THE EUROPEAN COMMISSION'S PROPOSED DATA GOVERNANCE ACT: SOME INITIAL REFLECTIONS ON THE INCREASINGLY COMPLEX EU REGULATORY PUZZLE OF STIMULATING DATA SHARING

R.M. Gellert & I. Graef[1]

1. Introduction

In 2020, the European Commission published its "European Strategy for Data", a Communication wherein it explained its vision concerning the creation of a European data economy in the next five to ten years.[2] Stimulating the use of data in various sectors of the economy is key to creating this data economy.[3] At present, the use and sharing of data remains sub-optimal because of a number of factors such as the insufficient availability of data, imbalances in market power, insufficient governance structures and technical infrastructures, or the lack of adequate tools that would empower consumers to make use of their rights that rely upon the sharing of data (i.e., data portability rights).[4]

As a result, the European Commission is proposing a number of initiatives including legislative ones. On the one hand, it published in November 2020 the proposed Data Governance Act (DGA).[5] Its goal is to strengthen and create governance mechanisms in order to facilitate the sharing of

---

1 Dr. R.M. (Raphaël) Gellert is Assistant Professor in ICT and private law at Radboud University and is affiliated to the Radboud Business Law Institute, and the interdisciplinary Hub for Security, Privacy and Data Governance (iHub). Dr. I. (Inge) Graef is Associate Professor of Competition Law at Tilburg University and is affiliated to the Tilburg Institute for Law, Technology, and Society (TILT) and the Tilburg Law and Economics Center (TILEC).

2 European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions 'A European strategy for data', 19 February 2020, COM(2020)66 final, 19, p. 1-2.

3 COM(2020)66 final, 19, p. 1-2.

4 COM(2020)66 final, 19, p. 6-11.

5 Proposal for a Regulation of the European Parliament and of the Council on European data governance (Data Governance Act), 25 November 2020, COM(2020)767 final.

data.[6] On the other hand, a so-called Data Act is expected to be proposed in 2021, the scope of which concerns actual rights on the access and use of data.[7]

As one can see, stimulating the European data economy is a complex puzzle. With the introduction of the proposed DGA, the European Commission is filling in a few new pieces illustrating the diversity of the tools and mechanisms it intends to use within its European data strategy. This chapter provides some critical observations on the proposed DGA. More specifically, it explores two inter-related sets of issues.

The first part of the chapter discusses the relation between the proposed DGA and the EU's General Data Protection Regulation (GDPR). For creating a new legal framework regulating the sharing of data, the compatibility between the proposed DGA and the GDPR is a key point. The analysis explores various areas of inconsistency between the two regimes, and focuses in particular on the distinction between personal and non-personal data, which has been a persistent issue for the EU policies concerning the sharing of data.

The second part of the chapter explores whether the proposed DGA will achieve its goal of stimulating the sharing of data, and further, to help build a European data economy. This is done by analysing in detail the contemplated data sharing services, which are the plinth of the whole data sharing mechanism of the proposed DGA. Will this new actor really lead to more sharing of data given its competition with other services regulated more advantageously under the proposed Digital Markets Act (DMA), and given the legal uncertainties associated to its liability for the implementation of the various relevant legal frameworks when it is anything but uncertain how these frameworks will apply in parallel?

The chapter concludes that the new governance institutions established by the proposed DGA create some legal uncertainty, which potentially puts its data sharing objectives at jeopardy and can undermine the relationship with other parts of the EU regulatory framework applicable to data sharing, such as EU data protection, competition law and the proposed DMA. We recommend the EU legislator to provide clearer guidance upfront

6 COM(2020)66 final, 19, p. 12; Explanatory memorandum, p. 1; Explanatory memorandum of the proposed DGA, p. 1.

7 COM(2020)66 final, 19, p. 13; Explanatory memorandum, p. 1; Explanatory memorandum of the proposed DGA, p. 1.

about how the DGA interacts with other parts of EU law to address these concerns.

