Owusu A, 'Data sharing in the personal data economy. Does sharing mean caring?' (2023) 2 EJPLT, 217 - 239.
DOI: https://doi.org/10.57230/EJPLT223AO

EJPLT
ISSN 2704-8012



# Data sharing in the personal data economy. Does sharing mean caring?

## *La condivisione dei dati nell'economia dei dati personali. Condividere vuol dire prendersi cura?*

ABIGAIL OWUSU
Postdoctoral Research Fellow
University of Verona
Lawyer

Abstract

Following its approval by the European Parliament in April 2022, the Data Governance Act (DGA) introduces regulation for the providers of data intermediation services. The Regulation seeks to empower data subjects and ensure the competitiveness of the markets in which data intermediaries operate. After providing the necessary background, this paper aims at offering a first general overview, from a private law standpoint, on both merits and limitations of the regulatory approach on data sharing adopted by the DGA. It outlines questions that need to be addressed in order to verify that the Regulation delivers the benefits it promises.

*In seguito alla sua approvazione, nell'aprile 2022, da parte del Parlamento europeo, il Data Governance Act (DGA) ha introdotto una normativa rivolta ai fornitori di servizi di intermediazione dei dati. Il regolamento mira a garantire agli interessati maggior controllo sui propri dati, nonché la competitività dei mercati in cui operano gli intermediari di dati. Il presente saggio, svolte alcune doverose premesse, intende offrire una prima panoramica generale sui pregi e sui limiti dell'approccio normativo, adottato dal DGA, al tema della condivisione dei dati, dal punto di vista del diritto privato. Lo scritto individua le questioni che devono essere affrontate al fine di verificare se il regolamento è realmente idoneo a perseguire i benefici promessi.*

© The author(s) 2023, published by Suor Orsola Benincasa Università Editrice. This contribution is licensed under a Creative Common Attribution 4.0 International Licence CC-BY-NC-ND, all the details on the license are available at: https://creativecommons.org/licenses/by-nc-nd/4.0/

Keywords: Data protection; Personal data; Non-personal data; Data sharing; Data intermediation services; Data Intermediaries; Commodification of personal data; Fundamental human rights.

Summary: Introduction. – 1. The background of the Regulation and the European Data Strategy. – 2. Types of data intermediaries. – 3. The DGA framework: subject matter, scope of application and definitions. – 4. Conditions for providing data intermediation services. – 5. The enforcement mechanism. – 6. Risks of data sharing and the limits of the DGA. – Conclusions

## Introduction.

Access to big data plays a crucial role for societal development. The availability of vast datasets enables data analysts to make accurate predictions in different business sectors, such as marketing and finance, tackling major challenges. Access to data is also extremely important in the context of Artificial Intelligence, since machine learning cannot take place without the availability of a large amount of data. Having access to data is a powerful tool to gain business advantage over competitors.

The question on how the governance of this data should be designed i.e. who has control over this data, who can use it, and who can benefit from its value is a key policy question for the development of the European data economy. It does not come as a surprise that data regulation in general and the debate on access to and ownership of data, in particular, have become the most visible regulatory discussions in recent EU regulatory policies.

This paper presents the result of a legal analysis of the European Commission's Data Governance Act (DGA), which entered into force on June 23, 2022, and is applicable since September 24, 2023, with respect to the provision of «data intermediation services».

According to the new Regulation, data intermediaries are expected to facilitate data sharing within the EU, by that means increasing the amount of data available to European businesses for their activities. On the other hand, due to the central role within the European data economy that data intermediaries, as two-sided platforms, will occupy, the EU legislator is aware of the risks for users and competition at large. In this perspective, the DGA is aimed both at establishing trust in data intermediaries, thereby strengthening their role, and, simultaneously, at pre-emptively limiting potential abuses.

The reactions of academics and stakeholders to the DGA are very ambivalent. Although many are welcoming the objectives and the basic approach of the DGA, there is an increasing awareness that the new Regulation also entails a lot of challenging problems. In addition to many unclear provisions and concerns about costs of compliance, open questions about the risks of the commodification of personal data, and the dangers of new forms of data concentration and data power have been raised.

Furthermore, crucial questions on its relationship with data protection law and the necessity of such a far-reaching horizontal regulation have emerged in

this discussion.

This paper intends to contribute to this debate by providing a preliminary analysis of the effects of the provisions in the DGA with respect to its objectives. This entails, in particular, an analysis of the ex-ante obligations imposed on data intermediation services, and whether they can be expected to be sufficiently effective for achieving its objectives. However, it also requires a broader critical analysis of the effects of the specific model of data governance envisaged in the DGA, which should enable all data holders and users to participate in the economic value created by intermediation services.

The paper is structured as follows: Section I will present some background on the governance problems of data, and on how the European Data Strategy was conceived. Section II describes different data sharing models and the corresponding market developments in the absence of specific regulation. Against this background, the subsequent sections of the paper focus on the architecture of the DGA, illustrating the subject matter, its scope of application, definitions, enforcement mechanisms, and, most importantly, the ex-ante obligations imposed on data intermediation services. Section VI discusses the risks of data sharing and the limits of the DGA. The last section draws some conclusions.

## 1. The background of the Regulation and the European Data Strategy.

In recent years, data-driven technologies have had transformative effects on all sectors of the economy.

The proliferation of products connected to the Internet of Things in particular has increased the volume and potential value of data for consumers, businesses, and society.

The ability to store, arrange, and analyze data in order to gain insights is what gives data its enormous financial value.[1]

Data markets consist of three main links along the data value chain: collection, synthesis and analysis, and use.[2]

The collection of data relates to the recording, aggregation, and organization of information into a form that can be used for data mining.[3]

Synthesis and analysis relate to the integration of different types of data and the analytical processing of data in order to find correlations.[4]

[1] OECD, Data-Driven innovation: Big data for growth and well-being (2015) 150, https://www.oecdilibrary.org/science-and-technology/data-driven innovation_9789264229358-en.

[2] N Elkin-Koren, MS Gal, The Chilling Effect of Governance-by-Data on Data Markets, (2019) 86(2) The University of Chicago Law Review, 410, https://chicagounbound.uchicago.edu/uclrev/vol86/iss2/6.

[3] See KJ Strandburg, 'Monitoring, Datafication, and Consent: Legal Approaches to Privacy in the Big Data Context', in J Lane (ed.), *Privacy, Big Data, and the Public Good: Frameworks for Engagement* (Cambridge, 2014), 5, 10 ff.

[4] Elkin-Koren, Gal, 'The Chilling Effect of Governance-by-Data' 410.

The last link, use, involves utilizing data-based information to improve decision-making in order to innovate[5] or to increase productivity.[6] For example, personal data can be used to create a digital profile for each individual, which could then be used to improve personalized products and services or for microtargeted advertising.[7]

What sets data apart from other resources is their re-usability: the great value of data lies in their nature as non-rivalrous goods. Multiple businesses can use the same data simultaneously or subsequently for their individual purposes without its value diminishing.[8]

Data are also considered multi-purpose inputs, i.e. useable for a multitude of different purposes, many of which cannot be anticipated a priori.[9]

Because of the economic and societal value of data, the European Commission issued a communication called «A European strategy for data» in 2020, announcing the «aim to create a single European data space – a genuine single market for data, open to data from across the world – where personal as well as non-personal data, including sensitive business data, are secure and businesses also have easy access to an almost infinite amount of high-quality industrial data, boosting growth and creating value, while minimising the human carbon and environmental footprint».[10]

Stimulating the use of data in various sectors of the economy is key to creating the EU data economy.[11] Currently, the use and sharing of data is negatively influenced by several factors such as the insufficient availability of data, imbalances in market power, insufficient governance structures and technical infrastructures, or the lack of adequate tools that would empower consumers to make use of their rights that rely upon the sharing of data (i.e., data portability rights).[12]

The initiatives that have fostered the development of the European data economy are the Regulation (EU) 2022/868 on European data governance (Data Governance Act),[13] the Regulation (EU) 2022/1925 on contestable and fair markets in the digital sector (Digital Markets Act),[14] and the Regulation

[5] T Niebel, F Rasel, S Viete, 'BIG data – BIG gains? Understanding the link between big data analytics and innovation' (2019) 28(3) Economics of Innovation and New Technology, 296 ff. https://doi.org/10.1080/10438599.2018.1493075.

