COMPUTER LAW & SECURITY REVIEW 50 (2023) 105830

Available online at www.sciencedirect.com

ScienceDirect

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

Computer Law & Security Review

Regulating data intermediaries: The impact of the Data Governance Act on the EU's data economy

Gabriele Carovano[a,1,*], *Michèle Finck*[b,1]

[a] *Postdoctoral Researcher in Law and Artificial Intelligence, University of Tübingen, Geschwister-Scholl-Platz, D-72074, Tübingen, Germany*

[b] *Professor of Law and Artificial Intelligence, University of Tübingen, Geschwister-Scholl-Platz, D-72074, Tübingen, Germany*

ARTICLE INFO

Keywords:
Data governance act
General data protection regulation
Data act
Digital markets act
Data intermediaries
European data economy

ABSTRACT

As part of the European Commission's broader data strategy, the Data Governance Act ("DGA") introduces a new regulatory regime for data intermediaries, which, inter alia, pursues the objective of increasing the competitiveness of the European data economy by bolstering trust in data-sharing mechanisms. Against this backdrop, we introduce data intermediaries and critically examine the DGA's related legal regime by testing its underlying assumptions and highlighting its intrinsic weaknesses and limitations as part of the broader EU data law puzzle. As a result, the paper brings to the fore certain contradictions between DGA's means and ends. Indeed, due to various questionable assumptions, the DGA imposes requirements that not all data intermediaries can satisfy and entrenches a specific techno-organisational form for data intermediation services that may turn out to be economically non-viable. Consequently, one must wonder whether the DGA's rules on data intermediaries are necessary and proportionate in light of the freedom to conduct a business. We furthermore uncover inconsistencies and loopholes between the DGA, the GDPR, the draft Data Act, and the Digital Markets Act. Overall, while the DGA's underlying efforts are laudable, its precise postulations may hinder the achievement of its underlying objectives due to two main factors. First its own internal limitations and incoherences, and, second, uncertainties and tensions resulting from its interplay with the broader EU data law framework.

* Corresponding author.
E-mail addresses: Gabriele.Carovano@uni-tuebingen.de (G. Carovano), Michele.Finck@uni-tuebingen.de (M. Finck).

[1] Both authors contributed equally to the paper.

https://doi.org/10.1016/j.clsr.2023.105830

1. Introduction

The Data Governance Act ("DGA")[1] was enacted in May 2022 and most of its provisions will become binding in September 2023.[2] It forms part of the European Commission's broader data strategy,[3] and, inter alia, seeks to incentivise data-sharing in order to strengthen the Digital Single Market.[4] In contrast to the new data-sharing regime for IoT data envisaged by the draft Data Act, the DGA incentivises the *voluntary* sharing of data between different actors, inter alia through the creation of a legal regime for data intermediaries ("DIs"), that is to say entities that intermediate between data holders/subjects and potential data users to facilitate sharing of personal and non-personal data.

A DI is a middleman that interposes between data holders and data users to facilitate the exchange of data in a neutral fashion (that is to say without processing the data to its own ends).[5] As such, DIs are expected to restructure the EU data economy so as to, first, redistribute the excessive concentration of data and, second, facilitate the fluidity of currently mostly idle data in compliance with EU fundamental rights. It therefore pursues three interlinked aspirations: (i) the formation of a European model for trustworthy data sharing that is respectful of fundamental rights; (ii) the formation of a more diversified, and less concentrated data economy; (iii) the reduction of the market power of non-European tech firms.

The DGA is driven by four underlying assumptions. First, that the above objectives can only be realised through a middleman: the data intermediary, despite all criticisms directed towards middlemen in recent years. Second, that all DIs are aware of the characteristics of the data they intermediate. Third, that although DIs are likely to replicate some of the existing tech giants' most criticised features (as they are likewise expected to benefit from network and lock-in effects, economies of scale, and high switching barriers), the DGA will be able to tame them. Fourth, that neutral DIs are economically viable despite the prohibition of vertical integrations or cross-subsidisations.[6]

This paper brings those assumptions to the fore and tests their validity. We introduce data intermediaries (Section 2) and the DGA's related legal regime (Section 3) before testing its underlying assumptions and highlighting its intrinsic weaknesses (Section 4) as well as limitations when contextualised within the broader EU data law puzzle (Section 5). We conclude by arguing that the DGA's well-intended regime on data intermediaries is likely to encounter significant tensions and uncertainties that may ultimately stand in the way of the realisation of its objectives (Section 6).

2. Introducing data intermediaries and their economic function

In recent years, there have been growing calls for supranational norms that can facilitate access to and sharing of data to stimulate data-related innovation in the EU. As a result, the European Commission has put forward an entire suite of legislative proposals that set out different measures designed to incentivise a greater accessibility of personal and non-personal data. As one of these norms, the DGA creates three new legal regimes. First, rules for the re-use, in the EU, of certain categories of data held by public sector bodies; second, a notification and supervisory framework for the provision of data intermediation services ("DISs"); and finally, a framework for voluntary registration of data altruism services (a mechanism that enables data subjects to donate their personal data).

We focus on the DGA's novel legal regime on data intermediaries, which are envisioned to play a pivotal role in reshaping the data economy by increasing trust in data-sharing and eliminating asymmetries of power and information through the emergence of a new middleman that interposes itself in a neutral fashion between data holders/subjects and data users. Despite a plurality of methodologies to conceptualise data intermediaries that have been advanced by academics, institutions, and practitioners, terminology and taxonomy are still in flux.[7] This is because data intermediaries are a nascent class of techno-economic actors in a relatively early stage of de-

[1] Regulation 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), O.J. L152, 3.6.2022, p. 1-44.

[2] Notably, the focus of this paper, i.e., the legal regime on data intermediation services, will not enter into force together with the other provisions of the DGA in September 2023. Rather, based on Article 37, data intermediaries have thirty-nine extra months for complying with DGA Chapter III obligations. This can be taken as a sign that these provisions are burdensome and time-consuming to implement.

[3] A European strategy for data, COM/2020/66 final, Brussels, (2020).

[4] This is a broader legislative objective that is, inter alia, also pursued by the draft Data Act.

[5] It is, however, important to stress that data intermediaries already exist today and can also currently lawfully operate provided they comply with the provisions of EU data law that preceded the DGA.

[6] Article 12 DGA.

[7] A. Shaharudin, B. Van Loenen, M. Janssen, 'Towards a Common Definition of Open Data Intermediaries', *Digit. Gov.: Res. Pract*, (2023), (<https://doi.org/10.1145/3585537>); H. Richter, 'Looking at the Data Governance Act and Beyond: How to Better Integrate Data Intermediaries in the Market Order for Data Sharing', *GRUR International*, (2023); L. von Ditfurth, G. Lienemann, 'The Data Governance Act: – Promoting or Restricting Data Intermediaries?', (2022) *Competition and Regulation in Network Industries,* 23(4), 270–295, (<;https://doi.org/10.1177/17835917221141324>); H. Janssen, J. Singh, 'The Data Intermediary', *Internet Policy Review,* (2022) 11(1), (<https://doi.org/10.14763/2022.1.1644>); N. Zingales, 'Data collaboratives, competition law and the governance of EU data spaces' (*Concurrences*, 2021); N. Simon *et al.*, 'Definition and analysis of the EU and worldwide data market trends and industrial needs for growth' (*TRUSTS Trusted Secure Data Sharing Space*, 2021), p.21-25; A. Wernick, C. Olk, M. Von Grafenstein, 'Defining Data Intermediaries: A Clearer View through the Lens of Intellectual Property Governance' (2020) 2 *Technology and Regulation* 65; OECD, 'Enhancing Access to and Sharing of Data: Reconciling Risks and Benefits for Data Re-use across Societies', *OECD Publishing*, Paris, (<https://doi.org/10.1787/276aaca8-en>).

velopment, which exhibit different business models, techno-organisational structures, and typologies of services offered.[8]

2.1. *Business models*

DISs can be provided either by private or public entities[9] that in turn can have either a for-profit or a not-for-profit orientation.[10] They finance their activities in a plurality of ways, such as through subscription plans to access centrally provided datasets,[11] transaction fees calculated as a percentage of the data transactions, subscription plans,[12] or through private, public, or mixed financial contributions to sponsor and support data collaborations in certain sectors.[13]

2.2. *Structure*

DIs also exhibit different structures. They can position themselves anywhere in between centralised, hierarchical set-ups, on the one hand, and horizontal, fully distributed models on the other. They offer their services either through centralised servers or through fully public and permissionless blockchains.[14] Similarly, DIs have variable degrees of control over the data they vehiculate such as by storing, checking, filtering, and protecting all the data they handle, or more simply in limiting themselves at facilitating the data sharing between data holders/subjects and data users.

2.3. *Value-added services*

Finally, DIs can provide services that exceed pure intermediation including security, authentication, and fraud prevention services such as anonymisation or pseudo-anonymisation services, regulatory compliance services ("RegTech"),[15] or personal information management services ("PIMSs") to give data subjects more control over their personal data.[16] DIs act either as trusted third parties,[17] or as data custodians[18] eventually also offering trusted protected environments for data analysis[19] or other auditing services of data driven technologies,[20] or as data trustees[21] that ultimately could go as far as enabling automated intermediation through trusted digital agents.[22] Such add-ons can allow DIs to acquire a competitive edge over their competitors, yet as seen below, also bears regulatory risk under the DGA as it remains somewhat unclear what services beyond intermediation DIs can legally offer.

Additionally, DIs can either be data marketplaces that centrally store and exchange data between data holders/subjects and data users,[23] or more simply be orchestrators of ecosystems that are open to all interested parties.[24] This is the case, for instance, for the European data spaces or data pools established jointly by several legal (such as data cooperatives) or natural persons with the intention to licence the use of pooled data to all participants so as to reward those who contributed to their formation. Finally, DIs may not handle any sharing at all but simply make available the specific technical infrastructure needed to interconnect data subjects and data holders with data users.[25]

Fig. 1 captures the complex and dynamic reality of DIs, which are driven by different business models, and provide a wide spectrum of different services. Below, we argue that the DGA one-fits-all regime may entrench specific techno-organisational structures that disregard ongoing innovations, render certain DIs economically non-viable, and impose requirements that not all DIs can satisfy. There is thus reason to worry that the DGA curtails ongoing innovation in a manner that ends up impeding its underlying objectives.

3. The data governance act's new legal regime for data intermediaries

The DGA establishes a new legal regime for DIs, which comprises various procedural and substantive requirements.

3.1. *The DGA's material scope of application*

The DGA creates a sui generis legal framework for DISs. Whereas the Regulation defines what a 'data intermediation

[8] Centre for Data Ethics and Innovation, Unlocking the value of data: exploring the role of data intermediaries, Department for Digital, Culture, Media and Sport, (2021).

[9] For an example of an intergovernmental organisation offering data intermediary services, see ELIXIR (<https://elixir-europe.org/about-us>).

[10] For examples of not-for-profit DIs, see the Open Humans program (<https://www.openhumans.org/about/>) or the HiLo Maritime Risk Management ("HiLo").

[11] See, e.g. agdatahub (<https://agdatahub.eu/api-agro/tarifs/>) or NumAlim (<https://www.plateforme-numalim.fr/nos-tarifs/>).

