article 2(16), DGA.

[76] Recital 45, DGA.

draft form, where they emphasised this line of research and purposes are not covered allowed by the GDPR, inviting for a clearer definition which was not followed.[77] As explained the lack of clear definition is in line with the objective of data use for general interest of the society, and can accommodate the dynamic nature of the concept. The reference point can, however, be the principle of solidarity which might dictate that commercially driven initiatives be pursued only if the data processing involved is likely to result in technological progress that benefits society in a significant manner, or clearly has societal benefits, thereby anchoring data sharing practices more firmly in the societal interest. The involvement of commercial interests is not inherently negative and can lead to substantial public benefits through innovation and development of new technologies or services. A solidarity-based approach ensures that the primary focus remains on addressing pressing societal issues, thereby fostering a fairer distribution of benefits and costs derived from data resources. In cases where the definition of 'general interest' is ambiguous, solidarity provides a flexible yet coherent and value-driven approach to data sharing.

4.3. Assessing proportionate action

The increasing demands for data sharing, both on commercial and public interest grounds, are likely to create conflicts between the rights of data subjects and holders or owners and those of data users. While the legislative approach to data sharing seeks to promote data usage with the protection of individual rights, there is an inherent difficulty in aligning these goals, which may come to conflict. That raises a question of profound importance; when data protection and data sharing for general interest come into conflict, which one outweighs the other?

There is no clear hierarchy between these competing interests, and the outcome would depend on a balancing exercise. Overriding reasons can be justified when a fundamental right conflicts with a competing interest, provided they safeguard either other fundamental rights outlined in the Charter or equally significant 'general interests' recognised by the Union.[78] When the conflict is between the objective of general interest that the data sharing rests and the juxtaposing right to data protection,[79] there are a number of considerations that potentially is decisive which one prevails in *strictu sense* balancing exercise.[80] Solidarity, we contend, should

[77] EDPB and EDPS, 'EDPB-EDPS Joint Opinion 03/2021 on the Proposal for a Regulation of the European Parliament and of the Council on European Data Governance (Data Governance Act)' (2021), p. 41.

[78] Article 52, EU Charter of Fundamental Rights.

[79] Although case law regarding privacy conflicts with general interest is pertinent, the Charter of Fundamental Rights distinguishes between privacy, protected under Article 7, and data protection, covered by Article 8, which encompasses a broader substance, while data protection issues are considered under Article 8 on right to respect for private and family life. For more on this distinction, J. Kokott and C. Sobotta, 'The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR', 3 *International Data Privacy Law* (2013), p. 223.

[80] In the CJEU's proportionality assessment, the data user must first demonstrate how data sharing contributes to the achievement of the objective. A more challenging step is proving necessity, which requires showing that there is no less intrusive method to achieve the intended objective of the data sharing. Insight can be drawn from Schecke, where the Court assessed whether the full disclosure of the beneficiaries of the funds was proportionate for the attainment of the objective of transparency. At the crux of the analysis that led to the decision of disproportionate action lied the necessity of full disclosure of the personal data of all beneficiaries of EU public funds for the attainment of transparency objective, and in this sense, whether less intrusive measures were possible, such as such as publishing anonymous statistics or only disclosing data exceeding certain thresholds,

be one of them. Particularly in cases involving health protection, environmental issues, and social welfare, solidarity emerges as a key factor in achieving a balanced approach that considers both the needs and vulnerabilities of society on one hand, and those of the individual on the other.