[6] E Brynjolfsson, W Jin, K McElheran, 'The power of prediction: Predictive analytics, workplace complements, and business performance' (2021) 56(4) Business Economics, 217 ff., https://doi.org/10.1057/s11369-021-00224-5.

[7] See S Zuboff, 'Big Other: Surveillance Capitalism and the Prospects of an Information Civilization' (2015) 30 Journal of Information Technology, 78-79.

[8] OECD, Data-Driven innovation: Big data for growth and well-being, 179; see also B Custers, D Bachlechner, 'Advancing the EU data economy: Conditions for realizing the full potential of data reuse' (2017) 3-4, https://ssrn.com/abstract=3091038.

[9] OECD, Data-Driven innovation: Big data for growth and well-being, 181.

[10] European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions 'A European strategy for data' [COM(2020)86 final].

[11] European Commission, A European strategy for data, 1-2.

[12] ibid 6 ff.

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

[14] 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 (Digital Markets Act).

(EU) 2022/1925 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act).[15]

The Data Governance Act, which will be applicable as of September 24, 2023, is the first legislative instrument announced in the European Data Strategy to come into force. The DGA aims to facilitate the re-use and sharing of data in and between the private and public sectors.

The apex of the European Commission's regulatory initiatives for the data economy is the Proposal for a Regulation on harmonised rules on fair access to and use of data (Data Act) [COM/2022/68 final] published on February 23, 2022.[16] The Data Act (DA) is another building stone for a regulatory framework to support data access and its re-use in view of consolidating a European data space that guarantees a high level of data protection.

## 2. Types of data intermediaries.

At various stages of the data life cycle, it has become increasingly common for businesses to rely upon third-party services. More precisely, data intermediaries have emerged as a new type of third-party services addressing the sharing of data between consumers and businesses (C2B) as well as between businesses themselves (B2B).

The two most important types of B2B data intermediaries potentially covered by the DGA are data marketplaces and industrial data platforms.[17]

Data marketplaces correspond to the classic model of a two-sided matching platform: on data marketplaces, data holders can offer their data to potential data users, while users can search different data offerings to find the purpose-specific data they need.[18]

Data marketplaces are in principle open and therefore target a wide and unknown range of participants.[19]

---

[15] 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 (Digital Services Act).

[16] European Commission, Proposal for a Regulation of The European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act) [COM/2022/68 final], Bruxelles, 23.2.2022. On November 9, 2023, the European Parliament has adopted the final version of the Data Act. The Act is now subject to formal approval by the Council and once adopted, will enter into force 20 days after Official Journal publication, becoming applicable after 20 months.
On the Data Act proposal, see Fernandez, 'The Data Act: the next step in moving forward to a European Data Space' (2022) 8(1) European Data Protection Law Review, 108-114; Gallese, 'A first commentary to the proposal for a new Regulation on fair access and use of data (Data Act) (2022) 3 Media Laws, 237-270; Leistner, Antoine, 'Attention, here comes the EU Data Act! A critical in-depth analysis of the Commission's 2022 Proposal' (2022) 13(3) Journal of Intellectual Property, Information Technology and Electronic Commerce Law, 339-349; Kerber, 'Governance of IoT Data: why the EU Data Act will not fulfill its objectives' (2023) 72(2) GRUR International, 120-135.

[17] European Commission, Commission Staff Working Document on the free flow of data and emerging issues of the European data economy, Accompanying the document Building a European data economy. Commission, Free flow of data. SWD/2017/2 final, 17.

[18] See P Koutroumpis and others, 'Markets for data' (2020) 29(3) Industrial and Corporate Change, 647, https://doi.org/10.1093/icc/dtaa002. Dawex (https://www.dawex.com/en/) is an example of a platform for matching supply and demand for individual data. Its services are essentially limited to finding the right buyer for a company that wants to monetize data it holds.

[19] L von Ditfurth, G Lienemann, 'The Data Governance Act: – Promoting or Restricting Data Intermediaries?' (2022) 23(4) Competition and Regulation in Network Industries, 274, https://doi.org/10.1177/17835917221141324; H Richter, PR Slowinski, 'The data sharing economy: On

In addition, data marketplaces may become much more than a mere enabler for data sharing, should it offer additional services like anonymization and adjust the data to specific business needs of the companies.[20]

The other important type of data intermediaries falling within the scope of the DGA are so-called industrial data platforms. [21] Unlike with data marketplaces, the main purpose of industrial data platforms is to provide the technical infrastructure for companies to share data with each other as part of their broader collaboration.[22] It is also common to speak of "data pooling": participants enter certain data into the data pool and in return receive access to the data fed into the pool by the other participants, thereby increasing the amount of data available for all of the participants.[23]

Furthermore, data spaces serve as the fast and secure infrastructure for individual data exchanges among their users.[24]

Industrial data platforms can be open or closed. In the case of open platforms, participation is open to all companies that meet certain criteria. Closed platforms, on the other hand, restrict participation to certain cooperating firms.[25]

Somewhere in between entirely "open" and "closed" platforms are those which allow sharing between specific companies, while the "data sharing club" is open to new entrants if they fulfill certain requirements.[26]

Other forms of B2B-data intermediaries are data cooperatives and data brokers.

Data cooperatives store and aggregate data for their users – typically small businesses from specific sectors – and enable them to manage their data in a self-determined and informed manner.[27]

Data brokers are the most established and commercially successful type of data intermediary as they collect and aggregate data from a wide range of sources (including businesses) and then sell the aggregated data to third parties.[28]

The most common type of C2B data intermediaries are Personal Information Management Services (PIMS).

---

the emergence of new intermediaries' (2019) 50(1) International Review of Intellectual Property and Competition Law, 12, https://doi.org/10.1007/s40319-018-00777-7.

[20] Richter, Slowinski, 'The data sharing economy' 12.

[21] European Commission, Document on the free flow of data, 18.

[22] European Commission, Study on data sharing between companies in Europe (2018) 62, https://op.europa.eu/de/publication-detail/-/publication/8b8776ff-4834-11e8-be1d-01aa75ed71a1/language-en.

[23] A Wernick, C Olk, and M Grafenstein, 'Defining data intermediaries. A Clearer View through the Lens of Intellectual Property Governance' (2020) 2 Technology and Regulation, 74, https://doi.org/10.26116/techreg.2020.007.

[24] European Commission, Study on data sharing, 62.

[25] L von Ditfurth, G Lienemann, 'The Data Governance Act' 275.

[26] H Richter, PR Slowinski, 'The data sharing economy' 12. An interesting example of this type of platform is iShare (https://hollandfintech.com) which enables everyone in the logistics sector to share information with all participants.

[27] M Jouanjean and others, 'Issues around data governance in the digital transformation of agriculture: The farmers' perspective', in *OECD Food, Agriculture and Fisheries Papers* 146 (OECD Publishing, 2020) 15 ff., https://doi.org/10.1787/53ecf2ab-en.

[28] OECD, Enhancing Access to and sharing of data: Reconciling risks and benefits for data Re-use across societies (2019) 37, https://www.oecd-ilibrary.org/science-and-technology/enhancing-access-to-andsharing-of-data_276aaca8-en.