2. The proposed DGA and the GDPR: a complicated relationship?

2.1 General data protection issues

As indicated in §1, the proposed DGA is part of the European Commission's Strategy for Data, which itself can be seen as the continuation of earlier policy initiatives aiming to build an EU data economy.[8]

Since these earlier policy proposals, authors have noticed the tension existing between data protection principles prohibiting the sharing of data by default (i.e., only possible if certain conditions are fulfilled), and policy/legal initiatives wishing, on the contrary, to stimulate as much as possible the sharing of data.[9] For this reason, some authors have referred to data protection law as 'the elephant in the room' as far as the EU strategy for the data economy is concerned.[10]

In their recent joint opinion on the proposed DGA, the European Data Protection Board (EDPB) and the European Data Protection Supervisor (EDPS) seem to share these concerns.[11] In this joint opinion, the two bodies highlight a number of inconsistencies between the GDPR and the proposed DGA.[12] Among these, one can highlight the diverging definitions and terminology between the GDPR and the proposed DGA, the issue of the legal basis for processing personal data under the proposed DGA, and the

8 European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions 'Building a European Data Economy', 10 January 2017, COM(2017)9 final.

9 See, e.g., R. Gellert, 'Economie Digitale: Vers Une Protection Des Données Personnelles Marginalisée?', *L'observatoire* 2017, mesdatasetmoi.fr.

10 See, C. Wendehorst, 'Of Elephants in the Room and Paper Tigers - How to Reconcile Data Protection and the Data Economy', in: Reiner Schulze et al. (eds.), *Trading Data in the Digital Economy: Legal Concepts and Tools*, Baden-Baden/Oxford: Nomos/Hart Publishing 2017.

11 EDPB & EDPS, 'EDPB-EDPS Joint Opinion 03/2021 on the Proposal for a Regulation of the European Parliament and of the Council on European Data Governance (Data Governance Act)', 2021.

12 EDPB & EDPS 2021, p. 14.

blurring distinction between the processing of personal data and non-personal data.[13]

As far as the terminology is concerned, the joint opinion notes the confusion and incompatibility between the notion of data holder under the proposed DGA and that of data subject in the GDPR,[14] and between the notion of data user under the proposed DGA and that of a data controller under the GDPR.[15] In both these cases, there could be conflicts between the rights and prerogatives derived from these overlapping concepts.[16]

As far as the legal basis is concerned, the joint opinion points to the problematic notion of the 'permission of the data holder', which would legitimise the sharing of data.[17] On the one hand, such notion of permission does not coincide with the GDPR's notion of consent,[18] which means that it would allow for the sharing/processing of data insofar as it constitutes a legal basis in the meaning of art. 6(1)(c) or (e) GDPR. On the other hand however, the joint opinion clarifies that as it stands the new concept of 'permission' does not fulfil the criteria of art. 6(3) GDPR in order to qualify as a legal basis under art. 6(1)(c) or (e) GDPR.[19]

Finally, the joint opinion addresses the blurring between the notion of personal data and non-personal data, and what this also means for the EU Regulation on the Free Flow of Non-personal Data (FFNPDR). On the one hand, the concept of personal data is the material scope of the GDPR, meaning that any processing of personal data falls under the GDPR. On the other hand, the EU adopted in 2018 a Regulation that specifically regulates certain aspects of non-personal data. In other words, the proposed DGA might be at odds not only with the GDPR but also with the FFNPDR. The

13 EDPB & EDPS 2021, p. 8-9.
14 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 (*OJ* 2016, L 119/1).
15 EDPB & EDPS 2021, p. 9-11.
16 EDPB & EDPS 2021, p. 9-11.
17 EDPB & EDPS 2021, p. 13. See, Proposal for a Regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC, COM(825)2020 final, art. 5(6), 7(2)(c), 11(11), or 19(3).
18 This is not explicitly said, but is implicit because the joint opinion only looks at the qualification of 'permission' under art. 6(1)(c), (e) GDPR. See COM(825)2020 final, art. 5(6), 7(2)(c), 11(11), or 19(3).
19 EDPB & EDPS 2021, p. 14.

joint opinion argues that the strict distinction operated by the proposed DGA between personal and non-personal data is hard to realise in practice,[20] especially given the contextual nature of the concept.[21] This creates a lot of uncertainty since a dataset could first be subject to the proposed DGA along with the FFNPDR, and then at some unspecified future point in time be subject to the proposed DGA along with the GDPR.