[12] See, e.g.Dawex (<https://www.dawex.com/en/>).

[13] For examples of industrial data platforms, see the Advanced Product Concept Analysis Environment; HiLO; the Online Safety Data Initiative; and the MK:Smart Hub.

[14] See, e.g. Ocean Protocol (<https://oceanprotocol.com>).

[15] E.g. Quantexa (<https://www.quantexa.com>); SteelEye (<https://www.steel-eye.com>); Kompli Global (<https://www.kompli-global.com>); etc.

[16] For some examples of DIs offering personal information management systems ("PIMSs") see digi.me (<https://digi.me>) or Solid (<https://solidproject.org/about>).

[17] E.g. the UK Open Banking Implementation Entity.

[18] E.g. the UK Pension Dashboard Programme (<https://www.pensionsdashboardsprogramme.org.uk>) or the Genomics England project (<https://www.genomicsengland.co.uk>).

[19] OpenSAFELY, for instance, is a data custodian that, through federated learning technologies, provides a secure analytics platform for electronic health records. Specifically, OpenSAFELY enables independent researchers to run analyses without ever being able to see the underlying data directly and without transferring the data out of the secure data centre in which it resides.

[20] E.g., the U.S. National Institute of Standards and Technology.

[21] E.g., the Data Intelligence Hub created by Deutsche Telekom.

[22] World Economic Forum. 2022. Insight report – 'Advancing Digital Agency: the Power of Data Intermediaries'.

[23] E.g., AWS Data Exchange.

[24] Recital 32 DGA.

[25] E.g., Dawex (<https://www.dawex.com/en/>), which does not directly purchase or sell data but brings together companies interested in monetising and re-using data.

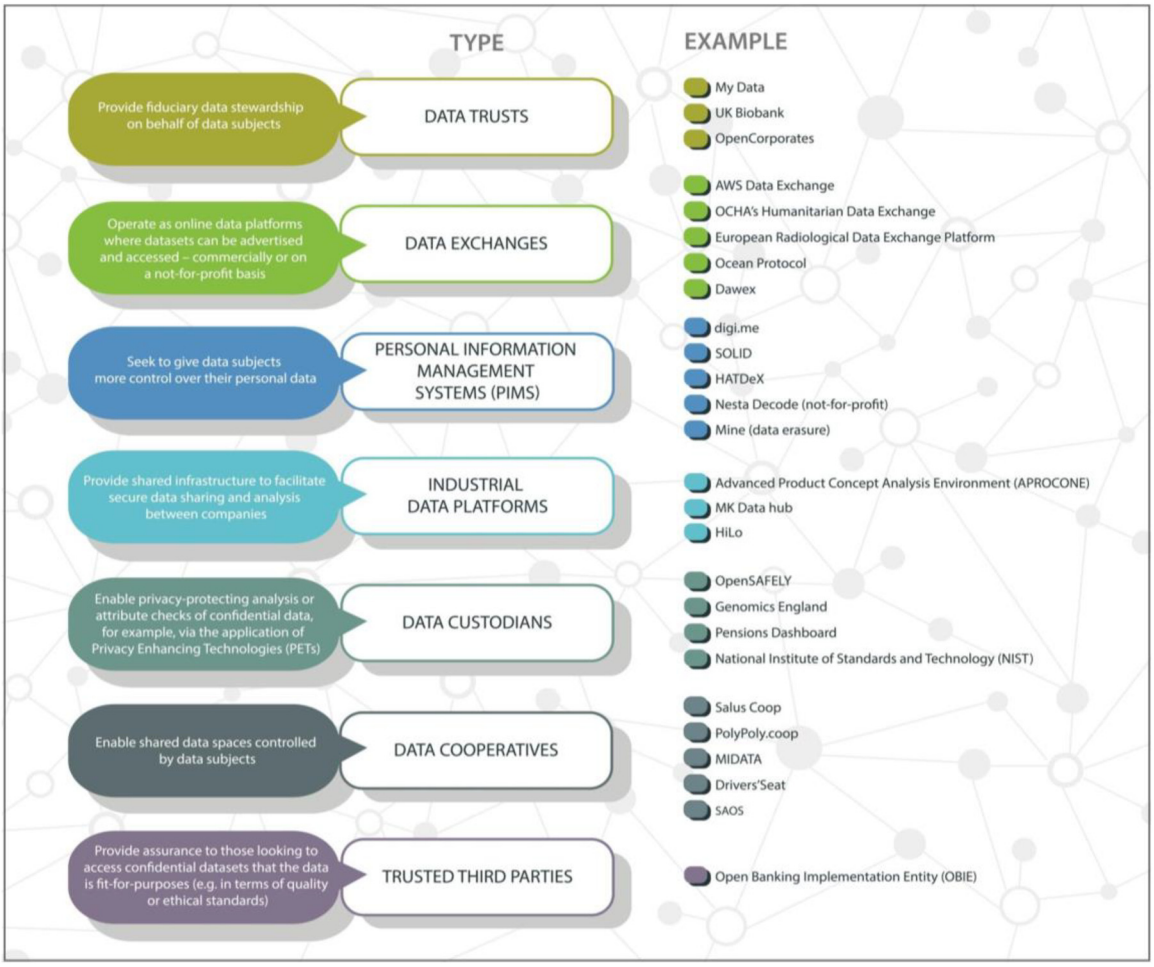

Fig. 1 – Different types of existing data intermediaries. *Source:* Realised by the authors.

service' is, it does not define the data intermediary providing these services.[26] It follows that the definition of the latter needs to be deduced from the former: a data intermediary is any entity that provides a data intermediation service.

DISs are services that aim '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, including for the purpose of exercising the rights of data subjects in relation to personal data'.[27] This definition implies that not all data sharing services are DISs and, consequently, that not all providers of data sharing services are providers of DISs in the sense of the DGA.

Notably, Article 2(11) DGA sets out four conditions for a service to qualify as a data intermediation service: (i) the service must occur for the sole purpose of data sharing; (ii) sharing must establish or aim to establish a commercial relationship; (iii) sharing must occur between an undetermined number of data holders/subjects and data users. Finally, this provision embraces a very broad material scope in providing that (iv) intermediation can occur through technical, legal, or other means.

3.1.1. *For the purposes of data sharing*

The DGA applies to actors that establish or aim to establish commercial relationships for the purposes of data sharing. Data sharing is defined as 'the provision of data by a data subject or a data holder to a data user for the purposes 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'.[28]

This definition omits engagement with the various forms through which data may be 'provided'. While it doubtlessly includes forms of data-sharing whereby the data is transferred from the servers of the intermediary to the data user, it can be questioned whether also included are technical tools that grant access to data in situ,[29] such as in safe execution en-

[26] Initially, data intermediaries were defined in Recital 22 of the European Commission's DGA proposal as 'providers of data sharing services'. Later on, however, the concept was completely erased from DGA's final text.

[27] Article 2(11) DGA.

[28] Article 2(10) DGA.

[29] E.g. Open Algorithms (so-called OPALs). On this, see T. Hardjono, D.L. Shrier, A. Pentland, 'Trusted Data. A new Framework

vironments. However, as Article 2(10) DGA generally defines data-sharing as 'the provision of data'[30] without specifying the modalities through which such provision occurs, it seems that algorithms transfers to the data (such as in federated learning) are also in scope as also here a 'provision of data' materialises.

The DGA excludes from its material scope services that intermediate copyright-protected content,[31] consolidated tape providers[32] and account information service providers[33] as these do not intermediate data for the sole purpose of sharing but also pursue additional ends. Equally excluded are data brokers, consultancies, and providers of products resulting from value added to the data by the provider.

In contrast, Article 2(11) includes data intermediations occurring 'for the purpose of exercising the rights of data subjects in relation to personal data', that is to say PIMS,[34] which are defined as a 'specific category' of data intermediation services.[35]

3.1.2. *(Direct?) Commercial relationships*

The DGA only applies to services that aim to establish commercial relationships for the purposes of data sharing.[36] Consequently, the DGA excludes from its definition of DIS not-for-profit data sharing providers whose activities qualify as data altruism.[37] These activities fall under the distinct legal regime applicable to data altruism. Similarly excluded are services offered by public sector bodies to facilitate either the re-use of protected data or the use of any other data, insofar as those services do not translate into commercial relationships.[38]

The DGA does not define what a commercial relationship is, raising the question of how existing DIS offered for free (or only partially for free) by private operators ought to be classified.[39] Conventionally, a commercial relationship is 'connected with buying or selling goods or services'.[40] Article 12(1)(b) DGA refers to the 'commercial terms, including pricing', which raises the question of whether a price is a sufficient or necessary condition for a commercial relationship to exist. This leads to a presumption that such services are subject to the DGA, and the resulting compliance costs, even where they make no income from the intermediation that is provided.

The requirement that data must be provided for commercial purposes moreover leads to further interpretative qualms, such as whether the commercial relationship between data holders/subjects and users must be direct. This distinction is pertinent in relation to data trusts, which can be established with diverse degrees of beneficiary participation and power delegation. While they may offer services equivalent to those of PIMSs, one may wonder whether data trusts are caught by Article 2(11) given that, in contrast to PIMS, data trustees do not enable data subjects' direct exercise of their rights but achieve equivalent aims by acting on their behalf. Since data trusts offer fiduciary data stewardship services on behalf of their users, one may wonder whether they establish commercial relationships between data holders/subjects and data users in a DGA sense.

Furthermore, requiring direct commercial relationships might create room for circumvention strategies as a service provider can transform the data it holds through aggregation, enrichment, inferences, mixture with synthetic data or other means and later licence the resulting data product to data users to break the direct commercial relationship between data holders/subjects and users.[41] Whereas the DGA's underlying assumption is that such acts will threaten the neutrality of these intermediaries and furthermore defeat them of the logo and the assumed related trust, it remains unsure how much the market actually values neutrality.

The requirement that a DIS aims to establish commercial relationships for the purposes of data sharing is, moreover, an interpretative aid to determine whether mere providers of technical data sharing infrastructure fall within the scope of the DGA. While Article 10 and Recital 32 DGA explicitly include in the DGA's scope entities that provide a technical infrastructure for enabling data intermediation services,[42] Recital 28 DGA excludes from DGA's scope certain services that 'only provide technical tools for data subjects or data holders to share data with others'[43] but which neither (a) establish a commercial relationship between data holders and users, nor (b) allow the DIS provider to acquire information on the establishment of a commercial relationship.[44] Accordingly, Recital 28 explicitly excludes from DGA's scope providers of cloud storage and data sharing software provided that they only make available technical tools that do not aim 'to establish a commercial relationship between data holders and data users',[45] and that do not allow 'the data intermediation services provider to acquire information on the establishment of commercial relationships for the purposes of data sharing'.[46] Thus, 'orchestrators of data sharing ecosystems that are open to all interested parties' are DIS providers even where they

Identity and Data Sharing' (2019) MIT Connection Science & Engineering.

[30] Article 2(10) DGA.

[31] E.g. online content-sharing service providers as defined in Article 2, point (6), of Directive (EU) 2019/790. For their exclusion from DGA's regime, see Recital 29 DGA.

[32] As defined in Article 2(1), point (35), of Regulation (EU) No 600/2014. For their exclusion from DGA's regime, see Recital 29 DGA.