PIMS are intermediaries in the sense that they endeavor to connect to different ends of the markets by obtaining a commitment from data-generating companies to provide a "data handback" (i.e., a copy of the personal data) to consumers, so that the data can be stored, managed and shared with third parties through the PIMS ecosystem.[29]

In addition to providing secure spaces for the collation of personal information, PIMS increasingly provide additional functionalities such as profiling, automatic form completion, certification/verification services, a central digital letterbox for sharing information with, and receiving data from, controls to help consumers manage and filter what information they share, and to create personal profiles that they can share and use to make more informed decisions across the web.[30]

An early example of PIMS is a program called "Lumeria": a customer will store personal data in a SuperProfile. The more specific the information stored (about such things as age, sex, family status, etc.), the more valuable that profile will become to advertisers, who will pay handsomely to participate in Lumeria's network. In exchange Lumeria will give them the chance to do highly targeted, permission-based marketing to offer special deals on services to people of a predetermined demographic profile. Most of the money will go directly to Lumeria's users and Lumeria will take a small cut.[31]

Similarly, the Weople app, which is operated by an Italian company called Hoda srl, encourages web users to link third-party accounts (such as Gmail and other Google accounts) to port their personal data into a "digital vault" — where their data will be «masked and anonymized» so that it can be used to target them with personalized offers.[32] Weople users are able to generate virtual currency or other rewards and potentially earn actual money, in exchange for authorizing the use of their "masked" data for marketing purposes. The app also aggregates anonymized user data into blocks to trade with marketers.

PIMS are advertised as empowering individuals to obtain value from their personal data by selling or providing access to their personal data to data buyers.

From a data protection perspective, PIMS can serve as a means to declare consent and invoke the rights of access, erasure, rectification and portability on behalf of data subject.[33]

---

[29] N Zingales, 'The Rise of 'Infomediaries' and Its Implications for Antitrust' (ASCOLA, 2017) 21.
[30] ibid 21-22.
[31] T Lester, 'The Reinvention of Privacy' 2001 Atlantic Monthly 287(3), 36.
[32] Cf. weople.space/en/#functions. There have been concerns over Weople's approach of leveraging GDPR data portability rights to grease the commercial tradability of personal data.
Back in 2019, the app was referred to the European Data Protection Board (EDPB) by the Italian data protection authority (Garante per la Protezione dei Dati Personali), for an opinion on its approach to utilizing the GDPR's data subject portability rights to make money (Garante per la protezione dei dati personali, Dati in cambio di soldi: il Garante privacy porta la questione in Europa. Sotto la lente dell'Autorità la app "Weople", 1 August 2019, https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9126709). Later, the EDPB sent a letter to Weople, stating that the «request for an opinion […] was withdrawn by the Italian Supervisory Authority, and therefore the EDPB is no longer drafting such an opinion» (EDPB Secretariat, Response to Hoda letter, 21 January 2020, https://edpb.europa.eu/sites/default/files/files/file1/edpb_responsetohodaletter_final_0.pdf).
[33] von Ditfurth, Lienemann, 'The Data Governance Act' 275-276.

## 3. The DGA framework: subject matter, scope of application and definitions.

As mentioned in the previous sections, data intermediation services play a key role in the data economy, in particular in supporting and promoting voluntary data sharing practices between businesses. In the view of the EU legislator, «data intermediation services providers, which may include public sector bodies, that offer services that connect the different actors have the potential to contribute to the efficient pooling of data as well as to the facilitation of bilateral data sharing. Specialised data intermediation services that are independent from data subjects, data holders and data users could have a facilitating role in the emergence of new data-driven ecosystems independent from any player with a significant degree of market power, while allowing non-discriminatory access to the data economy for undertakings of all sizes, in particular SMEs and start-ups with limited financial, legal or administrative means. This will be particularly important in the context of the establishment of common European data spaces, namely purpose or sector-specific or cross-sectoral interoperable frameworks of common standards and practices to share or jointly process data for, inter alia, the development of new products and services, scientific research or civil society initiatives».[34]

On this premise, the DGA aim «to improve the conditions for data sharing in the internal market, by creating a harmonised framework for data exchanges and laying down certain basic requirements for data governance, paying specific attention to facilitating cooperation between Member States»,[35] with the ultimate goal of further developing «the borderless digital internal market and a human-centric, trustworthy and secure data society and economy».[36]

In addition to regulating data intermediaries (Arts. 10 – 15), the DGA also addresses the re-use of data held by the public sector (Arts. 3 – 9), and it further contains special rules for organizations that require and use personal data for altruistic purposes (Arts. 16 – 25).

This paper exclusively focuses on the regulation of data intermediation services: its goals, its enforcement mechanisms and, most importantly, its conditions for providing data intermediation services.

The main activity regulated by the DGA, i.e. data sharing, is defined as «the provision of data by a data subject or a data holder to a data user for the purpose of the joint or individual use of such data, based on voluntary agreements or Union or national law, directly or through an intermediary, for example under open or commercial licences subject to a fee or free of charge».[37]

Other than the data subject as referred to in Art. 4 (1) GDPR, two are the new subjects to whom the Regulation is addressed: the «data holder» and the «data user».

The data holder is the «legal person, including public sector bodies and international organisations, or a natural person who is not a data subject with respect to the specific data in question, which, in accordance with applicable

[34] Cf. Recital 27 DGA.
[35] Cf. Recital 3 DGA.
[36] ibid.
[37] Art. 2 (10) DGA

Union or national law, has the right to grant access to or to share certain personal data or non-personal data».[38]

Data user means «a natural or legal person who has lawful access to certain personal or non-personal data and has the right, including under Regulation (EU) 2016/679 in the case of personal data, to use that data for commercial or non- commercial purposes».[39]

In their joint opinion on the DGA proposal, the European Data Protection Board (EDPB) and the European Data Protection Supervisor (EDPS) shared their concerns on the existing tension between data protection principles and data sharing.[40] In this joint opinion the two authorities highlighted a number of inconsistencies between the GDPR and the DGA proposal.

As far as the terminology is concerned, the joint opinion noted the confusion and incompatibility between the notion of «data holder» under the DGA proposal and that of «data subject» in the GDPR, and between the notion of «data user» under the DGA proposal and that of a «data controller» under the GDPR: in both these cases, there could be conflicts between the rights and prerogatives derived from these partially overlapping concepts.[41]

The joint opinion concluded that the DGA proposal «does not duly take into account the need to ensure and guarantee the level of protection of personal data provided under EU law»,[42] and therefore «raises serious concerns from a fundamental rights viewpoint».[43]

The above-mentioned concerns where endorsed by some academics.[44]

Although the transition between the November 2020 version of the DGA proposal and the subsequently dismissed version show a rethinking of the new language adopted, by maintaining alongside the «data holder» and the «data user» the notion of «data subject» as referred to in Art. 4 (1) GDPR), the EU regulatory evolution toward the commodification of personal data is undeniable. As it will be further discussed, the new trend is confirmed, among other things, by the reference to the possibility of data recovery in the event of insolvency of the data intermediation services provider (Art. 12 (h) DGA).

By affirming that the «data holder» has the right to grant access to or to share certain personal data or non-personal data in favor of «data users» the DGA also emphasizes another legal status, i.e. those of «data users», who have their own individual legal position, which can be qualified in various ways, depending on how the processing of data takes place, and are, therefore, difficult to define a priori.[45] The reference to the GDPR indicates cases where the «data user» already has, as the «data controller», autonomous legal

[38] Art. 2 (8) DGA.
[39] Art. 2 (9) DGA.
[40] 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), 8 ff., https://edps.europa.eu/data-protection/our-work/publications/edps-edpb-joint-opinions/edpb-edps-joint-opinion-proposal_en.
[41] EDPB and EDPS, EDPB-EDPS Joint Opinion 03/2021, 9 ff.
[42] EDPB and EDPS, EDPB-EDPS Joint Opinion 03/2021, 7.
[43] ibid.
[44] See F Bravo, 'Intermediazione di dati personali e servizi di data sharing dal GDPR al Data Governance Act' (2021) 1 Contratto e impresa Europa, 239 ff.
[45] ibid. 241.

situations over such data, by virtue of the legal bases set forth in Articles 6(1) and 9(2) GDPR.[46]

The user's rights to access and use data generated by IoT devices and to share such data with third parties are expressly regulated by the Data Act[47].