The joint opinion therefore concludes that the proposed DGA "does not duly take into account the need to ensure and guarantee the level of protection of personal data provided under EU law",[22] and therefore "raises serious concerns from a fundamental rights viewpoint".[23]

It remains to be seen how the European legislator will address these critical remarks, and whether that would lead to a more felicitous articulation of this new data sharing framework with the EU data protection *acquis*. In any case, the interaction with the GDPR deserves to be addressed more proactively to prevent uncertainty after the entry into force of the proposed DGA.

In the following lines, this contribution will look more in detail at the issue of personal *vs* non-personal, as it has been a lingering one. The fact that this issue has been put forward for some years already, and has so far not received any satisfactory legal and policy response (i.e., there is a complete *status quo* on the matter) might suggest that the articulation between the data protection *acquis* and the European Commission's data sharing plans run into some intractable difficulties.

2.2 Personal and non-personal data

Even though the notion of non-personal data is already implicitly acknowledged in the GPDR (since the latter applies to personal data it means GDPR does not apply to non-personal data),[24] the complicated relationship between personal and non-personal data from a regulatory viewpoint came to the fore in 2018 when the EU adopted the first instrument regulating the processing of non-personal data, the Free Flow of Non-Personal

20 EDPB & EDPS 2021, p. 15. See also art. 2(3) proposed DGA.
21 Art. 4(1) GDPR defines personal data as: "any information relating to an identified or identifiable natural person".
22 EDPB & EDPS 2021, p. 7.
23 EDPB & EDPS 2021, p. 7.
24 See, art. 2(1) GDPR: "This Regulation applies to the processing of personal data".

Data Regulation.[25] In a previous contribution, the present authors highlighted various types of difficulties relating to the very broad conception of the notion of personal data under the GDPR,[26] the dynamic nature of personal data and the coexistence of personal and non-personal data.[27] As it was argued, this is problematic for various reasons. On the one hand, the FFNPDR provides for fewer constraints on the processing of data, meaning that it should be easier to share non-personal data than personal data under the GDPR. On the other hand, there is a discrepancy in the way both instruments regulate the free movement of data between Member States.[28]

The following lines will show that these problems have not been solved, quite the contrary. Thus, instead of solving already observed problems concerning the articulation between regimes regulating personal and non-personal data, the proposed DGA perpetuates these problems. Indeed, even though, contrary to the FFNPDR, the proposed DGA applies to both personal and non-personal data, it still distinguishes between personal and non-personal data,[29] and at times provides specific rules for non-personal data,[30] or personal data.[31]

2.2.1 Parallel application

A first difficulty associated to the concomitant regulation of personal and non-personal data is linked to the existence of so-called 'mixed datasets'.[32] A mixed dataset can be defined as a dataset consisting of "both personal and non-personal data",[33] meaning that one has to distinguish between the non-personal data falling under the FFNPDR and the personal data falling

25 Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union (*OJ* 2018, L 303/59).

26 On the breadth of the notion of personal data, see, N. Purtova, 'The Law of Everything. Broad Concept of Personal Data and Future of EU Data Protection Law', *Law, Innov. Technol.* (10) 2018, afl. 1, p. 40.

27 I. Graef, R. Gellert & M. Husovec, 'Towards a Holistic Regulatory Approach for the European Data Economy: Why the Illusive Notion of Non-Personal Data Is Counterproductive to Data Innovation', *EULR* (44) 2019, p. 605.

28 Graef, Gellert & Husovec, *EULR* 2019, p. 610-613.

29 Proposal for a Regulation of the European Parliament and of the Council on European data governance (Data Governance Act), COM(2020)767 final, art. 2(3).