[33] As defined in Article 4(19) Directive 2015/2366/EU. For their exclusion from DGA's regime, see Recital 29 DGA.

[34] Personal Information Management Systems (PIMSs) assist individuals in exercising their GDPR rights. See further H. Janssen, J. Singh, 'Personal Information Management Systems', *Internet Policy Review*, (2022), 11(2), (<https://policyreview.info/glossary/personal-information-management-systems>).

[35] Recital 30 DGA.

[36] Recital 28 DGA.

[37] Article 15 DGA.

[38] Recital 29 DGA.

[39] Notwithstanding, this notion is used repeatedly in the Act. See, e.g., Recitals 28, 29, and 30 DGA.

[40] Oxford dictionary (<https://www.oxfordlearnersdictionaries.com/definition/english/commercial_1>).

[41] Recital 28 DGA.

[42] Article 10(1)(a) and Recital 32 DGA.

[43] Recital 28 DGA.

[44] Recital 28 DGA.

[45] *Ibid*.

[46] *Ibid*.

only make available technical infrastructure to the extent that the above conditions are met.[47]

In practice, the distinction between the mere provision of technical infrastructure and the provision of technical infrastructure in view of facilitating (direct?) commercial relationships that the DIS provider can detect will be difficult to draw. Consider, by way of example, Dawex, which does not directly purchase or sell data but brings together companies interested in monetising and re-using data and provides them the technical infrastructure to both create personalised data hubs or data exchanges and acquire and sell data on the broader market.[48] Does Dawex establish a commercial relationship in the sense of the DGA and does it have sufficient knowledge of the existence of such relationships in order to qualify as a DIS provider under EU law? As data (sharing) ecosystems become ever more complex and potentially more decentralised, these questions will burden the determination of the DGA's scope of application. Beyond such factual uncertainties it also remains to be seen what weight the ECJ will give to clarifications in the Recitals, which only have interpretative value, vis-à-vis the legally binding text of the Regulation, considering that Article 2(11) and 10 DGA do not presuppose that the DIS provider has awareness of the formation of direct commercial relationships between data holders and users.

3.1.3. *Undetermined number*

Thirdly, DIS providers only fall within the DGA's scope if they intermediate between an undetermined number of data holders/subjects and data users.[49] The draft DGA contained a reference to 'indefinite' rather than 'undetermined' and the change of terminology is likely due to the criticism voiced by a joint opinion of the European Data Protection Board and the European Data Protection Supervisor that warned that intermediating between an 'indefinite' number of data holders and users as an open data marketplace would be contrary to the data protection principles of privacy by design and by default, transparency and purpose limitation if the platform does not allow a pre-selection of and prior information about the purposes and users of personal data to the data subject.[50]

According to the Cambridge Dictionary, indeterminate does not mean unlimited but rather 'not being measured, counted or clearly known'.[51] Yet, it is unlikely that the co-legislators intended for DIs to be able to evade the DGA's scope of application simply by ignoring user metrics. Indeed, even the most popular DIs will always be able to monitor the number of actors using their services. Yet, if that is the case then why insert this criterion at all?

Taking a teleological perspective, it is worth noting that Article 2(11)(c) and Recital 28 explicitly exclude services meant to be used either by a closed group or by one data holder to enable the use of its data.[52] In this sense, providers of cloud services, data sharing software, web browsers, or email services are excluded from its scope of application.[53] Data exchange platforms used by a single data holder to enable third parties' use of data and Internet-of-Things data platforms that are exclusively developed to ensure functionalities of the connected devices and allow value added services are similarly excluded.[54]

Notwithstanding, understanding when a group of users is not closed so as to make it undetermined remains problematic as it will always be possible to determine the number of users. The DGA indeed does not define a threshold to distinguish between a closed group and an undetermined number. These are not questions that should be left for the private sector or courts to define. Moreover, Article 12(1)(a) and Recital 27 further complicate matters as they, in slight contrast with Article 2(11) and Recital 28, explicitly mention bilateral sharing of data as DIS. In this sense, it is difficult to imagine how a bilateral exchange can occur between an undetermined number of data holders/subjects and data users.

The most likely explanation is that the intention of the legislator was not to look at specific user metrics but rather conditions of access, i.e. whether specific access controls are in place. Indeed, an alternative methodology to assess indeterminacy would be to disregard the actual number of users and consider the modalities of commercialisation. In other words, if a given DIS is provided in an open, unrestricted, and non-discriminatory fashion, it is not used by a closed group even if the actual number of users is minimal. Whether this is really different from the limitation in the GDPR[55] that were highlighted above and which the EU data protection authorities expressed concern over is, however, a matter of debate and potentially a question for courts to settle in the future.

Noticeably, these two alternative interpretations will have different implications. The former will reduce the number of DISs caught by the DGA, whereas the latter will have the opposite effect. They also affect the circumvention strategies that DIs can put in place in restricting access or design access to their services in order to evade the DGA's obligations. In this context, it remains to be seen how courts react to predominantly symbolic restrictions or expansions.

Finally, while the DGA excludes one-to-many, many-to-one, and many-to-few situations from its scope of application, it does not distinguish between scenarios where data sharing occurs in a business-to-business context, business-to-consumer context, or in a consumer-to-consumer context. They all fall within its scope as long as they concern many-to-many (direct?) commercial relationships between data holders/subjects and data users.

[47] *Ibid*.

[48] See Dawex, *supra* n.25.

[49] Article 2(11) DGA.

[50] 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), Version 1.1., p.30.

[51] Cambridge Dictionary (<https://dictionary.cambridge.org/fr/dictionnaire/anglais/indeterminacy>).

[52] E.g., see BMW CarData Platform (<https://bmw-cardata.bmwgroup.com/thirdparty/public/car-data/overview>).

[53] Recital 28 DGA.

[54] *Ibid*.

[55] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance) OJ L 119, 4.5.2016, p. 1–88; cor. OJ L 127, 23.5.2018.

3.1.4. *Through technical, legal, or other means*

The three requirements examined above restrict the DGA's material scope. It is, however, worth noting that this scope is again expanded by its broad approach towards the means through which the data intermediation service occurs. Indeed, as long as the other three requirements are satisfied any data sharing falls within DGA's remit regardless of whether such sharing occurs through technical, legal, or other means.

It seems that even companies merely facilitating the signature of bilateral or multilateral legal contracts for data-sharing may be caught if they meet the requirements in Article 2(11). As a consequence, any type of company, potentially even law firms, which facilitate data-sharing between multiple parties even if only sporadically and without any technical sophistication, might be required to comply with Articles 11 and 12. The omission of a de minimis threshold also stands in contrast to the approach adopted by the draft Data Act, which exempts micro and small enterprises from its B2C and B2B data portability obligations.[56]

The DGA refers to 'technical, legal, or other' means. The definition of 'other' means remains somewhat unclear and this wording is presumably intended to keep the door open for future developments in this space with the unavoidable disadvantage of creating legal uncertainty.

3.1.5. *Article 10 DGA and its relationship with Article 2(11)*

While Article 2(11) generally defines what a data intermediation service is, Article 10 identifies which DISs are subject to the conditions set out in Articles 11 and 12.[57] This may invite interpretations that only providers of the subset of DISs mentioned in Article 10 are subject to the DGA.

Article 10 lists (i) intermediation services between data holders and potential data users, including technical services or other means needed to enable the former ;[58] (ii) intermediation services between data subjects and data users concerning the personal data of the former, including the technical services or other means needed to enable the latter;[59] (iii) intermediation services between natural persons and data users concerning the non-personal data of the former, including the technical services or other means needed to enable the latter;[60] (iv) services of data cooperatives.[61]

This invites speculation as to whether Article 10 really creates a subset of DIS (compared to the general definition in Article 2(11)) that are alone subject to Articles 11 and 12. Yet, the most likely explanation is that this was not the legislative intention, rather this provision needs to be understood in the context of the original draft of the DGA, which did not define DISs, and the precedent of now Article 10 (Article 9 draft DGA) was the only provision defying which data sharing services were subject to the DGA.

Yet, Article 10 will likely require judicial interpretations in the future as DIS may try to argue that they are outside the DGA's scope as not explicitly included in Article 10,[62] such as services of a data cooperatives not mentioned by Article 2(15),[63] namely those not exclusively constituted by data subjects, one-person undertakings, or SMEs and that do not have as their main objectives the task to support their members in the exercise of their data protection rights.[64]

3.2. *Data intermediaries' duties under the DGA*

The DGA imposes procedural and substantive requirements on data intermediaries with a focus on the former.

3.2.1. *Procedural requirements*

The DGA creates a notification framework under which intermediaries ought to send a notification to the competent authority of the Member State[65] of their main establishment[66] or, in the absence thereof, where their legal representative is based.[67] In some ways, this notification duty constitutes an interesting *revirement* in EU data law as data protection law previously contained obligations to notify data processing activities that have been abolished by the GDPR as this had become unmanageable in light of the swelling processing of personal data in all areas of life.

The notification takes the form of a simple declaration of the intention to provide services listed in Article 10 and has to include: (a) the provider's name; (b) its legal status, form, ownership structure, relevant subsidiaries and, where registered in a trade or other similar public national register, registration number; (c) the address of its main establishment in the Union and eventual secondary branch(es) or, in the absence thereof, the address of the legal representative; (d) a public website where complete and up-to-date information on the provider can be found; (e) the provider's contact persons and details; (f) a description of the service it intends to provide as well as its legal qualification under Article 10; (g) the estimated date for starting the activity, if different from the notification date.[68]

Data intermediaries are not dependant on an administrative decision authorising their activities as a simple notification is sufficient. This presents the benefits of a compulsory

[56] Article 7 dDA.
[57] Article 10(1) DGA.
[58] Article 10(1)(a) DGA.
[59] Article 10(1)(b) DGA.
[60] Article 10(1)(b) DGA.
[61] Article 10(1)(c) DGA. For a critique of the vagueness of the definition of 'services of data cooperatives', see J. Baloup *et al.*, 'White Paper on Data Governance Act' (2021) CiTiP Working Paper 2021, 29, (<https://www.researchgate.net/publication/352690055_White_Paper_on_the_Data_Governance_Act>); EDPB-EDPS, *supra* n. 50, 32. Notably, despite Article 2(15)'s explicit aim is defining what services of data cooperatives are, it instead seems to define what a data cooperative is and qualifies as 'services of data cooperatives' any DIS offered by those subjects.
[62] Such an outcome could be achieved by interpreting letters (a)-(b)-(c) of Article 10 in relation to one another, as reciprocally dependent. We however reject this interpretation as excessively sophisticated, unsupported by the DGA's text, iterative evolution, and not mentioned in the academic literature. Furthermore, this interpretation would create excessive room for circumvention by excluding from DGA's scope an undefined set of DISs.
[63] Notably, the words 'services of data cooperatives' only appear in Article 2(15) and Article 10(1)(c) in the entire DGA's text.
[64] Recital 31 DGA.
[65] Recital 44 DGA.
[66] Recital 41 DGA.
[67] Article 11(11) DGA.
[68] Article 11(6) DGA.

regime, while confining the regulatory burden on market players. However, the DGA leaves the door open to additional future requirements.[69]

Once the notification has been issued and at the simple request of the provider, the competent authority shall investigate and confirm whether the data intermediary complies with Articles 11 and 12.[70] The exact depth of this investigation remains undefined. One possible reading would be that authorities only need to evaluate intermediaries' statements regarding, e.g. what technical, legal and organisational measures they use to prevent unlawful access to the data. Alternatively, authorities may be required to inspect this themselves through access to the data and technical infrastructure.[71] The exact depth of the required inspection will of course have far-reaching implications for the future shape of this legal regime as well as the resulting administrative and compliance costs.