Art. 2 (11) DGA, defines the data intermediation service as «a service which aims to establish commercial relationships for the purposes of data sharing between an undetermined number of data subjects and data holders on the one hand and data users on the other, through technical, legal or other means (…)».

In order to be classified as a provider of data intermediation services, it is not sufficient to merely provide the technical tools for data sharing without the aim to establish or gather information on commercial relationships between data holders and users.[48]

The DGA identifies three types of data intermediation services.

The first category includes «intermediation services between data holders and potential data users, including making available the technical or other means to enable such services; those services may include bilateral or multilateral exchanges of data or the creation of platforms or databases enabling the exchange or joint use of data, as well as the establishment of other specific infrastructure for the interconnection of data holders with data users».

Data marketplaces are typically covered by the definition of Art. 2 (11) DGA.[49]

Open industrial data platforms may fall within the scope of application of Art. 2 (11) DGA, if they assist in the establishment of commercial relationships and do not merely assist with the technical aspects of data sharing.[50]

Data intermediaries that do not establish direct relations between data holders and data users – which prominently includes data brokers[51] – are excluded from the scope of application of the DGA.

It is surprising that the DGA does not apply to the most established and commercially successful type of data intermediary.

Furthermore, it is necessary for a data intermediary to aim at establishing relations between an undetermined number of data holders and users.

---

[46] F Bravo, '«Destinatario» dell'informazione e trattamento dei dati personali nell'evoluzione dell'ordinamento europeo', in M D'Auria (ed.), I problemi dell' informazione nel diritto civile, oggi studi in onore di Vincenzo Cuffaro (Roma TrE-Press, 2022), 454.

[47] Art. 4 (1) DA « Where data cannot be directly accessed by the user from the connected product or related service, data holders shall make readily available data, as well as the relevant metadata necessary to interpret and use those data, accessible to the user without undue delay, of the same quality as is available to the data holder, easily, securely, free of charge, in a comprehensive, structured, commonly used and machine-readable format and, where relevant and technically feasible, continuously and in real-time. This shall be done on the basis of a simple request through electronic means where technically feasible».
Art. 5 (1) DA « Upon request by a user, or by a party acting on behalf of a user, the data holder shall make available readily available data, as well as the relevant metadata necessary to interpret and use those data, to a third party without undue delay, of the same quality as is available to the data holder, easily, securely, free of charge to the user, in a comprehensive, structured, commonly used and machine-readable format and, where relevant and technically feasible, continuously and in real-time. The data shall be made available by the data holder to the third party in accordance with Articles 8 and 9».

[48] Cf. Recital 28 DGA.

[49] ibid.

[50] von Ditfurth, Lienemann, 'The Data Governance Act' 280.

[51] Ibid.

Therefore, the DGA does not cover closed services which are only available to a single data holder or to a pre-selected group of businesses.[52]

According to Art. 10 (a) DGA, providers of technical or other means for enabling data intermediation services are themselves considered data intermediaries under the DGA. Nevertheless, pursuant to Recital 28 DGA, such providers only fall within the scope of the regulation if the provision of such tools is either aimed at establishing a commercial relationship or allows them to acquire information on the establishment of commercial relationships.

Ordinary cloud services, data sharing software, web browsers or email services are not covered by the Regulation.[53]

Art. 10 (b) explicitly addresses C2B intermediaries which provide «intermediation services between data subjects that seek to make their personal data available or natural persons that seek to make non-personal data available, and potential data users, including making available the technical or other means to enable such services, and in particular enabling the exercise of the data subjects' rights provided in Regulation (EU) 2016/679».

This category includes PIMS and related services.

Such data intermediation services providers assist data subjects in exercising their rights under the GDPR, in particular giving and withdrawing their consent to data processing, the right of access to their own data, the right to the rectification of inaccurate personal data, the right of erasure or right "to be forgotten", the right to restrict processing and the right to data portability. In this regard, the DGA deems crucial that the business model of such providers ensures that there are no misaligned incentives that encourage data subjects to use such services to make more data relating to them available for processing than would be in their interest.[54]

The language of the provision is reminiscent of art. 80 GDPR which facilitates the defence of the rights of data subjects by accepting mandates for non-profit organisations.[55]

Data subjects, by law, can now give a power of attorney [56] to data intermediation services providers, which acts in force of a contract of mandate.

This provision is introduced for legal systems that do not have an existing discipline regarding mandate, and, in legal systems where this contract already exists,[57] to force by law data intermediation services providers to promptly comply with that mandate.

Thanks to this new provision, the possibility to use a mandate and the obligation to comply are clearly laid out by law.

Lastly, Art. 10 (c) DGA includes data intermediation services provided by data cooperatives (as defined in Art. 2 (15) DGA) into the scope of application of the Regulation.

According to Recital 31 DGA, data cooperatives seek to influence the terms and conditions of data user organisations attached to data use in a manner that

[52] Cf. Art. 2 (11) (c) and Recital 28 DGA.
[53] Cf. Recital 28 DGA.
[54] Cf. Recital 30 DGA.
[55] R Kulms, 'Data sharing and data protection' (2022) 1 Romanian Review of Private Law, 140.
[56] Understood as the unilateral act by which one person empowers another to represent him/her/them.
[57] E.g. Art. 1703 of the Italian Civil Code: «The mandate is the contract by which one party commits to perform one or more legal acts on behalf of the other».

gives better choices to the individual members of the group or potentially finding solutions to conflicting positions of individual members of a group on how data can be used where such data relates to several data subjects within that group, thus strengthening the position of individuals in making informed choices before consenting to data use.

Data cooperatives could also be useful for one-person undertakings and SMEs which, in terms of knowledge of data sharing, are often comparable to individuals.

Art. 2 (11) (b) and (d) DGA set out further exceptions to the applicability of the DGA: lett. (b) exempts intermediaries that focus on the intermediation of copyright-protected content, while lett. (d) applies to public-sector bodies that do not seek to establish commercial relationships.[58]

Finally, Art. 15 DGA deems its regime non-applicable to recognised data altruism organisations which do not establish commercial relationships.

Despite the definition regarding the concept of data intermediation the role of data intermediation services providers remains ambiguous: shaped as entities capable of securing the rights of data subjects in the technological context, they could instead end up enhancing the profitability of personal data encouraging its use for commercial purposes.[59] As it will be further discussed in section VI, this could lead to the reduction of the level of protection of personal data provided under EU law, implicating the debasement of fundamental rights.

### 4. Conditions for providing data intermediation services.

Art. 12 DGA imposes 15 conditions on data intermediation services.

Most obligations aim at protecting fair competition and ensuring a high level of security for users' data.

Art. 12 (a) DGA requires data intermediaries to refrain from using the data for which they provide data intermediation services for purposes other than to put them at the disposal of data users.

Providers of data intermediation services are prohibited from analysing and using the data shared by data holders for their own (or any other) purposes.[60]

Art. 12 (a) is further supplemented by Art. 12 (c) DGA, which prohibits the use of certain kinds of meta-data for other purposes than improving intermediation services.