30 See, e.g., art. 5(11)-(13), 30 proposed DGA.

31 See, e.g., art. 5(3), 7(2)(b), 9(1)(b) proposed DGA.

32 Graef, Gellert & Husovec, *EULR* 2019, p. 610-611.

33 European Commission, 'Communication from the Commission to the European Parliament and the Council: Guidance on the Regulation on a Framework for the Free Flow of Non-Personal Data in the European Union', COM(2019)250 final, p. 8.

under the GDPR.[34] The European Commission argues that mixed datasets are bound to constitute the majority of datasets in the data economy.[35]

Yet, such mixed datasets are bound to encounter intractable problems. For indeed, how is it practically feasible to distinguish within one dataset the personal data from the non-personal data?[36] In this regard, it is telling to observe that the proposed DGA does not contain a single word about mixed datasets (this also holds true for the explanatory memorandum). Similarly, the European Strategy for Data only mentions the issue of mixed datasets once and limits itself to refer to the European Guidance on the FFNPDR.[37] However, the latter does not provide any guidance in this regard.[38] In other words, the proposed DGA builds upon this problem without solving it.[39] As indicated at the beginning of this section, even though the proposed DGA now encompasses both personal and non-personal data, it still distinguishes between the two,[40] and at times provides specific rules for non-personal data,[41] or personal data.[42] So in practice, the problem remains.

Furthermore, according to the FFNPDR, when such mixed datasets are 'inextricably linked', then the FFNPDR can apply to the whole dataset only insofar as it does not prejudice the application of the GDPR.[43] This is a step further from 'regular' mixed datasets, which allow for the parallel application of the two regimes. In this case, the European Commission has interpreted this provision as meaning that the GDPR applies exclusively to such datasets.[44] A difficulty is that the precise meaning of 'inextricably linked' is not given anywhere. The European Commission has

34 Art. 2(2) FFNPDR.
35 COM(2019)250 final, p. 8.
36 Graef, Gellert & Husovec, *EULR* 2019, p. 610.
37 European Commission, 'Communication from the Commission to the European Parliament and the Council, the European Economic and Social Committee and the Committee of the Regions: A European Strategy for Data', COM(2020)6.
38 COM(2019)250 final, p. 8-9.
39 As a matter of fact, in a recent report on the European Strategy for data, the European Parliament's Committee on Industry, Research and Energy has called on the European Commission to "further define guidance and practices on how to govern and utilise mixed data sets", Committee on Industry Research and Energy of the European Parliament, 'Report on a European Strategy for Data (A9-0027/2021)', COM(2021)26.
40 Art. 2(3) proposed DGA.
41 See, e.g., art. 5(11)-(13), 30 proposed DGA.
42 See, e.g., art. 5(3), 7(2)(b), 9(1)(b) proposed DGA.
43 Art. 2(2) FFNPDR.
44 COM(2019)250 final, p. 9.

previously argued that a dataset is 'inextricably linked' if "separating the [data sets] would either be impossible or considered by the controller to be economically inefficient or not technically feasible",[45] and that personal data can represent "only a small part of the dataset".[46] Given this broad interpretation, this means that many mixed datasets would in practice be inextricably linked. Here it suffices to mention that the issues of 'inextricably linked' mixed datasets is absent both from the European Data Strategy and from the proposed DGA. This is particularly problematic for the proposed DGA because it does apply "without prejudice to specific provisions in other Union legal acts", including the GDPR.[47] The wording is not exactly the same as that of the FFNPDR, which makes sense since the DGA's purpose is to apply to all data (contrary to the FFNPDR). However, the EDPB-EPDS joint opinion has highlighted that such wording does little to avoid conflicts in practice between the GDPR and specific provisions of the proposed DGA that might go counter the GDPR.[48] At present, what would happen in case of conflict is not exactly clear. But absent specific rules to accommodate the situation, it might simply lead to the application of the GDPR at the expense of the proposed DGA.

2.2.2 Subsequent application

Another issue that was mentioned concerning the FFNPDR and which has not been addressed in the proposed DGA is the subsequent application of the relevant instruments.[49] This problem is connected to the broad and dynamic notion of personal data. As acknowledged by the European Commission itself, data can change in nature, meaning that a piece of non-personal data can become a piece of personal data.[50] The notion of personal data is not only broad, it is also extremely contextual.[51] According to the GDPR, a piece of data will qualify as personal data if it relates to an individual who is identifiable.[52] These two criteria ('relating to' and 'identifiable') are highly dependent upon social and contextual factors. For instance, a piece of data can relate to a data subject not only because of its content (i.e., name or address), but also because of the purpose of