Compliant DIS may then use the label 'data intermediation services provider recognised in the Union' in its logo and in their spoken and written communications both offline and online.[72] It is expected that this label will generate trust in data intermediation in the EU, which presumably justifies the costs for public authorities associated with the *ex ante* investigation. Whether this is a realistic expectation can, however, be debated as it appears questionable that such a label will in itself be sufficient to change current attitudes towards data-sharing.

Intermediaries further ought to have procedures in place to maintain a record of all intermediation activities,[73] ensure a reasonable continuity of their offering and, therefore, have sufficient guarantees in place to ensure data storage and access, or transfer to stored data also in case of insolvency.[74]

3.2.2. *Substantive requirements*

The main substantive requirement is the neutrality obligation in Article 12(1)(a), which requires that intermediaries only intermediate and not use data for other purposes. Similarly, metadata can only be used for the provision of the intermediation service as well as the 'development' thereof (presumably an improvement of the product they offer).[75] This prevents business models using vertical integration, such as where an entity makes internal data available to third parties and then develops a platform that incorporates data flows from third parties.[76] Economists have warned that although the neutrality obligation is intuitively appealing, it is unclear why it would contribute to functioning data markets given the lacking empirical evidence that the absence of neutrality is, in fact, the reason why data is at this stage not shared with intermediaries.[77] Rather, the evidence seems to suggest that data is not increasingly shared due to information asymmetries and lacking control mechanisms over data users' usage of data, both factors not addressed by the DGA.[78]

While data intermediaries cannot use data for purposes other than intermediation, they may include additional tools and services to the extent that they facilitate the exchange of data and provided that the additions were either explicitly requested or approved by the data subjects/holders.[79] Importantly, however, this prevents DIs from offering other add-ons, such as, for instance, analytics services, thus restraining DIs' ability to acquire a competitive edge over another. Additional services or tools may include temporary storage, curation, conversion, anonymisation and pseudonymisation. Where intermediaries provide tools for obtaining consent or permission from, respectively, data subjects and data holders, they must specify the third-country jurisdiction in which the data is intended to be used and provide equivalent tools to withdraw either consent or permissions depending on the circumstances.[80]

This entails that if an intermediary offers additional services, it must structurally separate those from intermediation through the creation of a separate legal entity to ensure neutrality.[81] This might offer an easy way out to circumvent the substance of the neutrality duty through the simple creation of separate legal entities. Judicial interpretations will thus have to define what the neutrality obligation effectively entails.

Intermediaries have to ensure the highest level of security when handling competitively sensitive information.[82] Indeed, although data sharing services are expected to create innovation and efficiencies, they could also restrict competition. This might be the case, for instance, where sensitive information is shared between competitors, when the data exchange enables hub-and-spoke cartels amongst downstream or upstream competitors, or when an exchange provides data crucial to compete in downstream markets. While Article 11(9) draft DGA demanded 'procedures to ensure compliance with EU and national rules on competition',[83] this was watered down in what is now Article 12(1)(l) due to the technical difficulties for intermediaries to guarantee that their activities respect competition law.[84] Notwithstanding, Article 12(1)(l) might still end up conflicting with other European projects and slowing down their realisation.

[69] Recital 40 DGA.
[70] Article 11(9) DGA.
[71] Article 12(1)(j) DGA.
[72] *Ibid*.
[73] Article 12(1)(o) DGA.
[74] Article 12(1)(h) DGA.
[75] Article 12(1)(c) DGA.
[76] A. Blankertz, L. Specht, 'What Regulation For Data Trusts Should Look Like' Steiftung Neue Verantwortung (2021), p. 12.
[77] Kerber, 'DGA - einige Bemerkungen aus ökonomischer Sicht', (Jan. 2021),(last accessed 21.09.2022).
[78] *Ibid*.
[79] Article 12(1)(e) DGA.
[80] Article 12(1)(n) DGA.
[81] Article 12(1)(a) and Recital 33 DGA.
[82] Article 12(1)(l) DGA.
[83] Article 11(9) draft DGA.
[84] Article 1(4), Article 12(1)(l), and Recital 37 DGA. The mismatch between Article 11(9) draft DGA and Article 12(1)(l) DGA is still visible in the misalignment between Article 12(1)(l) and Recital 37 DGA given that the latter was designed to mirror previous Article 11(9) draft DGA and out of negligence was not updated by the legislator when amending now Article 12(1)(l) DGA. Similarly on this, see H. Richter, *supra* n.7.

One such example is the tension existing between the DGA and GAIA-X. While GAIA-X exceptionally obtained a comfort letter from the Commission informally providing legal certainty over its compatibility with antitrust rules,[85] it is now unclear whether and how it can practically satisfy the security requirements of the DGA given the uncertainties and unclarity surrounding the latter.[86] CATENA-X, a sub-component of GAIA-X aimed at realising a data network ecosystem enabling collaboration and greater interoperability in the automotive industry, faces the same problem.[87] Whereas the CATENA-X project was approved by the Bundeskartellamt based on its innovative and pro-competitive potential, it is now questionable whether the Bundeskartellamt's requirements can be reconciled with those of Article 12(1)(l) for competitively sensitive information.[88] In fact, while the Bundeskartellamt did not impose specific modalities for the exchange of competitively sensitive information and allowed their exchange when they are 'absolutely necessary for the cooperation',[89] Article 12(1)(l) requires the highest level of security, whatever the latter may be, and does not circumscribe the situations in which competitively sensitive data-sharing is allowed.

Additionally, to avoid that intermediaries excessively manipulate data and extract value from it, they must prioritise the sharing of the data in their original format and allow their conversion into other formats only (i) to enhance interoperability within and across sectors; (ii) if requested by the data user; (iii) where mandated by Union law; or (iv) to ensure harmonisation with international or European data standards.[90]

A further substantive obligation is to make sure that access to their services is fair, transparent, and non-discriminatory (the so-called FRAND principles) for both data holders and users, including as regards prices and terms of service.[91] To diminish the risk of anti-competitive behaviours and lock-in strategies, the DGA further mandates intermediaries to take appropriate measures to ensure interoperability with other intermediation services.[92] At the same time, it leaves the consequences of such interoperability, namely the ability to combine datasets, open. The central question here is what liability different actors face where such combination results, for instance, in the ability to turn pseudonymous data into personal data through the acquisition of additional information.[93] The same ratio also lies behind the provision prohibiting data intermediaries to commercially bundle their services with additional services provided by either the same intermediary or a related entity.[94]

Moreover, DIS providers that offer services to data subjects shall act in their best interest when facilitating the exercise of their rights.[95] Notably, this duty goes further when the intermediary exchanges data between data subjects and legal persons as data users. Here, they 'bear fiduciary duty towards the individuals, to ensure that they act in the best interest of the data subjects'.[96]

Finally, intermediaries ought to have procedures in place to prevent fraudulent or abusive practices in relation to parties seeking access to data,[97] take measures to ensure a high level of security for the storage and transmission of non-personal data,[98] communicate eventual unauthorised access, transfers, or uses.[99]

4. The DGA's underlying assumptions and their potential unintended consequences

To better grasp the rationale behind the DGA as well as its future effects, it is not just important to understand its explicitly formulated rules but also their underlying implicit assumptions. This section makes the implicit explicit and evaluates the effect these norms will likely come to have on future interpretations of the DGA as well as the data (intermediation) economy more broadly.

4.1. *First assumption: a more decentralised data economy requires new middlemen*

The legislative assumption behind the DGA is that a more diversified, less concentrated, more contestable, and fair digital economy can only be realised through a new middleman: the neutral intermediary. This can be perceived as ironic given the multitude of criticisms directed towards digital intermediaries leveraging network effects voiced over the past years. At the same time, it may simply be a recognition that digital business models require network effects.[100]

Data intermediaries are assumed to increase trust in data-sharing and eliminate existing asymmetries of power and information in interposing themselves in a neutral fashion between data holders and users. The focus on centralised middlemen may, however, be outdated and harmful

[85] European Commission, Letter to Gaia-X (19.10.2021), (<https://gaia-x.eu/sites/default/files/2021-11/Letter%20to%20G>).
[86] H. Schweitzer *et al*., Data access and sharing in Germany and in the EU: Towards a coherent legal framework for the emerging data economy. A legal, economic and competition policy angle. Final report (July 2022); B. Falkhofen, Infrastrukturrecht des digitalen Raums, EuZW, 2021,787(794). On the unclarity of DGA's obligations, see J. Baloup *et al*., *supra* n.61, p.37.
[87] CATENA-X, for instance, would enable the development of new technologies allowing the traceability of car components, the measurement of their carbon footprint along the value chain, etc.
[88] Bundeskartellamt, First component for Gaia-X: Bundeskartellamt gives green light for establishing data network for automotive industry (Catena-X) (Press release of 24.5.2022), (<https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2022/24_05_2022_Catena.html>).
[89] *Ibid*.
[90] Article 12(1)(d) DGA.
[91] Article 12(1)(f) DGA.
[92] Article 12(1)(i) DGA.
[93] See, generally, M. Finck, F. Pallas, They who must not be identified—distinguishing personal from non-personal data under the GDPR, *International Data Privacy Law*, V.10(1), 2020, pp.11–36.
[94] Article 12(1)(b) and Recital 33 DGA.
[95] Article 12(1)(m) DGA.
[96] Recital 33, DGA.
[97] Article 12(1)(g) DGA.
[98] Article 12(1)(j) DGA.
[99] Article 12(1)(k) DGA.
[100] J. Laffont, P. Rey, J. Tirole. Network Competition: I. Overview and Nondiscriminatory Pricing The Rand Journal of Economics. 29: 1. DOI: 10.2307/2555814; J. Tirole. Economics for the common good (Princeton University Press (2017)).

to the achievement of the DGA's objectives. Indeed, over the last decade markets have tried to eliminate middlemen,[101] shorten supply chains and production pipelines,[102] reduce transaction costs,[103] and ultimately provide higher quality and cheaper services to consumers.

No technology is more closely associated with aspirations for a more decentralised digital world than blockchain, which promises to form trust amongst untrusting parties without the need for trusted intermediaries. There are indeed examples of blockchain-native data exchanges, which for instance use data decentralised organisations ('data DAOs') and represent datasets as non-fungible tokens that can be traded between wallets.[104] While blockchains bear the promise of decentralisation, there currently remain many centralised chokepoints in these protocols and related business models.[105] Whether this is an infant illness remains to be seen, yet the DGA may stifle innovation in this domain in contrast to EU efforts to create legal certainty for decentralised technologies elsewhere.[106]

A question that will inevitably emerge is whether different forms of blockchain-based data sharing will fall within the scope of the DGA at all.[107] Recital 28 explicitly excludes providers of cloud storage and data sharing software that only make available technical tools that do not aim to establish a commercial relationship between data holders and users nor allow DIS providers to acquire information about the establishment of such a commercial relationship.[108] Here a case-by-case analysis will be needed to determine whether a provider has awareness of the formation of commercial relationships. More generally, it will be interesting to see how courts interpret this provision as it is difficult to imagine scenarios in which software is created that allows for the formation of commercial relationships between data holders and users but was not intended to do so (and intent will be difficult to prove).