Art. 12 (a) and (c) DGA by prohibiting providers of data information services to use both the data obtained from their users and the data collected by themselves to their users' disadvantage is aimed at avoiding conflicts of interest.[61]

The requirement of neutrality addresses concerns about vertically integrated platforms having a dual role by simultaneously acting as

[58] Cf. Recital 29 DGA.
[59] D Poletti, 'Gli intermediari dei dati' (2022) 1 European Journal of Privacy Law & Technologies, 53, https://doi.org/10.57230/EJPLT221DP.
[60] Cf. Recital 33 DGA.
[61] von Ditfurth, Lienemann, "The Data Governance Act' 283.

intermediary between businesses and users as well as competing with those businesses in offering their own services. An example is an undertaking that at the same time provides a marketplace where independent businesses can sell products to consumers and sells products as a retailer on the same marketplace in competition with the independent businesses. Such situations provide room for practices of self-preferencing, whereby a platform treats its own services more favourably than those of rivals.[62]

As mentioned, services providers may not use the data for other purposes than putting them at the disposal of their users. This implies that data intermediaries are generally not allowed to offer any additional data-related services to their users.

However, under Art. 12 (e) DGA data intermediaries may offer data-related services whose purpose it is to facilitate the exchange of data. For instance, data intermediation service providers can assist their users with the anonymisation of data.[63]

To make sure that data for which intermediation services are provided is not used for other purposes, Art. 12 (a) DGA imposes a requirement for the structural separation of data intermediation services from other units of the same company («the data intermediation services provider […] shall provide data intermediation services through a separate legal person»).

The structural separation should ensure that data or other insights gained from the provision of data intermediation services cannot be used for other activities pursued by the parent company or other affiliated firms.[64]

Art. 12 (b) DGA further prohibits providers from making the commercial terms, including pricing, for the provision of data intermediation services dependent on whether the data holder or data user uses other services provided by the same data intermediation services provider or by a related entity.

Art. 12 (d) DGA requires providers of data intermediation services to conduct the exchange of the data in the format in which they receive it from a data subject or a data holder.

This should prevent service providers from imposing their own data standards on their users which could lead to the so-called "user lock-in".[65] However, the conversion of data formats is permitted if it improves interoperability, is requested by the parties to the data transaction, or is necessary to comply with international or European standards. In these instances, data holders and data subjects must be offered an opt-out option regarding the conversion. Alternatively, format conversion can be mandated by Union law: in those cases, data holders and data subjects cannot refuse conversion.

Relatedly, according to Art. 12 (i) DGA the services providers shall take appropriate measures to ensure interoperability with other data

[62] I Graef, R Gellert, 'The European Commission's proposed data governance act: Some initial reflections on the increasingly complex EU regulatory puzzle of stimulating data sharing' (2021) 006 TILEC Discussion Paper, 12, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3814721.
[63] Cf. Recital 32 DGA.
[64] von Ditfurth, Lienemann, 'The Data Governance Act' 284.
[65] ibid. 285.

intermediation services, i.e. by using common and open standards in the reference sector.

Additionally, common and open interoperability specifications will be promoted by the DA across sectors to achieve effective interoperability

between service providers. Arts. 33[66], 34[67] and 35[68] DA lay down the essential requirements and conditions to facilitate interoperability of data, data sharing

[66] Art. 33 DA « 1. Participants in data spaces that offer data or data services to other participants shall comply with the following essential requirements to facilitate the interoperability of data, of data sharing mechanisms and services, as well as of common European data spaces which are purpose- or sector-specific or cross- sectoral interoperable frameworks for common standards and practices to share or jointly process data for, inter alia, the development of new products and services, scientific research or civil society initiatives:
(a) the dataset content, use restrictions, licences, data collection methodology, data quality and uncertainty shall be sufficiently described, where applicable, in a machine-readable format, to allow the recipient to find, access and use the data;
(b) the data structures, data formats, vocabularies, classification schemes, taxonomies and code lists, where available, shall be described in a publicly available and consistent manner;
(c) the technical means to access the data, such as application programming interfaces, and their terms of use and quality of service shall be sufficiently described to enable automatic access and transmission of data between parties, including continuously, in bulk download or in real-time in a machine- readable format where that is technically feasible and does not hamper the good functioning of the connected product;
(d) where applicable, the means to enable the interoperability of tools for automating the execution of data sharing agreements, such as smart contracts shall be provided.
The requirements can have a generic nature or concern specific sectors, while taking fully into account the interrelation with requirements arising from other Union or national law.
2. The Commission is empowered to adopt delegated acts, in accordance with Article 45 of this Regulation to supplement this Regulation by further specifying the essential requirements laid down in paragraph 1 of this Article, in relation to those requirements that, by their nature, cannot produce the intended effect unless they are further specified in binding Union legal acts and in order to properly reflect technological and market developments.
The Commission shall when adopting delegated acts take into account the advice of the EDIB in accordance with Article 42, point (c)(iii).
3. The participants in data spaces that offer data or data services to other participants in data spaces which meet the harmonised standards or parts thereof, the references of which are published in the Official Journal of the European Union, shall be presumed to be in conformity with the essential requirements laid down in paragraph 1 to the extent that those requirements are covered by such harmonised standards or parts thereof.
4. The Commission shall, pursuant to Article 10 of Regulation (EU) No 1025/2012, request one or more European standardisation organisations to draft harmonised standards that satisfy the essential requirements laid down in paragraph 1 of this Article.
5. The Commission may, by means of implementing acts, adopt common specifications covering any or all of the essential requirements laid down in paragraph 1 where the following conditions have been fulfilled:
(a) the Commission has requested, pursuant to Article 10(1) of Regulation (EU) No 1025/2012, one or more European standardisation organisations to draft a harmonised standard that satisfies the essential requirements laid down in paragraph 1 of this Article and:
(i) the request has not been accepted;
(ii) the harmonised standards addressing that request are not delivered within the deadline set in accordance with Article 10(1) of Regulation (EU) No 1025/2012; or
(iii) the harmonised standards do not comply with the request; and
(b) no reference to harmonised standards covering the relevant essential requirements laid down in paragraph 1 of this Article is published in the Official Journal of the European Union in accordance with Regulation (EU) No 1025/2012 and no such reference is expected to be published within a reasonable period.
Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 46(2).
6. Before preparing a draft implementing act referred to in paragraph 5 of this Article, the Commission shall inform the committee referred to in Article 22 of Regulation EU No 1025/2012 that it considers that the conditions in paragraph 5 of this Article have been fulfilled.
7. When preparing the draft implementing act referred to in paragraph 5, the Commission shall take into account the advice of the EDIB and views of other relevant bodies or expert groups and shall duly consult all relevant stakeholders.
8. The participants in data spaces that offer data or data services to other participants in data spaces that meet the common specifications established by implementing acts referred to in paragraph 5 or parts thereof shall be presumed to be in conformity with the essential requirements laid down in paragraph 1 to the extent that those requirements are covered by such common specifications or parts thereof.

mechanisms, common European data spaces, as well as of interoperability of data processing services. Art. 36 DA also specifies some essential requirements for data sharing when using smart contracts.[69]

9. Where a harmonised standard is adopted by a European standardisation organisation and proposed to the Commission for the purpose of publishing its reference in the Official Journal of the European Union, the Commission shall assess the harmonised standard in accordance with Regulation (EU) No 1025/2012. Where the reference of a harmonised standard is published in the Official Journal of the European Union, the Commission shall repeal the implementing acts referred to in paragraph 5 of this Article, or parts thereof which cover the same essential requirements as those covered by that harmonised standard.
10. When a Member State considers that a common specification does not entirely satisfy the essential requirements laid down in paragraph 1, it shall inform the Commission thereof by submitting a detailed explanation. The Commission shall assess that detailed explanation and may, if appropriate, amend the implementing act establishing the common specification in question.
11. The Commission may adopt guidelines taking into account the proposal of the EDIB in accordance with Article 30, point (h), of Regulation (EU) 2022/868 laying down interoperable frameworks for common standards and practices for the functioning of common European data spaces».