Solidarity, as a factor in balancing, has not been used in a case concerning fundamental right in the EU jurisprudence. However, case law from the European Court of Human Rights (ECtHR) can shed light on the potential role of solidarity in achieving a balance between individual rights under the European Convention on Human Rights (ECHR) and collective interest of the society, as several rulings have highlights how solidarity influences the resolution of conflicts between these rights.[81] For instance, in *Vavřička and Others v the Czech Republic*, the ECtHR examined whether mandatory nature of preschool vaccines infringed upon applicants' rights, including the right to privacy, as protected under Article 8 of the ECHR.[82] The Court observed that the obligation to vaccinate is founded on the principle of social solidarity, aimed at safeguarding the health of all society members, especially the most vulnerable to certain diseases, noting that the wider population is expected to accept a minimal risk through vaccination for this purpose.[83] In its proportionality assessment, the Court examined the implications of mandatory vaccination from multiple angles by evaluating benefits for vulnerable populations like unvaccinated children, consequences for non-compliance including fines and preschool denial, the legality of exemptions for medical or conscientious reasons, compensation mechanisms for vaccination-related injuries, and recognized that medically exempt children's preschool attendance hinges on high vaccination rates among their peers.[84] The Court concluded that "it cannot be regarded as disproportionate for a State to require those for whom vaccination represents a remote risk to health to accept this universally practised protective measure, as a matter of legal duty and in the name of social solidarity, for the sake of the small number of vulnerable children who are unable to benefit from vaccination".[85] Thus, social solidarity weighed in to lead the Court to conclude that the mandatory vaccination scheme was not disproportionate.

The ECtHR has also considered social solidarity in its balancing exercise in another case, *Pasquinelli and Others v. San Marino*, in the balancing of competing individual interest and general interest of public at large.[86] The case involved a group of health and social workers who refused COVID-19 vaccination and consequently faced employment-related measures. The applicants contested the measures, which laid down specific provisions for the unvaccinated public sector personnel, on grounds of equality and non-discrimination, arguing

---

could satisfy the transparency needs without severely impinging on personal privacy. Joined Cases C–92/09 and C–93/09 *Volker und Markus Schecke and Eifert*, EU:C:2010:662, para. 71.

[81] Solidarity has also been increasingly incorporated into its reasoning in recent times. For examples, see. Luxembourger Constitutional Court, Judgment No. 00172 of November 25, 2022, available at: https://legilux.public.lu/eli/etat/leg/acc/2022/11/25/a605/jo; Italian Constitutional Court, Judgment No.15 of 2023, available at: https://www.cortecostituzionale.it/actionJudgment.do.

[82] ECtHR, *Vavřička and Others v the Czech Republic,* Application Nos. 47621/13 and 5 others (8 April 2021).

[83] Ibid, para 279.

[84] Ibid, paras. 292-306.

[85] Ibid, para 306.

[86] ECtHR, *Pasquinelli and Others v. San Marino*, Application No. 24622/22 (29 August 2024). For a similar case concerning the legality of measures concerning Covid-19 vaccinations, see Italian Constitutional Court, Judgment No.15 of 2023, available at: https://www.cortecostituzionale.it/actionJudgment.do, para.10.3.

that no conclusive evidence showed that vaccinated individuals could not spread the virus.[87] They also viewed the measures as an overreach of governmental power, infringing on personal rights like self-determination, right to work and health.[88] The Constitutional Court of San Marino upheld the measures, ruling them justified given the extraordinary context of a global pandemic. The ECtHR highlighted that the measures did not mandate vaccination but imposed different treatment based on vaccination status, which was appropriate given the significant public health risks. Importantly, the ECtHR framed its decision considering the concept of solidarity, emphasising that individual freedoms sometimes yield to collective health needs, especially in crucial sectors like public health. For the Court, the principle of the collective protection of health justifies temporary sacrifices by unvaccinated individuals to protect the broader community.[89] The Court asserted that the measures struck a fair balance between the right to work and public health imperatives, ultimately affirming their legality and the proportionality of the government's pandemic response. "The more *primordial* interest of public health prevailed over a temporary restriction of the right to work of single individuals who refused to get vaccinated. Indeed, every individual freedom had its limits in the duty of solidarity towards the community they lived in. This duty of solidarity was all the more relevant in the public-health sector, to which the impugned measures had been limited".[90] Solidarity weighed in as a factor that the Court considered, against the implications of the restrictions on the applicants, which the Court considered limited.