45 COM(2019)250 final, p. 10.
46 COM(2019)250 final, p. 9.
47 Art. 1(2), proposed DGA.
48 EDPB & EDPS 2021, p. 6 and 9.
49 Graef, Gellert & Husovec, *EULR* 2019, p. 611-612.
50 COM(2019)250 final, p. 7 and 10.
51 See, Purtova, *Law Innov. Technol.* 2018.
52 Art. 4(1) GDPR.

the processing (i.e., traffic data used for traffic enforcement purposes).[53] Similarly, a data subject can be identifiable on the basis of information that the data controller or a third party does not have yet but can acquire provided reasonable efforts and given the context of the processing, including its purpose.[54]

The EDPB-EDPS joint opinion rightly points out that the context of machine learning and data sharing, which the proposed DGA builds upon and is meant to stimulate, will only makes things more complicated in this regard.[55] On the one hand, the increased sharing of data puts a lot of pressure on the anonymity of datasets since "the more non-personal data are combined with other available information, the more difficult it will be to ensure anonymisation because of the increased re-identification risk for data subjects".[56] This is especially the case when the original data was personal data that had already been anonymised.[57] On the other hand, one should not forget that one of the key goals of machine learning is also to extract and infer information from datasets,[58] hence the value of data from an economic viewpoint.[59] While valuable, this also has consequences from a data protection viewpoint. The literature has already underscored the risks associated to the extraction of very sensitive information from supposedly benign data.[60] This also means that data which is a priori non-personal can become personal data because of the information that is extracted therefrom (e.g., data on precision farming which allows to draw precise inferences on the working patterns of the employees working in the farm).[61] As one can see, given the current and future technological environment it is extremely difficult if not impossible to predict the exact moment when a piece of data will become personal and thus when the regulatory regime should change.[62] This observation, which had already

53 See, 'Opinion 4/2007 on the concept of personal data' [2007] art. 29 Working Party WP 136.
54 'Opinion 4/2007 on the concept of personal data' [2007] art. 29 Working Party WP 136.
55 See, EDPB & EDPS 2021, p. 15.
56 EDPB & EDPS 2021, p. 15.
57 EDPB & EDPS 2021, p. 15.
58 See, J.D. Kelleher & B. Tierney, *Data Science*, Cambridge (Massachusetts): MIT Press 2018.
59 See, e.g., N. Duch-Brown, B. Martens & F. Mueller-Langer, 'The Economics of Ownership, Access and Trade in Digital Data', *JRC Technical Reports* 2017.
60 See, e.g., T.Z Zarsky, 'Incompatible: The GDPR in the Age of Big Data', *Seton Hall Law Rev*. (47) 2017, p. 995.
61 COM(2019)250 final, p. 7.
62 Graef, Gellert & Husovec, *EULR* 2019, p. 612.

been made in the context of the FFNPDR and ignored in the present context, is particularly problematic for the goals of the proposed DGA and the European Data Strategy. The latter for instance estimates that the value of non-personal data in the manufacturing sector will be valued at "€1,5 trillion by 2027".[63] However, from what precedes there are high chances that a substantial amount of this data is personal data in practice, meaning that it might not be shared as easily as expected and create as much value as expected. And meaning that it would lead to the same difficulties highlighted concerning the specific rules the proposed DGA contains for personal and non-personal data, as well as its application without prejudice to the GDPR.

2.3 Conclusion: colliding legal regimes?

This rapid overview of some of data protection concerns raised by the proposed DGA leads to the following points. Along with the joint opinion of the EDPB-EDPS, there is a real risk that the regime of the DGA as it stands in the proposal will collide with the regime of the GDPR and in so doing will undermine the EU data protection *acquis*. This point is illustrated both by a general discussion of various data protection issues and by a more in-depth discussion of the personal data notion. The latter shows that the problems at stake are not new and can indeed be traced back since the European Commission's earliest plan to create a data economy.[64] Rather than addressing these issues, the proposed DGA simply builds upon them. The rationale of the European legislator for ignoring these issues is not very clear. The lack of clear action and guidance in this regard might simply suggest that data protection law is indeed 'the elephant in the room of the data economy', and that the objectives of the two regimes are simply too opposite to be reconciled, even though this is not our view (the GDPR as a framework applicable to personal data does not stand in the way of other legal frameworks pursuing complementary goals such as stimulating the data economy). However simply ignoring the problem will not help solve it. As things currently stand, there is a high chance that the ambitions and goals of the proposed DGA will simply not be able to materialise because of the many incoherencies in the regulatory framework.