[67] Art. 34 DA «1. The requirements laid down in Article 23, Article 24, Article 25(2), points (a)(ii), (a)(iv), (e) and (f) and Article 30(2) to (5) shall also apply mutatis mutandis to providers of data processing services to facilitate interoperability for the purposes of in-parallel use of data processing services.
2. Where a data processing service is being used in parallel with another data processing service, the providers of data processing services may impose data egress charges, but only for the purpose of passing on egress costs incurred, without exceeding such costs».

[68] Art. 35 DA «1. Open interoperability specifications and harmonised standards for the interoperability of data processing services shall:
(a) achieve, where technically feasible, interoperability between different data processing services that cover the same service type;
(b) enhance portability of digital assets between different data processing services that cover the same service type;
(c) facilitate, where technically feasible, functional equivalence between different data processing services referred to in Article 30(1) that cover the same service type;
(d) not have an adverse impact on the security and integrity of data processing services and data;
(e) be designed in such a way so as to allow for technical advances and the inclusion of new functions and innovation in data processing services.
2. Open interoperability specifications and harmonised standards for the interoperability of data processing services shall adequately address:
(a) the cloud interoperability aspects of transport interoperability, syntactic interoperability, semantic data interoperability, behavioural interoperability and policy interoperability;
(b) the cloud data portability aspects of data syntactic portability, data semantic portability and data policy portability;
(c) the cloud application aspects of application syntactic portability, application instruction portability, application metadata portability, application behaviour portability and application policy portability.
3. Open interoperability specifications shall comply with Annex II to Regulation (EU) No 1025/2012.
4. After taking into account relevant international and European standards and self- regulatory initiatives, the Commission may, in accordance with Article 10(1) of Regulation (EU) No 1025/2012, request one or more European standardisation organisations to draft harmonised standards that satisfy the essential requirements laid down in paragraphs 1 and 2 of this Article.
5. The Commission may, by means of implementing acts, adopt common specifications based on open interoperability specifications covering all of the essential requirements laid down in paragraphs 1 and 2.
6. When preparing the draft implementing act referred to in paragraph 5 of this Article, the Commission shall take into account the views of the relevant competent authorities referred to in Article 37(5), point (h) and other relevant bodies or expert groups and shall duly consult all relevant stakeholders
7. When a Member State considers that a common specification does not entirely satisfy the essential requirements laid down in paragraphs 1 and 2, it shall inform the Commission thereof by submitting a detailed explanation. The Commission shall assess that detailed explanation and may, if appropriate, amend the implementing act establishing the common specification in question.
8. For the purpose of Article 30(3), the Commission shall, by means of implementing acts, publish the references of harmonised standards and common specifications for the interoperability of data processing services in a central Union standards repository for the interoperability of data processing services.
9. The implementing acts referred to in this Article shall be adopted in accordance with the examination procedure referred to in Article 46(2)».

[69] Art. 36 DA «1. The vendor of an application using smart contracts or, in the absence thereof, the person whose trade, business or profession involves the deployment of smart contracts for others in the context

of executing an agreement or part of it, to make data available shall ensure that those smart contracts comply with the following essential requirements of:
(a) robustness and access control, to ensure that the smart contract has been designed to offer access control mechanisms and a very high degree of robustness to avoid functional errors and to withstand manipulation by third parties;
(b) safe termination and interruption, to ensure that a mechanism exists to terminate the continued execution of transactions and that the smart contract includes internal functions which can reset or instruct the contract to stop or interrupt the operation, in particular to avoid future accidental executions;
(c) data archiving and continuity, to ensure, in circumstances in which a smart contract must be terminated or deactivated, there is a possibility to archive the transactional data, smart contract logic and code in order to keep the record of operations performed on the data in the past (auditability);
(d) access control, to ensure that a smart contract is protected through rigorous access control mechanisms at the governance and smart contract layers; and
(e) consistency, to ensure consistency with the terms of the data sharing agreement that the smart contract executes.
2. The vendor of a smart contract or, in the absence thereof, the person whose trade, business or profession involves the deployment of smart contracts for others in the context of executing an agreement or part of it, to make data available shall perform a conformity assessment with a view to fulfilling the essential requirements laid down in paragraph 1 and, on the fulfilment of those requirements, issue an EU declaration of conformity.
3. By drawing up the EU declaration of conformity, the vendor of an application using smart contracts or, in the absence thereof, the person whose trade, business or profession involves the deployment of smart contracts for others in the context of executing an agreement or part of it, to make data available shall be responsible for compliance with the essential requirements laid down in paragraph 1.
4. A smart contract that meets the harmonised standards or the relevant parts thereof, the references of which are published in the Official Journal of the European Union, shall be presumed to be in conformity with the essential requirements laid down in paragraph 1 to the extent that those requirements are covered by such harmonised standards or parts thereof.
5. The Commission shall, pursuant to Article 10 of Regulation (EU) No 1025/2012, request one or more European standardisation organisations to draft harmonised standards that satisfy the essential requirements laid down in paragraph 1 of this Article.
6. The Commission may, by means of implementing acts, adopt common specifications covering any or all of the essential requirements laid down in paragraph 1 where the following conditions have been fulfilled:
(a) the Commission has requested, pursuant to Article 10(1) of Regulation (EU) No 1025/2012, one or more European standardisation organisations to draft a harmonised standard that satisfies the essential requirements laid down in paragraph 1 of this Article and:
(i) the request has not been accepted;
(ii) the harmonised standards addressing that request are not delivered within the deadline set in accordance with Article 10(1) of Regulation (EU) No 1025/2012; or
(iii) the harmonised standards do not comply with the request; and
(b) no reference to harmonised standards covering the relevant essential requirements laid down in paragraph 1 of this Article is published in the Official Journal of the European Union in accordance with Regulation (EU) No 1025/2012 and no such reference is expected to be published within a reasonable period.
Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 46(2).
7. Before preparing a draft implementing act referred to in paragraph 6 of this Article, the Commission shall inform the committee referred to in Article 22 of Regulation (EU) No 1025/2012 that it considers that the conditions in paragraph 6 of this Article have been fulfilled.
8. When preparing the draft implementing act referred to in paragraph 6, the Commission shall take into account the advice of the EDIB and views of other relevant bodies or expert groups and shall duly consult all relevant stakeholders.
9. The vendor of a smart contract or, in the absence thereof, the person whose trade, business or profession involves the deployment of smart contracts for others in the context of executing an agreement or part of it, to make data available that meet the common specifications established by implementing acts referred to in paragraph 6 or parts thereof shall be presumed to be in conformity with the essential requirements laid down in paragraph 1 to the extent that those requirements are covered by such common specifications or parts thereof.
10. Where a harmonised standard is adopted by a European standardisation organisation and proposed to the Commission for the purpose of publishing its reference in the Official Journal of the European Union, the Commission shall assess the harmonised standard in accordance with Regulation (EU) No 1025/2012. Where the reference of a harmonised standard is published in the Official Journal of the European Union,

Data intermediaries are also required to adhere to procedures for access to their services that are fair, transparent and non-discriminatory to users, including with regards to prices and terms of service (Art. 12 (f) DGA).

Providers of data intermediation services are prohibited from treating their users differently without justification. The prohibition on discrimination should prevent possible distortions of competition and market foreclosures.

Bearing in mind both the platform operators' ability to exclude third party providers from their platforms or to otherwise disadvantage them,[70] Art. 12 (f) DGA addresses the "gatekeeper" position of data intermediation services providers, obliging them to ensure that the procedure for access to their service is fair, transparent and non-discriminatory for both data subjects and data holders, as well as for data users, including with regard to prices and terms of service.