The DGA thus entrenches a specific techno-organisational form of data access and use that may, down the line, turn out to be as misguided as the Database Directive has turned out to be in relation to data (assuming that the economically valuable part is the database, not the data it contains).[109] This likely disincentives experimentation with alternative data-sharing models so that the focus on middlemen might prevent the emergence of alternative models that would ultimately be better suited to incentivise its data-sharing objectives in the mid-to-long term.

4.2. *Second assumption: data intermediaries are aware of the characteristics of the data they intermediate*

The DGA assumes that all data intermediaries are aware of the characteristics of the data they intermediate. It indeed requires that DISs providers adopt specific measures for specific kinds of data. Beyond, other supranational norms mandate the same. For example, the GDPR imposes various obligations on DIs qua controllers in relation to personal data.

This emerges, for instance, from Article 12(1)(l), which demands that intermediaries ensure an 'appropriate level of security' for non-personal data and 'the highest level of security for the storage and transmission of competitively sensitive information'.[110] Indeed, by demanding specific behaviours depending on the type of data handled, e.g. non-personal data or competitively sensitive information, Article 12 postulates that DIs ought to be aware of the quality of the data they intermediate. Yet, not all existing data intermediaries can effectively comply with similar provisions. This is the case, for instance, for those DIs that do not centrally store data or only centrally store encrypted data that they have no decryption keys for. Similarly, entities that only make a technical intermediation structure available appear unable to comply with these postulates.[111]

Similar problems also arise in respect of personal data. This is because, as it will be further explained below, when intermediaries intermediate personal data, they qualify as data controllers and, as such, are subject to comply with the GDPR.[112] As a consequence, DIS providers need to determine whether they intermediate personal data in order to be able to comply with their obligations under the GDPR, such as respect for the core data protection principles,[113] provide data subjects with the information required under Articles 13 and 14 GDPR, exercise the documentation duties related to the accountability principle,[114] and facilitate the exercise of data subjects' rights.

Crucially, Article 12 leaves open whether DIs need to independently determine the type of data they handle or whether the data holder needs to make indications in this respect. Yet, this central point impacts DIs'operation and their potential liabilities. While independent verification by the DIs will be difficult to implement for those DIs which have no direct access to the data they intermediate, relying on outside assessments

[101] L. Grassi, D. Lanfranchi, A. Faes, F.M. Renga, 'Do we still need financial intermediation? The case of decentralised finance – DeFi', *Qualitative Research in Accounting & Management*, (2022), Vol. 19(3), pp. 323-347. https://doi.org/10.1108/QRAM-03-2021-0051; C.W. Cai, 'Disruption of financial intermediation by FinTech: a review on crowdfunding and blockchain', *Accounting & Finance* 58 (2018) 965-992.

[102] European Central Bank, 'Global value chains: measurement, trends and drivers', Occasional Paper Series, (Jan. 2022), No.289, (last accessed 20.09.2022).

[103] J. Clark, J. Busch, 'The Economic Benefit of a Shortened Supply Chain, A Case Study Involving Molded Composite Parts', *SAE Technical Paper* 2002-01-2041, 2002.

[104] See, e.g. Ocean Protocol (<https://oceanprotocol.com>).

[105] M. Marlinspike, My first impressions of web3, (Jan. 2022), (last accessed 21.09.2022).

[106] E.g. see Proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-assets, and amending Directive (EU) 2019/1937, COM/2020/593 final.

[107] Concerning GAIA-X, for instance, Schweitzer *et al., supra* n.86, note that there is 'some general uncertainty in the industry about the DGA's scope of application on GAIA-X- federated applications.'

[108] Recital 28 DGA.

[109] Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases, OJ L 77, 27.3.1996, p. 20–28.

[110] Article 12(1)(l) DGA.

[111] Article 2(11) DGA.

[112] Article 1(3) DGA.

[113] Article 5 GDPR.

[114] Recital 30 GDPR.

would risk reducing the utility of Article 12 as DIs have no incentive or, depending on circumstances, ability to verify what data holders declare and the ultimate security of their DISs may be compromised as they might inadvertently treat competitively sensitive information as non-competitively sensitive data and vice-versa. Needless to say, the first option is also exponentially more costly for DIS providers.

4.3. *Third assumption: even though data intermediaries are likely to (re-)create some of the tech giants' most criticised features, the DGA will be able to tame them*

The DGA seems to assume that despite data intermediaries being likely to (re-)create the tech giants' monopolistic nature, it can nevertheless tame them. Indeed, after an initial phase of more or less fair and open competition, certain data intermediaries will likely acquire substantial market power with regard to certain typologies of data, industries, or sectors.[115] DIs can then leverage their dominance in a given data market to others to expand their reach and improve the overall quality of their services. This would indeed be possible because Article 12(1)(b) only prohibits bundles of services but remains silent with regard to bundles of data.

The DGA implements various measures designed to prevent that DIs create massive network and lock-in effects, economies of scale, and high switching barriers, including the neutrality duty, the bundling prohibition, the interoperability duty, the duty to grant access on FRAND terms and the duty to preserve the original format as default. It is noteworthy that these mechanisms mirror the Digital Markets Act's instruments to rein in tech giants, such as FRAND access conditions,[116] prohibition of bundling,[117] and interoperability duties.[118]

On the one hand, the DGA's foresight that DIs will become data monopolies, at least in their respective sectors, just seems realistic in light of the experience to date that concentration is the most likely outcome in business models that are digital and require network effects. The DGA also has a geopolitical dimension in that it explicitly encourages the creation of EU-based DIs, which adhere to European norms, after largely missing out on the benefits of the Web.2 era. Thus, even if winner-takes-all or winner-takes-most market actors will emerge, the EU benefits to the extent that they reside in, and provide data to, the internal market.

At the same time, such concentration will undermine the legislative goal of realising a less concentrated, more diversified EU data economy. Indeed, its various measures might indeed contribute to lowering competition in data markets as it not only creates compliance costs that smaller DIs may struggle to accommodate, and, second, the neutrality duty prevents DIs from acquiring a competitive edge through add-on services to data that may lead to a more diversified data economy with more players specialised in specific services.

4.4. *Fourth assumption: strongly regulated data intermediaries are economically viable*

Finally, the DGA assumes that neutral intermediaries can successfully compete in data markets through alternative business models that, inter alia, are not vertically integrated.[119] Yet, while the DGA introduces a considerable regulatory burden on data intermediaries, it does not provide any counterbalancing regulatory benefit to ensure their economic viability vis-a-vis vertically integrated competitors not subject to its requirements. Whereas it certainly is not a given that each regulatory obligation needs to be counterbalanced by a symmetric regulatory advantage, the DGA imposes considerable costs on those subject to its regime, whereas other 'intermediaries' are spared these costs, providing the latter with a competitive advantage.

If the neutrality duty is interpreted narrowly (as it seems it should), data intermediaries will likely not be able to compete with the large tech platforms (regarding the kinds of data these platforms have) if the latter decide to enter data intermediation markets. Through the seemingly insurmountable amount of data they collect and aggregate, tech giants could easily offer data services equivalent to DISs without being simultaneously limited by the neutrality duty. They could, for example, offer equivalent services for free through cross-subsidisation strategies, or higher quality services by exploiting the inferences arising from their internal dataflows. Whether the offering of services free of charge will in itself be sufficient to bring DISs outside the scope of the DGA will, as outlined above, hinge on judicial interpretations of the concept 'commercial' in Article 2(11). In any event, large online platforms could offer only access to their own data as this will fall outside the scope of Articles 2(11) and 10 (although this will of course be a more limited collection of data than that potentially made available through the DGA).

Similarly, the requirement to grant access at FRAND conditions might excessively undermine intermediaries' market viability. Although FRAND is a blurred and often litigated concept,[120] it is hard to see why data intermediaries should not be

[115] For an analysis of the factors that could lead to such outcomes in data markets, see P. Koutroumpis, A. Leiponen, L. DW Thomas, Markets for data, *Industrial and Corporate Change*, 2020(29)3, p.645–660.

[116] E.g. Article 6(5),(11), and (12) DMA.

[117] E.g. Article 5(7)-(8) and Article 6(3) DMA.

[118] E.g. Article 6(7) and Article 7 DMA.

[119] Surviving in data intermediation services, however, is not easy and multiple instances of failed data platforms already exist. Remarkable is the case of Microsoft Azure DataMarket, which was disbanded in March 2017 (<https://social.msdn.microsoft.com/Forums/en-US/1005630f-a6da-4b00-ad4e-adfc968d9416/azure-datamarket-to-retire->). On this, see also V. Markl, Project Final Report: Data Supply Chains for Pools, Services and Analytics in Economics and Finance, (2014), TU Berlin: Berlin, Germany; P. Carnelley *et al.*, 'Europe's data marketplaces—current status and future perspectives,' in European Data Market SMART 2013/0063 D.39. IDC, (2016), (<https://datalandscape.eu/data-driven-stories/europe's-data-marketplaces--current-status-and-future-perspectives>).

[120] Case C-170/13, *Huawei Technologies Co. Ltd v. ZTE Corp. e ZTE Deutschland GmbH*, 16 July 2015, ECLI:EU:C:2015:477. For an overview of the divergent approaches materialised in the aftermath of the ECJ Huawei judgement, see *Sisvel v Haier*, District Court of Duesseldorf, 3 November 2015, Case No. 4a O 93/14; *Sisvel v Haier*, Higher District Court of Duesseldorf, 30 March 2017, Case No. I-15

allowed to price differentiate, refute their services, or somehow restrict the usability of those services when interacting with tech giants given the competitive threat the latter may represent for the former.

Thirdly, the DGA requires that DIs have in place adequate technical, legal, and organisational measures: (i) to prevent fraudulent or abusive access to data from parties seeking access through their services; (ii) to ensure a high level of security for the storage and transmission of non-personal data; (iii) to prevent transfer or access to non-personal data that is unlawful under Union law. Although these requirements produce clear benefits for clients and also improve DIs' competitiveness, the exact meaning of these provisions is still unclear. If these provisions will be interpreted expansively, data intermediaries will be subject to security obligations that resemble those of data controllers under Articles 24, 25, and 32, GDPR, and differently from the latter, the former do not vary their severity based on 'the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons'.[121] Crucially, these provisions also apply where intermediaries only handle non-personal data. This creates compliance costs for intermediaries that other actors offering data access are not subject to.

5. Data intermediaries in the wider context of EU data law

The impact of the DGA will also be shaped by its interactions with the broader data law framework (Fig. 2). The former indeed does not apply in a vacuum as providers need to abide by a wider panoply of EU and national norms on data.

5.1. *Data intermediaries and the GDPR: are data intermediaries data controllers?*

Regarding the relationship between the DGA and the GDPR, the first question that needs to be resolved is whether a DI is a data controller.[122] Recital 35 DGA affirms the obvious that where DIs are data controllers, they are bound by data protection law.[123]

The legal qualification of whether a data intermediary is a data controller is to be evaluated with reference to the GDPR. Indeed, as per Article 1(3) DGA, the DGA is without prejudice to the application of the GDPR and where conflicts between both norms arise, the former prevails.