Similarly, in the admissibility decision of *De Kok v. the Netherlands*, the ECtHR emphasised the role of solidarity and 'burden-sharing' in ensuring affordable health care.[91] The applicant claimed that the legal obligation to buy healthcare violated his ECHR rights (i.e., right to privacy, freedom of thought, conscience and religion, and right to property).[92] The ECtHR observed that the compulsory basic healthcare scheme addresses "the pressing social need to ensure affordable and accessible healthcare for the population".[93] Imposing a legal duty to have basic health insurance was a burden-sharing to ensure that everyone would have access to basic healthcare, indicating a "social or collective solidarity".[94] This responsibility-sharing was not onerous for the applicant to claim an ECHR right violation because the state balanced the interests of the community with the individual's interests in protecting the ECHR rights.[95]

Although these cases do not directly address data protection, they remain highly pertinent and important in at least two distinct ways. Firstly, they demonstrate that solidarity can be a legitimate consideration in legal deliberations, where the priority has traditionally been the protection of individual rights. Secondly, and more crucially for this analysis, the discussed cases reveal that solidarity can be a significant factor in shaping the outcome of the balancing process. A data-sharing framework founded on the principle of solidarity might suggest that individuals could be expected to permit the use of their personal data for societal benefits, especially when this supports vulnerable segments of the population without imposing a

[87] Ibid, para 11.

[88] Ibid.

[89] Ibid, para. 16.

[90] Ibid, para. 18 (our emphasis).

[91] ECtHR, *De Kok v. the Netherlands,* Application No. 1443/19 (26 April 2022).

[92] Ibid, para 7.

[93] Ibid, para 13.

[94] Ibid.

[95] Ibid, para 15.

disproportionate burden on the data providers. This principle could provide a robust justification for data-sharing measures, particularly in urgent situations related to public health and environmental protection. For example, during a pandemic, sharing health data could enhance the tracking and containment of the virus and accelerate medical research, leading to the development of effective treatments that significantly benefit public health.

To clarify, we do not suggest that the principle of solidarity allows communal interests to always override individual rights, nor should it be universally applied in all instances of data-sharing conflicts between general and individual interests. As previously mentioned, the principle of solidarity is nuanced. Although it is frequently employed to address functional necessities within the EU, it also embodies a value-based dimension, which is particularly relevant in the context of societal needs. In situations where the broader societal interest clashes with individual interests, solidarity should be applied selectively to support vulnerable beneficiaries, rather than to merely further public benefits associated with data sharing. For instance, while technological advancements are often considered in the general interest and can benefit society, not all such advancements address societal vulnerabilities. Solidarity, seen as a value-based principle, is essential for providing guidance by linking public interest considerations to societal vulnerabilities. This approach stands in contrast to those driven solely by functional or economic objectives, which might offer substantial societal benefits but overlook direct vulnerabilities, particularly prevalent in technological innovations. This nuanced application of solidarity is both necessary and justified when the conflicting interests involve fundamental rights.

4.3. Harm mitigation

Despite concerted efforts to prevent data infringements, the use of data may still lead to detrimental consequences for the data subject or owner. Although such harm is often associated with the commercial exploitation of data,[96] both commercial and public uses hold the potential to cause significant damage.[97] The Data Governance Act (DGA) acknowledges this risk, recognizing that the actions of data intermediation service providers or data altruism organizations may result in harm. Accordingly, it requires Member States to impose penalties designed to deter such infringements.[98] However, the DGA falls short of mandating that Member States implement measures aimed at mitigating the harm resulting from violations of the regulation, such as unauthorized data use arising from misleading or insufficient information provided prior to obtaining consent. The DGA also leaves unresolved the issue of situations where harm arises even when data sharing is conducted on a legitimate legal basis. Damage may occur even when data is shared lawfully, such as through consent granted under the data altruism scheme. While the DGA provides that data subjects and owners participating in such a scheme may be compensated for costs incurred when making their personal data available for objectives of general interest, there remain instances where the responsibility placed upon the individual may become heavy.

[96] For examples of such damages, see M. S. McCoy et al., 'Ethical responsibilities for companies that process personal data' 23 *The American Journal of Bioethics* (2023), p. 12.