This provision protects the ability of users to use multiple data intermediation services offered by different providers simultaneously (multi-homing), since exclusivity clauses imposed by providers on their users should be considered as unfair.[71]

Conversely, to facilitate the access and sharing of relevant data for companies that do not qualify as gatekeepers, the DA introduces an unfairness test for B2B contract clauses on data sharing that have been imposed on SMEs. More precisely, para 4 and 5 of Art. 13 DA lists a number of clauses that are unfair or presumed to be unfair, and contrary to good faith and fair dealing.[72]

---

the Commission shall repeal the implementing acts referred to in paragraph 6 of this Article, or parts thereof which cover the same essential requirements as those covered by that harmonised standard.

11. When a Member State considers that a common specification does not entirely satisfy the essential requirements laid down in paragraph 1, it shall inform the Commission thereof by submitting a detailed explanation. The Commission shall assess that detailed explanation and may, if appropriate, amend the implementing act establishing the common specification in question».

[70] Stigler Center, Stigler Committee on digital platforms: Final Report (2019), 74.

[71] von Ditfurth, Lienemann, 'The Data Governance Act' 286.

[72] Art. 13 (4) (5) DA «4. In particular, a contractual term shall be unfair for the purposes of paragraph 3, if its object or effect is to:

(a) exclude or limit the liability of the party that unilaterally imposed the term for intentional acts or gross negligence;

(b) exclude the remedies available to the party upon whom the term has been unilaterally imposed in the case of non-performance of contractual obligations, or the liability of the party that unilaterally imposed the term in the case of a breach of those obligations;

(c) give the party that unilaterally imposed the term the exclusive right to determine whether the data supplied are in conformity with the contract or to interpret any contractual term.

5. A contractual term shall be presumed to be unfair for the purposes of paragraph 3 if its object or effect is to:

(a) inappropriately limit remedies in the case of non-performance of contractual obligations or liability in the case of a breach of those obligations, or extend the liability of the enterprise upon whom the term has been unilaterally imposed;

(b) allow the party that unilaterally imposed the term to access and use the data of the other contracting party in a manner that is significantly detrimental to the legitimate interests of the other contracting party, in particular when such data contain commercially sensitive data or are protected by trade secrets or by intellectual property rights;

(c) prevent the party upon whom the term has been unilaterally imposed from using the data provided or generated by that party during the period of the contract, or to limit the use of such data to the extent that that party is not entitled to use, capture, access or control such data or exploit the value of such data in an adequate manner;

(d) prevent the party upon whom the term has been unilaterally imposed from terminating the agreement within a reasonable period;

As stated in Art. 12 (l) DGA, all necessary measures to ensure an appropriate level of security for the storage, processing and transmission of non-personal data must be taken by data intermediaries. Moreover, for the storage and transmission of competitively sensitive information it should be ensured the highest level of security.

Pursuant to Art. 12 (j) DGA, services providers are required to put in place adequate technical, legal and organisational measures in order to prevent unlawful transfers of or access to non-personal data. In substance, intermediation services providers are obligated to monitor data transactions of their users for violations of laws and to prevent illegal data transactions: providers are to assume responsibilities as "first-line enforcers" of the law.[73]

By focusing on the adequacy of measures, the provision could be interpreted in the sense that it would be sufficient to implement mechanisms for reporting legal violations by third parties and procedures for the exclusion of users.[74]

In the event of an unauthorized transfer, access or use of the non-personal data shared the data intermediation services provider is obliged to inform data holders without delay (Art. 12 (k) DGA).

According to Art. 12 (g) DGA, providers of data intermediation services are also required to have in place procedures for preventing fraudulent or abusive practices. Thus, data intermediation services providers will have to check the reliability of the services of potential users.

If the intermediaries offer data sharing services for natural persons, there is an additional fiduciary duty towards individuals that the provider bears in order to act in the best interests of data subjects when facilitating the exercise of their rights. This includes advising data subjects on potential data uses and on standard terms and conditions attached to such uses (Art. 12 (m) DGA).

An important data subject's right whose use data sharing services can facilitate is the right to data portability.[75]

---

(e) prevent the party upon whom the term has been unilaterally imposed from obtaining a copy of the data provided or generated by that party during the period of the contract or within a reasonable period after the termination thereof;
(f) enable the party that unilaterally imposed the term to terminate the contract at unreasonably short notice, taking into consideration any reasonable possibility of the other contracting party to switch to an alternative and comparable service and the financial detriment caused by such termination, except where there are serious grounds for so doing;
(g) enable the party that unilaterally imposed the term to substantially change the price specified in the contract or any other substantive condition related to the nature, format, quality or quantity of the data to be shared, where no valid reason and no right of the other party to terminate the contract in the case of such a change is specified in the contract.
Point (g) of the first subparagraph shall not affect terms by which the party that unilaterally imposed the term reserves the right to unilaterally change the terms of a contract of an indeterminate duration, provided that the contract specified a valid reason for such unilateral changes, that the party that unilaterally imposed the term is required to provide the other contracting party with reasonable notice of any such intended change, and that the other contracting party is free to terminate the contract at no cost in the case of a change».

[73] Graef, Gellert, 'The European Commission's proposed data governance act' 12.

[74] von Ditfurth, Lienemann, 'The Data Governance Act' 287.

[75] Art. 20 (4) GDPR. On this topic see S Troiano, 'Il diritto alla portabilità dei dati', in N Zorzi Galgano (ed.), *Persona e mercato dei dati. Riflessioni sul GDPR*, (Cedam, 2019), 197 ff.; E Pelino, 'Diritti dell'interessato', in C Bistolfi, (ed.), *Il regolamento privacy europeo. Commentario alla nuova disciplina sulla protezione dei dati personali*, (Giuffrè Francis Lefrebvre, 2016), 246 ff.; I Graef, M Husovec and N Purtova, 'Data Portability and Data Control: Lessons for an Emerging Concept in EU Law' (2018) 19(6) German Law Journal, 1359 ff., https://research.tilburguniversity.edu/en/publications/data-portability-and-data-control-lessons-for-an-emerging-concept.; L Somaini, 'The right to data portability and user control: ambitions and limitations'

Scholars highlighted the "multifunctional value" of this right which is capable, on the one hand, of enhancing at maximum the data subject's control over his/her data, thus representing the fullest expression of the right to personal data protection in its positive projection, on the other hand, being a right that has its initial justification in the stimulation of the market and competition, the data portability right represents a propulsive force for the free circulation of data.[76]

In the DGA's framework, the data portability right seems enhancing more the latter aspect, so much so that it appears more functional to the control of data holders, than to that of data subjects.[77]

Furthermore, where data subjects are provided with tools for giving consent or permissions to process data made available by data holders, the intermediary is obliged to specify the third-country jurisdiction in which the data use is intended to take place and provide data subjects with tools to both give and withdraw consent and data holders with tools to both give and withdraw permissions to process data (Art. 12 (n) DGA).

Art. 12 (h) provides in the event of the insolvency of the data intermediation services provider, imposing a reasonable continuity of the provision of data intermediation services. In addition, whenever the above-mentioned services ensure the storage of data, data holders and data users have the right to obtain access to, to transfer or to retrieve their data, and whenever such data intermediation services are provided between data subjects and data users, data subjects can exercise their rights.

It is unclear how data intermediaries are supposed to ensure the continuity of their services in the event of insolvency, considering that according to the insolvency laws of most Member States the legal authority to decide about the continuation of a business is transferred to a liquidator or insolvency administrator once insolvency proceedings have begun.[78]

Lastly, pursuant to art. 12 (o) DGA data intermediation services providers are obliged to maintain a log record of the data intermediation activity.