Article 4(7) GDPR sets out a functional test of control. It provides that a legal or natural person, which 'alone or jointly with others, determines the purposes and means of the processing of personal data'[124] (the purposes essentially are the 'why' and the means the 'how' of processing[125]) are controllers. The practical implementation of this legislative test has proven to be complex and riddled with uncertainty.[126] Together with technical developments that imply that ever more parties exercise some, albeit often only a small, degree of control over the purposes and means of processing, it has led to an inflation of potential data controllers.[127]

Whereas Article 4(7) reads as if the 'means' and 'purposes' are two criteria of equal standing, decision practice has shown the primacy of the purposes criterion.[128] This implies that parties that have a motivation to process personal data but exercise very little actual influence over the modalities of this processing are controllers. This is undesirable as it attributes duties to entities that they cannot comply with for lack of access to and control over the data as well as the technical infrastructures used to process it.[129]

The relevant criterion to determine whether data intermediaries are controllers is thus whether the former exercises control over the purposes and means of processing – purely as a result of intermediating the data.[130] This needs to be evaluated on a case-by-case basis. In general, it can be presumed that data intermediaries oftentimes influence the means of processing as their key service is the creation of a techno-economic infrastructure that enables the intermediation of data between a data holder and a prospective user.[131] Where the means chosen to enable intermediation are technical, the intermediary can be presumed to influence the means of personal data processing. Importantly, this conclusion also holds true where data intermediaries have no physical access to the data. Indeed, the CJEU's 2018 landmark ruling in *Jehovan Todistajat* established that it is not necessary for a controller to have physical access to the data in order to qualify as a controller. An interesting question emerges as to whether the determination of the 'legal or other means' also constitutes a determination of the means under data protection law.

In any event, the determination of the means alone is insufficient to trigger the qualification as a controller. Rather, Art 4(7) portrays the controller as an entity that determines the means *and* purposes of control and the CJEU's recent case law attributes higher weight to the purposes criterion. This then leads to the determinative question of when a data interme-

U 66/15; *Sisvel v. Haier*, Federal Court of Justice, 5 May 2020, Case No. KZR 36/17; and *Unwired Planet v. Huawei Technologies*, [2017] EWHC 711 (Pat), 5 April 2017, para 744-747, later confirmed by the Court of Appeal of England and Wales first (*Unwired Planet International Ltd. v. Huawei Techs. Co. Ltd.*, case number A3/2017/1784, EWCA Civ 2344 (2018), para 56) and the U.K. Supreme Court later (*Unwired Planet v. Huawei Technologies*, [2020] UKSC 37, 26 August 2020, para 149-158).

[121] Article 32 GDPR.

[122] In data protection law, the data controller is the natural or legal person liable to comply with data protection rules.

[123] Recital 35 DGA.

[124] Article 4(7) GDPR.

[125] EDPB Guidelines 07/2020 on the Concepts of Controller and Processor in the GDPR (July 2021), p.3.

[126] M. Finck, Cobwebs of control: the two imaginations of the data controller in EU law (2021) 4 International Data Privacy Law, Oxford Academic, pp. 333-347.

[127] *Ibid*.

[128] See Case C-2010/16, *Wirtschaftsakademie Schleswig-Holstein* (2018), ECLI:EU:C:2018:338, paras 26-28; Case C-25/17 *Jehovan todistajat* (2018) ECLI:EU:C:2018:551; Case 131/12 *Google Spain* ECLI:EU:C:2014:31, paras 28-41; Art 29 Working Party, Opinion 1/2010 on the concepts of 'Controller' and 'Processor' (WP 169) 00264/10/EN, 14; EDPB, *supra* n.124.

[129] M. Finck, *supra* n.125.

[130] Sharing personal data amounts to 'processing' personal data under Article 4(2) GDPR.

[131] Article 2(11) DGA.

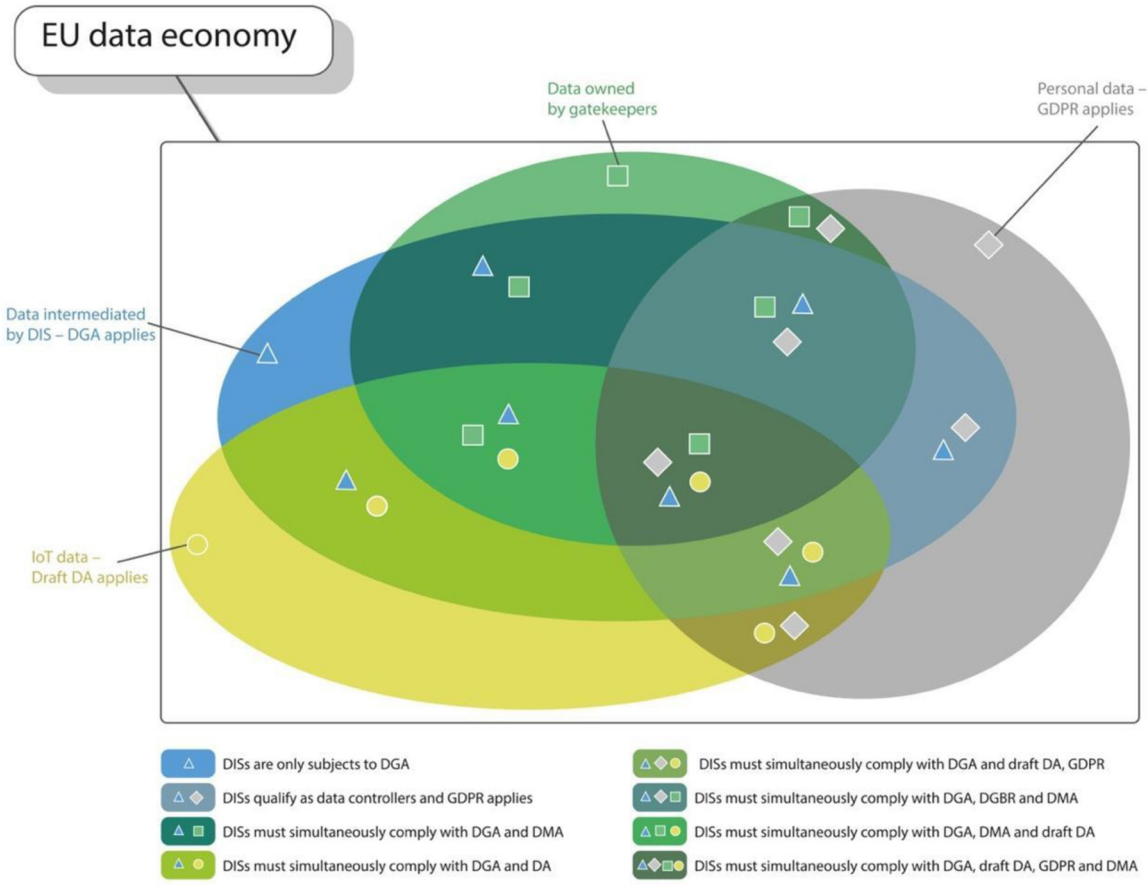

Fig. 2 – DGA's intersection with selected EU data acts.

diation service provider determines the purposes of data processing.

Intuitively, the DGA's neutrality obligation might be understood as indicating that intermediaries do not influence the purposes of processing. The neutrality obligation indeed applies 'with regard to the data exchanged between data holders or data subjects and data users' so that DIs can only intermediate and not 'use the data exchanged for any other *purpose*'.[132] In fact, data collected 'for the *purpose* of the provision of the data intermediation service (…) shall be used only for the development of the data intermediation service'.[133] Article 12(1)(a) DGA specifies that the 'data intermediation services provider shall not use the data for which it provides data intermediation services *for purposes other* than to put them at the disposal of data users'.[134] Although we cannot be sure of the legislative intent behind this formulation, it would be unfortunate[135] if this notion were to be given different interpretations across EU data law. The DGA hence explicitly qualifies intermediation as a purpose, and even if the neutrality obligation would invite a different conclusion, it could not change the definitional test under the GDPR as indeed Article 1(3) DGA sets out that where conflicts between the DGA and the GDPR arise, the latter prevails.

Intermediation itself is thus a purpose of personal data processing.[136] This derives both from interpretations of the purposes criterion under data protection law as well as from the text of the DGA itself. As a consequence, the provider is a data controller in particular where the intermediary also provides technical means of intermediation. This is also in line with recent decisional practice regarding cloud computing providers.[137]

There are, moreover, explicit textual indications in the DGA that indicate that data intermediaries are controllers. Article 12(1)(m) refers to the DI's duty to facilitate the exercise of data subject rights, whereas Article 12(1)(n) refers to them collecting data subjects' consent. Although control always needs to be determined on a contextual case-by-case basis, it must be concluded that most DISs providers processing personal data are data controllers. Whether this is desirable from a policy

[132] Recital 33 DGA.
[133] Article 12(1)(c) DGA.
[134] Article 12(1)(a) DGA.
[135] Though not unprecedented, see e.g., different definitions of the data holder under the DGA and the draft Data Act.

[136] A related question of crucial importance that cannot be exhaustively examined here is whether 'intermediation' as a purpose complies with the GDPR's requirements regarding purpose specification and compatible use.
[137] The Slovenian DPA indeed held in 2022 that cloud computing providers are data controllers, (<https://gdprhub.eu/index.php?title=IP_(Slovenia)_-_0612-23/2019/19&mtc=today>) (last accessed 21.09.2022).

perspective can be debated – in general,[138] but also specifically with respect to the DGA. This debate highlights the clash of policy objectives between the GDPR and the DGA. Whereas the former seeks to, through a broad personal and material scope of application, minimise the risks that arise where personal data is processed by creating a qualified prohibition on the processing of personal data, the latter is a legal framework explicitly designed to incentivise the processing of more (personal) data in the internal market. The interplay between the DGA and the GDPR also again raises the question, examined above, to what extent DIs need to be aware of the quality of the data they are intermediating. As controller duties under the GDPR only arise in relation to personal data, it appears that DIs will need to be able to determine what data they intermediate is personal data and what data is not. Yet, in practice, this will often be difficult to achieve.

5.2. *Data intermediaries and the draft Data Act*

The draft Data Act ("dDA")[139] contains general rules concerning access to and sharing of personal and non-personal data, while leaving the door open for potential future sector-specific regulations. It inter alia establishes provisions to: (i) allow users of connected devices to gain access to data generated by these devices and/or to share such data with third parties ;[140] (ii) measures to shield SMEs from unfair contractual terms by preventing abuses of contractual imbalances in data sharing contracts ;[141] (iii) enable customers to effectively switch between different cloud data-processing providers ;[142] (iv) set essential requirements for operators of data spaces and data processing service providers regarding interoperability and smart contracts. Whereas a detailed discussion of the draft Data Act is outside the scope of the present paper, we highlight potential interplays between both texts and ponder their impact on data intermediaries.