63 COM(2019)250 final, p. 26.

64 As a matter of fact, real conflicts between the GDPR and the FFNPDR had already been highlighted, see Graef, Gellert & Husovec, *EULR* 2019, p. 612-614.

3. Delegated enforcement by data intermediaries under the proposed DGA: counterproductive results?

The parallel application of the proposed DGA with other existing regulatory frameworks also plays a role in relation to the 'data sharing services' the DGA introduces in order to stimulate the European data economy.[65] In particular, the proposed DGA expects providers of data sharing services to put procedures in place to ensure the data exchanges they facilitate preserve key public interests including those related to data protection and competition.[66] This is an interesting but also a remarkable feature of the proposed DGA. Safeguarding these public interests amounts to important responsibilities in areas where the law is not always clear. This implies that important trade-offs as regards compliance with a diverse set of legal regimes are put in the hands of these data intermediaries. The message of this part of the chapter is that data intermediaries in principle can be expected to take up this role, considering the neutrality requirement they have to comply with. However, a question is whether they stand a chance towards the data sharing services provided by big tech firms that are regulated in a less strict manner under the proposed Digital Markets Act. In addition, more guidance is welcome on how data intermediaries as governed by the proposed DGA should exercise their responsibilities in areas where interests protected by different legal regimes overlap or even conflict. In the absence of such guidance, the extent of data sharing may still be less than the proposed DGA is aiming for due to fear of liability caused by legal uncertainty on the part of data intermediaries.

After introducing the role of the data sharing services in the new regime, this section will address these issues that could present significant difficulties in relation to the effective functioning of the data sharing regime of the proposed DGA in practice.

3.1 The notification framework for data sharing services

The proposed DGA sets up a notification framework for data sharing services. National authorities are put in charge of implementing the notification framework. Each Member State has to indicate which authority or authorities are competent to take up these tasks in its territory.[67] The

65 The terms 'data sharing services' and 'data intermediaries' are used synonymously here.
66 Art. 11 proposed DGA.
67 Art. 12(1) proposed DGA.

proposed DGA does not specify whether the national authority should have a particular expertise or mandate. It therefore seems up to Member States to decide whether their data protection, competition, consumer or even cybersecurity agency is best placed to implement the notification framework.[68]

The notification framework works as follows. A provider of data sharing services has to submit a notification to the competent national authority of the Member State in which it has its main establishment.[69] The notification includes information about the name, address and legal status of the provider as well as a description of the service the provider intends to provide.[70] Upon notification, the provider may start offering its data sharing service in all Member States.[71] The national authority will issue a standardised declaration at the request of the provider to confirm that it has submitted the notification.[72] The competent authority may charge fees for this, as long as the fees are proportionate and based on the administrative costs incurred for the tasks carried out in the notification framework.[73] Each notification is forwarded to the national competent authorities of the other Member States as well as to the European Commission.[74] The Commission keeps a register of providers of data sharing services in the EU.[75]

It is important to keep in mind that the competent national authorities do not conduct a compliance check at the time of notification. As indicated in the explanatory memorandum to the proposed DGA, the framework consists of compulsory notification with only ex post monitoring of whether providers of data sharing services comply with the applicable requirements. This policy option was chosen as an intermediary solution between: on the one hand, a voluntary labelling mechanisms, where the national authorities would carry out a fitness check upon acquiring the

68 Art. 12(3) proposed DGA does require the designated competent authorities to exchange information that is necessary for the exercise of their tasks with 'the data protection authorities, the national competition authorities, the authorities in charge of cybersecurity, and other relevant sectorial authorities'.
69 Art. 10(1) proposed DGA.
70 Art. 10(6) proposed DGA.
71 Art. 10(4) and (5) proposed DGA.
72 Art. 10(7) proposed DGA.
73 Art. 10(10) proposed DGA.
74 Art. 10(8) and (9) proposed DGA.
75 Art. 10(9) proposed DGA.