## 5. The enforcement mechanism.

Pursuant to Art. 13 (1) DGA each Member State is required to designate one or more authorities responsible for carrying out the notification procedure and enforcing the DGA's rules within their jurisdiction.

The DGA does not specify whether the national authority should have a particular expertise or mandate. It is up to Member States to decide whether their data protection, competition, consumer or even cybersecurity agency is best placed to implement the notification framework.[79]

(2018) 3 Rivista di diritto dei media, 164 ff., https://www.medialaws.eu/wp-content/uploads/2019/05/8.-Somaini.pdf.

[76] Troiano, 'Il diritto alla portabilità dei dati' 199 ff.

[77] Poletti, 'Gli intermediari dei dati' 55.

[78] von Ditfurth, Lienemann, 'The Data Governance Act' 290. For example, with regard to Italian insolvency law cf. Arts. 128-129 D.lgs. 12 January 2019, n. 14, ("Codice della crisi d'impresa e dell'insolvenza").

[79] For this remark on the DGA proposal, see Graef, Gellert, 'The European Commission's proposed data governance act' 8.

Providers of data intermediation services are required to submit a notification to the competent authority of the Member State in which they have their main establishment (Art. 11 (1) DGA).

This obligation also applies to data intermediaries which are not established in the EU as long as they offer their services within the EU. International data intermediaries are required to designate a legal representative in one of the Member States where they intend to offer their services (Art. 11 (3) DGA).

In such cases, the designation of a legal representative is deemed necessary given that such data intermediation services providers handle personal data as well as commercially confidential data, which entails the close monitoring of the compliance of data intermediation services providers with the DGA.[80]

Furthermore, the notification system is designed as a one-stop-shop: according to Art. 11 (5) DGA, data intermediaries are entitled to offer their services in all Member States once they have notified the competent authority.

It must be noted that it is not required that the providers of data intermediation services are to be approved by the competent authority before taking up their services. According to Art. 11 (4) DGA, they can begin offering their services as soon as they have submitted a notification to the competent authority. In any case, pursuant to Art. 11 (9) DGA they can request that the competent authority confirms their compliance with the conditions set out in Art. 11 and 12 DGA.

Once they have taken up their services, providers of data intermediation services are required to follow the conditions set out in Art. 12 DGA.

The competent authorities of the Member States monitor the providers' compliance with the notification procedures and the conditions for providing data intermediation services (Art. 14 (1) DGA). Thus, the DGA framework consists of compulsory notification with only ex-post monitoring of whether providers of data sharing services comply with the applicable requirements.

Since the legality of data intermediation services is not checked by the competent authorities before they are allowed to take up their services, the approach chosen by the European Commission could be less effective in building user trust than a system of ex-ante authorization: potential users of such services have to rely on the threat of sanctions to provide sufficient incentives for data intermediation services providers to comply with the rules of the DGA.[81].

## 6. Risks of data sharing and the limits of the DGA.

Scholars have expressed concerns about the adequacy of the DGA's framework to achieve its multiple objectives, both questioning its actual potential in terms of achieving a competitive data market and pointing out its inconsistency and even harmfulness in terms of protecting the fundamental rights of data subjects.

[80] Cf. Recital 42 DGA.
[81] von Ditfurth, Lienemann, 'The Data Governance Act' 281-282.

First of all, it appears to be a certain tension between the DGA's approach to protecting horizontal and vertical competition and its objective of promoting the scaling up of data intermediaries.

The strict obligations imposed on data intermediation services in order to protect competition could turn out to severely limit the potential value of data sharing. More precisely, by vertically unbundling data intermediation services from other data related services and restricting the use of data generated by data intermediaries (Art. 12 (a) and (c) DGA), the DGA restrains their ability to capture economies of scope. [82] In other words, data intermediaries are prohibited from combining data generated by different services in order to gain valuable insights that could raise the quality of their data intermediation services.

Due to its rigidity, the framework of the DGA prohibits practices without exceptions, even if they are procompetitive and efficient to the development of the EU data economy, thus reducing the value data intermediation services can provide to their users.[83]

Furthermore, the strict obligations aimed at protecting competition will increase the already considerable regulatory burdens faced by data intermediaries. They could also, in some instances, prevent pro-competitive and desirable activities by non-dominant data intermediaries and cut off the market's process of experimentation at a time when few data intermediaries have been established successfully.[84] In this respect, it must be noted that the addressee of the DGA are companies that are young and are yet to develop a relevant market power.

The scope and intensity of the DGA's framework can be compared to that of the Digital Markets Act.[85] However, it should be pointed out the different circumstances in the respective industries: while the industries targeted by the Digital Markets Act are quite concentrated and mainly consist of a few large US-based players, the data sharing services the DGA wishes to promote are still mostly in their infancy.[86]

With regard to the compatibility between the DGA and the instance of protecting data subjects' personal data from external aggression, it seems that the new Regulation reproduces the issues regarding the conflict between facilitating the mass transfer of personal data through interoperable formats or otherwise, allowing for the easy and rapid reuse of such data, and the principle of data minimization set forth in Art. 5 (1) (c) GDPR.[87]

The promotion of data sharing seems to hopelessly conflict with the underlying spirit of the other rights of the data subject, namely the need for minimization of data and related risks to processing of personal data.

In the DGA's framework data subjects' rights seem to be inextricably linked to the stimulation of the market and competition. According to the new

[82] ibid. 289.
[83] ibid.
[84] ibid. 292. See also G Resta, 'Pubblico, privato, collettivo nel sistema europeo di governo dei dati' (2022) 4 Rivista trimestrale di diritto pubblico, 990.
[85] J Baloup and others, 'White paper on the data governance act' (2021), 32, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3872703.
[86] Graef, Gellert, 'The European Commission's proposed data governance act' 11.
[87] See Troiano, 'Il diritto alla portabilità dei dati' 210-211 ff. on the data portability right.

Regulation, fundamental rights appear more functional to the commercial activity carried out by intermediaries and data holders, than to the protection of data subjects.

The DGA constitutes yet another confirmation of a new way of interpreting personal data protection law, whose personalistic principle gradually gives way to the need to promote the free movement of personal data.[88]

## Conclusions.

The regulatory approach chosen for the DGA, on the one hand, could keep data intermediation services from fully unlocking their potential as much-needed matchmakers on markets for data sharing, on the other hand, carries a tension between data protection principles and data sharing, as reported by the EDPB and the EDPS in their joint opinion.

With regard to this last aspect, it is undisputed that the coordination between the DGA and the GDPR requires going beyond general and abstract phrasing such as the one contained in Art. 1 (3) DGA, according to which «this Regulation is without prejudice to Regulation (EU) 2016/679 […]».

In general, the counterweights provided by the DGA do not seem sufficient to contain the risks of the commodification of personal data entailed in data intermediation services, due to their vagueness and difficult application.

At present, the compatibility of the DGA with the rest of the EU acquis looks like a mere afterthought that is left to market players to figure out.[89] If anything, to make sure the DGA achieves its objectives, compliance with the EU data protection law should have been considered upfront, during the legislative process. Only in doing so it would have been possible to offer a (consciously) positive answer to the question posed by this paper: does sharing mean caring?

[88] According to N Zorzi Galgano, 'Le due anime del GDPR e la tutela del diritto alla *privacy*', in N Zorzi Galgano (ed.), *Persona e mercato dei dati. Riflessioni sul GDPR*, (Cedam, 2019), 36 ff., two fundamental rights emerge from the GDPR, two souls that constitute an explication of the protection provided therein, on the one hand, the so-called right to privacy of the data subject, and on the other hand, the right to data processing and the right to data circulation, both manifestation of freedom to conduct a business.

[89] See, on the DGA proposal Graef, Gellert, 'The European Commission's proposed data governance act' 15.