5.2.1. *The draft Data Act as an additional avenue to acquire data for data intermediaries*

In facilitating B2C and B2B sharing of data generated by the use of a product[143] or related service[144] between data holders and data recipients, the Data Act creates a mandatory regime of data-sharing for data holders that fall within its scope.[145]

DIs can qualify as data recipients under the dDA as its Article 2(7) provides that 'data recipient means a legal or natural person, acting for purposes which are related to that person's trade, business, craft or profession, other than the user of a product or related service, to whom the data holder makes data available, including a third party (…)'. Indeed, Recital 35 dDA explicitly recognises that a DI can be a third party.[146]

To access data as a recipient, DIs need the consent of the data user that the data relates to. Access then needs to be granted without undue delay, free of charge to the user, and in exchange of a reasonable compensation to the data recipient.[147] The data made available needs to be of the same quality as is available to the data holder and, where applicable, be made available continuously and in real-time.[148]

The fact that DIs can be data recipients has numerous implications. *First*, and obviously from the perspective of data protection law, where a user such as a DI is not a data subject (i.e. a legal person), any personal data generated by the use of a product or related service shall only be made available where there is a valid legal basis under Article 6(1) GDPR and, where relevant, also in compliance with Article 9 GDPR's conditions for special categories of data.[149] The dDA, indeed, does not create a new legal basis for 'the data holder to provide access to personal data or make it available to a third party when requested by a user that is not a data subject (…)'.[150]

Second, the dDA provides that the data recipient 'shall not make the data it receives available to another third party (…) unless this is necessary to provide the service requested by the user'.[151] Considering that DISs providers can only acquire data for intermediation, the user needs to explicitly request intermediation as a service.[152] It is in this respect unclear whether the data user needs to authorise the intermediation service per se, irrespective of subsequent use, or also authorise every single subsequent use of the shared data. While the first interpretative option would be much more favourable in achieving the DGA's underlying aim of bolstering data-sharing, it also clashes with the spirit of Article 6(2)(c) dDA, which is to restrain an unlimited circulation of a given data user's data.[153]

---

[138] M. Finck, *supra* n.125.

[139] 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.

[140] Chapters II and III dDA.

[141] Chapter IVdDA.

[142] Chapter VI dDA.

[143] Article 2(2) dDA.

[144] Article 2(3) dDA.

[145] Notably, although Article 2 defines the concepts of 'data', 'product' and 'related service', it does not define what data can be considered as 'generated' by a product or a related service. On the consequences of this opaqueness, see see J. Drexl *et al*, Position Statement of the Max Planck Institute for Innovation and Competition of 25 May 2022 on the Commission's Proposal of 23 February 2022 for a Regulation on harmonised rules on fair access to and use of data (Data Act), para 22, (<https://www.ip.mpg.de/fileadmin/ipmpg/content/stellungnahmen/Position_Statement_MPI_Data_Act_Formal__13.06.2022.pdf>).

[146] Recital 35 dDA. Even more explicitly, see Recital 28 and 29 of the version of the dDA approved by the European Parliament on 14th March 2023 (See Amendments adopted by the European Parliament on 14 March 2023 on the 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)0068 – C9-0051/2022 – 2022/0047(COD).

[147] Article 9 dDA.

[148] Article 5(1) dDA.

[149] Article 5(6) dDA.

[150] Recital 24 dDA.

[151] Article 6(2)(c) and Recital 33 dDA.

[152] Critically on Article 6(2)(c)'s excessive permitted uses of IoT data, as it would allow users to share their data to any third party also for the sole purpose of generating income, see J. Drexl *et al*, *supra* n.144, para 14.

[153] Notably, Recital 29 dDA, EP 14th March 2023 version, states that 'The user should have the right to share non-personal data with third parties for commercial purposes. Upon the agreement with the user, and subject to the provisions of this Regulation, data recipients should be able to transfer the data access rights granted by the user to third parties, including in exchange for compensation. Data intermediation services [as regulated by Regulation

A reasonable middle ground between these two options would be that of amending Article 6(2)(c) dDA to exceptionally allow third-party data sharing only via EU certified data intermediaries for limited purposes.[154]

Third, the dDA establishes that the data recipient 'shall not use the data it receives to develop a product that competes with the product from which the accessed data originates or share the data with another third party for that purpose'.[155] Data intermediaries thus cannot intermediate data obtained under Article 5(1) dDA with data recipients that want to develop a product competing with the one of the data holders that provided the data.[156] Importantly, however, intermediaries will generally not be aware of the subsequent use of data made after the intermediation stage, and, depending on their precise configuration, the data that they are intermediating. This relates back to the broader question of the degree of awareness DISs providers need to have regarding the data they are intermediating.

5.2.2. *The draft Data Act as a potential barrier to data intermediaries' success*

The dDA imposes additional regulatory duties on DIs qua 'data holders'[157] or 'providers of data processing services'.[158]

A *Are DIs Data Holders under the dDA?*

The definition of the 'data holder' under the dDA is of high controversy in the ongoing legislative process, yet will be very significant for the Act's relevance for DISs providers. Article 2(6) dDA defines the 'data holder' as a legal or natural person 'who has the right or obligation (…) or in the case of non-personal data and through control of the technical design of the product and related services, the ability, to make available certain data'.[159] This indicates that the concept of the data holder may be broader than just manufacturers of IoT products and suppliers of related services.

This expansive reading finds support in Article 1(1), which announces that the dDA 'lays down harmonised rules on making data generated by the use of a product or related service available to the user of that product or service, on the making data available by data holders to data recipients'.[160] Similarly, Article 1(2) specifies that it applies to both 'manufacturers of products and suppliers of related services placed on the market in the Union and the users of such products or services' ;[161] as well as 'data holders that make data available to data recipients'.[162]

Pursuant to this interpretation, data intermediaries qualify as data holders and need to comply with the obligations the DA establishes for the latter. This implies that DIs, to the extent that they own data generated by the use of a product or related service, will be required (upon a simple user request or upon a request made by a third-party acting on behalf of a user) to make available those data without undue delay, free of charge to the data user who generated those data,[163] or for a compensation that could not exceed the direct costs needed to make the data available whether the data recipient is a SMEs,[164] or for a compensation that nevertheless must be 'reasonable' in all residual circumstances.[165] Needless to say, this presents compliance costs and liability risks for DIs.

At the same time, an alternative reading of Article 2(6) dDA has been suggested, namely that the concepts of data holders and manufacturers overlap. This reading hinges on the fact that Article 2(6) relies on the 'ability' to make the data available and then links such an ability to the 'control of the technical design of the product and related service'.[166] Accordingly, since normally only manufacturers of products and suppliers of related services are in a position to have such a technical control, only the latter are data holders under the dDA and shall comply with its obligations. This would exempt data intermediaries from the DA. However, while such a scenario might look appealing at first glance from data intermediaries' perspective, a better look suggests otherwise. In such a scenario, indeed, it will be more rational for potential data users to have recourse directly to data holders under the DA instead of DIs under the DGA anytime possible. The former indeed must provide the data, upon a simple user request or on its behalf,[167] without undue delay, of the same quality as available to themselves, continuously and in real-time (where applicable),[168] and, more importantly, for a compensation that in best case scenarios must be 'reasonable'[169] and if the data recipi-

(EU) 2022/868] may support users or data recipients in establishing a commercial relation for any lawful purpose on the basis of data falling within the scope of this Regulation. They could play an instrumental role in aggregating access to data from a large number of individual potential data users so that big data analyses or machine learning can be facilitated, as long as such users remain in full control on whether to contribute their data to such aggregation and the commercial terms under which their data will be used.'

[154] Similarly, see H. Richter, *supra* n.7, p.12; J. Drexl *et al*, *supra* n.144, para 338.

[155] Article 6(2)(e) draft DA.

[156] Note that while data circulated under the dDA's regime cannot be used to develop a competing product, they can be used to develop competing aftermarket services. Recital 28 dDA explicitly recognises data users' right to share their data with third parties 'offering an aftermarket service that may be in competition with a service provided by the data holder, or to instruct the data holder to do so'.

[157] Generally, the legal or natural person who has the right, obligation, or the ability to make available certain data.

[158] Generally, a PDPS provides a digital service to a customer which enables on-demand administration and broad remote access to a scalable and elastic pool of shareable computing resources.

[159] Article 2(6) dDA.

[160] Article 1(1) dDA.

[161] Article 1(2)(a) dDA.

[162] Article 1(2)(b) dDA.

[163] Article 5(1) dDA.

[164] Article 9(2) dDA.

[165] Article 9(1) dDA.

[166] J. Drexl *et al*, *supra* n.144, para 62, which however called for greater clarity in the recitals.

[167] Recital 31 dDA.

[168] Article 5(1) dDA.

[169] Article 9(1) dDA. Recital 46 dDA states the relevant factors to assess the reasonableness of a price. Recital 45 dDA, then, specifies which costs should be considered as direct costs. On this, see also G. Monti, T. Tombal, I. Graef, Study for developing criteria for assessing "reasonable compensation" in the case of statutory data access right. Study for the European Commission

ent is a SME,[170] costs cannot exceed those 'directly related to making the data available to the data recipient and which are attributable to the request.'[171] Recourse to DIs will therefore likely result in higher costs.[172]

The above overview highlights that the definition of the 'data holder' under the dDA remains far from settled and it remains to be seen what formulation is adopted in the final text coming out of the trilogue in order to determine the dDA's significance for DISs providers.[173]

A *Data intermediaries as 'providers of data processing services'*

Chapters VI, VII, and VIII of the dDA, respectively, (i) facilitate switching between providers of data processing services, (ii) mandate a series of technical, legal, and organisational measures to prevent unlawful international access to non-personal data held in the Union; (iii) specify the essential requirements to be complied with by operators of data spaces and providers of data processing services to enhance the interoperability of their data, data sharing mechanisms, and services,[174] including smart contracts.[175]

These provisions apply to providers of data processing services ("PDPS") offering such services to customers in the Union.[176] Some DISs providers may qualify as PDPS. Article 2(12) dDA, defines a 'data processing service' as a 'digital service other than an online content service as defined in Article 2(5) of Regulation (EU) 2017/1128, provided to a customer, which enables on-demand administration and broad remote access to a scalable and elastic pool of shareable computing resources of a centralised, distributed or highly distributed nature'.[177] Recital 71 dDA further states that such services include networks, servers or other virtual or physical infrastructure, operating systems, software, including software development tools, storage, applications and services. Given the broad scope of the definition, some DISs providers qualify as PDPS, particularly where they offer data sharing services and some additional data processing services (e.g. temporary cloud storage).[178]

Consequently, DISs providers that qualify as PDPS bear additional switching and interoperability obligations that may weaken their competitiveness. They need to facilitate customers switching while simultaneously improving their interoperability. This prevents them from adopting business strategies aimed at locking-in customers and generating network effects. Instead, data intermediaries' existing customers can easily switch to competing PDPS that might not be data intermediaries, whereas data intermediaries' will struggle to attract new customers that might achieve equivalent benefits through the interoperability between their non-DI PDPS and the data intermediary whose access is needed.[179]

5.3. *Data intermediaries and the Digital Markets Act*

Through the Digital Markets Act ("DMA")[180] the EU aims at ensuring contestable and fair markets in the digital sector.[181] In this sense, the DMA is expected to rein in a small number of large undertakings, so-called 'gatekeepers', which have established an entrenched and durable power position within the internal market.