label, and on the other hand, a compulsory certification scheme managed by private conformity assessment bodies.[76]

The thinking behind the notification framework as an intermediary solution is that it strikes a balance between the objective of increasing trust in the functioning of data intermediaries (above the level of trust a voluntary mechanism would create), while limiting the regulatory burden and costs for market players (below the level of costs of a compulsory scheme).[77] As will be further discussed below, the consequence of this choice for only ex post monitoring is that the data intermediaries carry the initial responsibility and risk for ensuring that the data exchanges facilitated via their services comply with all applicable regimes. In terms of the competences to ensure compliance, the proposed DGA lays down that national authorities have the power to require providers of data sharing providers to stop a breach of the applicable requirements either immediately or within a reasonable time limit and to take appropriate and proportionate measures aimed at ensuring compliance. In this regard, national authorities can impose deterrent fines and require termination or postponement of the provision of the data sharing service.[78]

3.2 The responsibilities of data sharing services

The notification framework does not apply to not-for-profit entities who seek to collect data only for objectives of general interest.[79] This implies that the requirements target commercial data intermediaries. Art. 9(1) of the proposed DGA defines the three types of data sharing services that are subject to the notification regime as follows:

(1) intermediation services between data holders with legal personality and potential data users. As illustration of such services, reference is made to bilateral or multilateral exchanges of data, platforms or databases facilitating exchange or joint exploitation of data, and the creation of an infrastructure to connect data holders and data users. Dawex is an example of a data exchange platform that matches supply and demand for data without itself accessing the data exchanged on its transaction platform.[80]

76 Proposed DGA, Explanatory memorandum, p. 5.
77 Proposed DGA, Explanatory memorandum, p. 5.
78 Art. 13(4) proposed DGA.
79 Art. 14 proposed DGA.
80 See dawex.com/en/.

(2) intermediation services between data subjects wishing to make their personal data available and potential data users when exercising the rights provided by GDPR. These services include the provision of technical or other means to enable such services. Examples are personal information management services (PIMs), such as developed in the DECODE[81] and Solid[82] projects, which enable individuals to control the sharing of their personal data.[83]

(3) services of so-called data cooperatives. These are described as services that support data subjects or small enterprises "in making informed choices before consenting to data processing, and allowing for mechanisms to exchange views on data processing purposes and conditions that would best represent the[ir] interests".[84] The provision explains that data subjects or small enterprises can be either members of the cooperative or confer the power to the cooperative to negotiate the conditions for data processing before they consent. An example of the development of data cooperatives is the MyData movement.[85]

These three types of data sharing services are subject to variety of conditions as laid down in art. 11. The most fundamental requirement is for providers of data sharing services to be neutral as regards the data exchanged. This entails that providers may only act as intermediaries and cannot use the data exchanged for any other purpose than to put them at the disposal of data users.[86] The metadata collected from the provision of a data sharing service may also only be used for the development of that service.[87] To avoid conflicts of interest, data sharing services have to be placed in a separate legal entity so that there is a structural separation between the data sharing service and any other services offered by the same provider.[88] If the provider offers data sharing services for natural persons, there is an additional fiduciary duty towards individuals that the provider bears in order to act in the best interests of data subjects when facilitating the exercise of their rights. This includes in particular advising data

81 See decodeproject.eu/.
82 See solid.mit.edu/.
83 For a discussion of the opportunities of PIMs, see the EDPS Opinion 9/2016 'Personal Information Management Systems: Towards more user empowerment in managing and processing personal data', 2016.
84 Art. 9(1)(c) proposed DGA.
85 See mydata.org/.
86 Art. 11(1) and recital 26 proposed DGA.
87 Art. 11(2) and recital 26 proposed DGA.
88 Art. 11(1) and recital 26 proposed DGA.

subjects on potential data uses and on standard terms and conditions attached to such uses.[89]

Beyond these more general requirements, providers of data sharing services also have to implement measures to protect specific interests namely to:

- ensure that access to their services is fair, transparent and non-discriminatory, including as regards prices;[90]
- prevent fraudulent or abusive practices in relation to access to data from parties seeking access through their services;[91]
- to prevent transfer or access to non-personal data that is unlawful under EU law;[92]
- to ensure a high level of security for the storage and transmission of non-personal data;[93]
- to ensure compliance with EU and national competition rules.[94]

The list of requirements illustrates the responsibilities data intermediaries have in ensuring that data exchanges take place in compliance with our European values. This brings us to the question of how one can qualify the role of data intermediaries in the proposed DGA: are they amounting to 'private regulators' of data sharing?