[97] For examples, see R. Peeters and A. C. Widlak, 'Administrative exclusion in the infrastructure-level bureaucracy: The case of the Dutch daycare benefit scandal', 83 *Public Administration Review* (2023), p. 863 ; R. Richardson, J. M. Schultz, and K. Crawford, 'Dirty data, bad predictions: How civil rights violations impact police data, predictive policing systems, and justice' *NYU Law Review* (2019), pp. 21-40.

[98] Article 34(2)(b), DGA.

Solidarity calls for a comprehensive framework to address and remedy harms arising from data sharing. Such harms may not only stem from regulatory infringements but also from the lawful use of data, including data altruism, if it results in detriment to the contributor. In instances where data is utilised for public interest purposes, such as scientific research, the principle of solidarity demands and reinforces the necessity of providing effective remedies for any damages incurred.

An example of the flip-side of the coin—that is, solidarity towards the individual—being effectively implemented can be found in constitutional jurisprudence. A notable instance is the mandatory vaccination scheme, which significantly stirs debate over its constitutional validity, particularly the imposition of such obligations to protect public health under the protection of constitutional freedoms. When the constitutionality of mandatory childhood vaccinations was challenged, the Constitutional Court of Slovenia affirmed the state's mandate to enforce vaccinations to ensure public health and collective immunity against infectious diseases.[99] Nonetheless, the Court declared the legislative act unconstitutional for not clearly defining the procedures and rights related to medical exemptions from mandatory vaccinations. The Court emphasised that the principle of solidarity, which supports the state's vaccination mandates enacted for public welfare, also necessitates the compensation for individuals adversely affected by these measures.[100]

5. Concluding remarks

Despite its significant potential to shape a nascent and complex legal framework where data sharing is a primary objective, it is surprising that the principle of solidarity is not explicitly employed within the legislative framing of data sharing. While not all data sharing is driven by solidarity, there is a strong rationale for using data to serve the general interest of society, whether in health innovation or technological advancement. This article argues that the principle of solidarity can help clarify the vague concept of 'general interest'. By promoting a broad understanding that extends beyond immediate or localised benefits, it ensures that the purpose of data sharing is anchored in contributing to societal causes, tackling vulnerabilities, and improving the well-being of others. Solidarity can inform the balance between individual and societal interests, often compelling a greater emphasis on collective benefits over individual rights, especially when societal needs are pressing and potential benefits are substantial. However, solidarity is not always at odds with individual interests. In cases of harm, solidarity equally serves to address vulnerabilities and demand effective harm mitigation. Integrating solidarity into this dialogue can promote a value-oriented approach to the EU's data governance, particularly in data sharing. It promises a fairer distribution of risks and benefits in managing the increasingly conflicting interests of data protection and data sharing for the common good.

In this article, we examined from a legal perspective how solidarity influences and informs data governance in general, and data sharing in particular. An area we have not explored, but that merits attention, is how data sharing might in turn shape and influence solidarity as a legal principle. Data altruism provides the EU with a strategic opportunity to foster solidarity among its citizens, moving beyond traditional inter-state approaches. Data governance provides a framework where relationships can flourish, not only between Member

[99] Constitutional Court of Slovenia, SI:USRS:2004:U.I.127.01, 12 February 2004, para.27. available at: https://www.us-rs.si/decisions/?lang=en.

[100] Ibid, para 27.

States driven by legal obligations but also among individuals. Altruistic data sharing goes beyond merely demonstrating data owners' willingness to support fellow EU citizens; it also embodies the foundational trust in these relationships. This approach potentially shifts the focus from sacrificing short-term interests to long-term communal benefits and broadens the scope of solidarity by surpassing traditional interstate or interpersonal dynamics. Given the modest effectiveness of judicial initiatives in promoting social solidarity and the resistance to fulfilling obligations under EU responsibility-sharing schemes, this innovative method could offer an ideal environment to strengthen and expand the social foundations of solidarity. Such a paradigm shift could foster deeper, value-driven solidarity among individuals, aligning with the EU's vison of becoming a community rooted in shared values.