The DMA, without prejudicing the GDPR[182] and while complementing competition rules,[183] was adopted to mitigate the latter's shortcomings, such as: (i) the excessive length, complexity, and cost of investigations in digital sectors; (ii) the reactive, ex post, and, therefore, strategically limited function that proceedings can play in addressing the structural challenges posed by digital gatekeepers to the effective functioning of the internal market; (iii) the modest almost non-existent results obtained so far by remedies. Therefore, the DMA was designed to regain contestability and fairness in those digital services characterised by high entry barriers, intense economies of scale and scope, robust network and lock-in effects, scarce interoperability, and lack of multi-homing. Against this backdrop, the DMA establishes a one-size-fits-all set of ex-ante and self-applicable obligations and prohibitions that apply across a plurality of firms and services irrespective of their business models[184] and any actual, potential, or

Directorate-General Justice and Consumers, Final Report, (2022), JUST/2021/PR/SCON/CIVI/0122.

[170] As defined in Article 2 of the Annex to Recommendation 2003/361/EC.

[171] Article 9(2) dDA.

[172] Article 8(1) and Recital 38 dDA.

[173] Notably, the European Parliament's version of the dDA, *supra* n.145, considerably modified the original definition of data holder. Updated Article 2(6) dDA states that: 'data holder means a legal or natural person, who has accessed data from the connected product or has generated data during the provision of a related service and who has the contractually agreed right to use such data, and the obligation, in accordance with this Regulation, applicable Union law or national legislation implementing Union law to make available certain data to the user or a data recipient'.

[174] Recital 79 dDA.

[175] Recital 80 dDA.

[176] Article 1(2)(e) dDA.

[177] Article 2(12) and Recital 71 dDA.

[178] Similarly, see J. Drexl *et al*, *supra* n.144, paras 172-173. Noteworthy, moreover, is also the updated version of Recital 71 dDA, European Parliament's version, *supra* n.145. While the updated version of Recital 71 dDA explicitly excludes online platforms as defined in point (i) of Article 3 of the Digital Services Act and online content services as defined in Article 2(5) of Regulation 2017/1128 from the definition of providers of data processing services within the meaning of the dDA, it does not mention DIs. This non-explicit exclusion of DIs seems to further corroborate the possibility that some DIs are PDPS.

[179] Notably, the fact that Art.12(1)(i) DGA mandates interoperability between DIs does not diminish the value of the argument as the dDA mandates interoperability between a wider spectrum of subjects, including but not limited to DIs.

[180] 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), OJ L 265, 12.10.2022, p. 1–66.

[181] Article 1(1) DMA.

[182] Recital 12 DMA.

[183] See Recitals 10 and 11 DMA. Importantly, while competition rules have their own enforcement space, their application should not affect the obligations imposed on gatekeepers by the DMA and their uniform and effective application in the internal market.

[184] The DMA partially addresses its one-size-fits-all problematic character with Article 9(1), which allows gatekeepers to demonstrate that compliance with a specific DMA obligation would en-

presumed effect on competition of the conduct prohibited or mandated to gatekeepers.[185]

The DMA and the DGA thus share the common policy objective of promoting a new, more diversified, less concentrated, more contestable, and fair digital economy. Accordingly, the DMA and the DGA have some positive synergies. The DMA, indeed, includes several provisions which could display beneficial effects for DISs providers. Relevant, in this sense, are, amongst others, those DMA provisions mandating effective data portability,[186] FRAND access conditions,[187] interoperability duties.[188] Notwithstanding, the interplay between the two Acts may result in unintended consequences harmful to the attainment of the common objectives. First, both acts fail to prohibit gatekeepers from offering intermediation services outside the scope of the DGA. Second, the DMA might encourage gatekeepers' entrance in markets for data intermediation. Third, the DGA's neutrality duty might prove ineffective where gatekeepers own data intermediaries.

5.3.1. *Gatekeepers can free-ride data intermediation markets*

Firstly, the DMA does not prohibit gatekeepers from offering services equivalent to DISs without the need to comply with DGA's regime. As noted above, this risks compromising the market viability of DIs. This could happen because gatekeepers, on top of being capable of offering services equivalent to that of intermediaries thanks to their vast troves of data, can avoid being qualified as a DIs under the DGA by offering either one-to-many intermediation services or free DISs cross-subsidised through their other services. This could enable gatekeepers to outcompete DIs, for instance, by offering through their ecosystems either DISs for free or at predatory prices, or higher quality DISs that leverage the inferences arising from their internal dataflows; or by bundling their intermediation services with one or more of their other services not qualified as core platform services under the DMA.[189]

From this perspective, the DGA and the DMA lack coordination. To correct the identified regulatory gap moving forward, as DMA obligations get fine tuned, it would be necessary that, alternatively,: (i) either gatekeepers are prevented from offering intermediation services; or were allowed, (ii) gatekeepers should be subject to the identical, if not stricter, requirements than those envisaged for DIs by the DGA.[190] Imposing asymmetric obligations on gatekeepers seems reasonable and proportionate given their unrivalled ability to acquire, collect, aggregate, and extract value from data. In this sense, the dDA explicitly excludes gatekeepers amongst the beneficiaries of its data access and portability rights.[191]

5.3.2. *The DMA might inadvertently incentivise gatekeepers' entrance into data intermediation markets*

Second, the DMA imposes several data access and sharing duties on gatekeepers that may hinder DIs' success. Notably, Article 6(9) DMA obliges gatekeepers to provide 'end users and third parties authorised by an end user, at their request and free of charge, with effective portability of data provided by the end user or generated through the activity of the end user in the context of the use of the relevant core platform service'.[192] Such obligation includes the provision of free of charge tools enabling continuous and real-time access to such data.

Article 6(9) DMA, therefore, might inadvertently discourage the utilisation of data intermediaries anytime a data seeker looks for data also owned by a gatekeeper. In similar circumstances, indeed, it is not clear why a data seeker should purchase the needed data from a data intermediary if it could obtain the same or equivalent data for free by a gatekeeper under Article 6(9). The DMA regime is in fact even more convenient for potential data users than the dDA. While the dDA, upon a data user's simple request, mandates data holders to provide the required data in exchange for reasonable compensation, the DMA mandates the same for free. Furthermore, given that IoT's data is expected to grow exponentially[193] and gatekeepers to stretch their 'data areas' either through proxies, correlations, and inferences, or through new business acquisitions (that sometimes even turn into 'killing-acquisitions'[194]), it is likely that in the near future more instances will emerge in which there are more attractive routers for data acquisition than DIs. While this supports the broader data-sharing goals of the Union legislature, it may also turn out to hamper DIs' competitiveness making them unprofitable overall, thus also threatening their role in furthering data-access in scenarios not caught by the DMA and dDA.

Conversely, Article 6(9) DMA, produces an economic incentive for gatekeepers to create separate legal entities that qualify as data intermediaries and offer the same data to the public not for free, as mandated by the DMA, but under the more profitable regime established by the DGA for DIs. It follows that Article 6(9) DMA may end up promoting direct competition between gatekeepers and DIs which is likely to undermine the market entry and success of the latter.

---

danger the economic viability of its operation in the Union. Consequently, the EC may exceptionally suspend, in whole or in part, specific DMA obligations when convinced by gatekeepers' reasoned requests.

[185] For an analysis of the DMA, see P. Akman, 'Regulating Competition in Digital Platform Markets: A Critical Assessment of the Framework and Approach of the EU Digital Markets Act', (2022) 85 *ELR*; M. Schnitzer *et al*., 'International coherence in digital platform regulation: an economic perspective on the US and EU proposals' (2021) *Policy Discussion Paper n*. 5. *Yale Tobin Center for Economic Policy*; G. Monti, 'The Digital Markets Act: Improving its Institutional Design', (2021) 5 *CoRe*, 90; R. Podszun, P. Bongartz, and S. Langenstein, 'Proposals on how to Improve the Digital Markets Act', (2021) *CPI*; A. De Streel, P. Larouche, 'The European Digital Markets Act Proposal: How to Improve a Regulatory Revolution', (2021) *Concurrences*, 46; P.I. Colomo, 'The Draft Digital Markets Act: A Legal and Institutional Analysis', (2021) 12(7) *JECLP*, 561-575.

[186] Article 6(9) DMA.

[187] Article 6(5)-(11)-(12) DMA.

[188] Articles 6(7) and 7 DMA.

[189] Article 5(8) DMA only prohibits bundling between core platform services and no other combinations.

[190] Articles 8, 12, 19, and 49 DMA.

[191] Article 5(2) and Recital 36 dDA.

[192] Article 6(9) DMA.

[193] OECD, *supra* n.7.

[194] C. Cunningham, S. Ma, F. Ederer, 'Killer Acquisitions', (2021) ⟨13:italic ⟩Journal of Political Economy⟨/13:italic⟩, Vol. 129, N. 3, pp. 649-702. For an overview of the legal discussion on the topic see R. Nazzini & G. Carovano, 'Addressing the 'kill zone' of antitrust enforcement without killing legal certainty', (2020) *Competition Law & Policy Debate, 6*(2), 44-50.

What is more, Article 6(2) DMA impedes gatekeepers from using, in competition with business users, non-public data generated or provided by business users in the context of their use of the relevant core platform services or related services. As a result of Article 6(2) DMA, (i) gatekeepers can use those data for purposes other than competing with the business users which generated the data, e.g. they could use those data, for instance, to offer intermediation services ;[195] (ii) gatekeepers have an incentive in publicising those data perhaps in an anonymised and aggregated fashion through the offering of intermediation services, in a way to water down or completely devoid of any practical meaning the prohibition embedded in Article 6(2) DMA. Hence, once again, Article 6(2) DMA represents an additional scenario in which one DMA provision may end up promoting direct competition between gatekeepers and DIs with huge risks for the latter.

5.3.3. *Gatekeepers and the inadequacy of the DGA's duty of neutrality*

Thirdly, if gatekeepers establish separate legal entities that qualify as data intermediaries and offer data intermediation services, the duty of neutrality established in Article 12(1)(a) DGA might not be sufficient to prevent and rein in full the conflicts of interests that could potentially emerge. This is the case because gatekeepers-owned DIs, although structurally separated from other gatekeepers' entities, could still steer, and distort data sharing markets in ways that, while formally respecting the duty of neutrality, could *de facto* substantially infringe it. A similar circumstance, for instance, could occur if, once that gatekeepers-owned DIs become dominant or otherwise acquire substantial economic power in markets for intermediation services, they could start deciding their offerings in strategic ways to either support or damage downstream applications and innovation depending on their own circumstantial economic interests. As a result, it seems that the DGA fell short of considering similar occurrences and did not offer sufficient legal guarantees to address them.

6. Conclusions

This paper has examined the new legal regime for providers of data intermediation services in EU law. Whereas the DGA is intended to boost a more competitive and innovative Digital Single Market in facilitating the availability of data, both factors internal to the new legislation as well as its interplay with the broader EU data law framework cast doubt on whether these goals can really be achieved.

Declaration of Competing Interest

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Data availability

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

Acknowledgements

The authors were funded by the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) under Germany's Excellence Strategy – EXC number 2064/1 – Project number 390727645. Michèle Finck also gratefully acknowledges funding from the Carl Zeiss Foundation. An early version of the paper was presented at Pompeu Fabra University as well as Durham University.

[195] Likely, intermediation services neither infringe to the DMA anti-circumvention provision (Article 13 DMA).