3.3 Data intermediaries as neutral 'private regulators'?

The proposed DGA is not the only recent legislative initiative published at the EU level. After the European Commission published the proposed DGA on 25 November 2020, it unveiled two other long-awaited instruments on 15 December 2020: the proposal for a Digital Markets Act (DMA),[95] already mentioned in the introduction, and the proposal for a Digital Services Act (DSA).[96] The proposed DSA and DMA lay down ru-

89 Art. 11(10) and recital 26 proposed DGA.
90 Art. 11(3) proposed DGA.
91 Art. 11(5) proposed DGA.
92 Art. 11(7) proposed DGA.
93 Art. 11(8) proposed DGA.
94 Art. 11(9) proposed DGA.
95 Proposal for a Regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act), COM(2020)842 final.
96 Proposal for a Regulation of the European Parliament and of the Council on a Single Market for Digital Services (Digital Services Act) and amending Directive 2000/31/EC, COM(2020)825 final.

les to restrict the freedom of a certain category of intermediaries namely online platforms, for instance as regards content moderation in the DSA and by banning certain practices in the relationship between gatekeeping platforms and businesses as well as end users in the DMA. It is interesting to observe that the proposed DGA seems to aim at increasing the ability for another type of platforms to be active in the European data economy by providing them with key responsibilities that are subject to ex post monitoring by national authorities. These developments seem to hint at a tension in the overall approach of the European Commission, as the freedom of platforms is limited in one area while their rise is promoted in another area. However, one should also keep in mind the different circumstances in the respective industries. While the industries targeted by the proposed DSA and DMA are quite concentrated and mainly consist of a few large US-based players, the data sharing services the proposed DGA wishes to promote are still mostly in their infancy.[97]

To explore whether it is appropriate for the EU legislator to take measures to stimulate the rise of data sharing services as novel key intermediaries in the European data economy, it is useful to examine some of the concerns expressed about the dependence of businesses and consumers on platforms in the areas targeted by the proposed DSA and DMA. These concerns relate in particular to the bottleneck or gatekeeping character of platforms (including search engines, social networks, app stores and e-commerce marketplaces) that can unilaterally impose their own conditions on how businesses and consumers interact to the extent it limits their freedom of choice and steers the exercise of democratic freedoms. Considering that these are key public interests that are normally enforced and implemented by regulatory authorities and legislators, this phenomenon has been referred to by the notion of 'platforms as regulators'.[98] The type and extent of control held by platforms has been said to qualify them as private regulators of public interests.[99] It is therefore interesting to observe that the Commission seems to grant data intermediaries a similar

97 One may also wonder to what extent an industrial policy objective is behind the idea of promoting the development of European data sharing services where our values can be integrated into the design from the very start.

98 See, J. Crémer, Y.A. de Montjoye & H. Schweitzer, *Competition policy for the digital era*. *Expert report for Commissioner Vestager*, 2019, p. 60-63 and N. Dunne, 'Platforms as regulators', *J. Antitrust Enforc.* (forthcoming) 2020.

99 For an early source, see K.J. Boudreau & A. Hagiu, 'Platform Rules: Multi-Sided Platforms as Regulators', in A. Gawer (red.), *Platforms, Markets and Innovation*, Cheltenham: Edward Elgar Publishing 2009). See the previous footnote for more recent references.

regulatory role as 'first-line enforcers' to ensure that the data exchanges taking place via their services comply with the various applicable legal regimes.

Apart from the different stage of development of the industries, another key difference with the situation now facilitated by the proposed DGA is that a requirement of neutrality is imposed on providers of data sharing services. As a result, the provider may only act as an intermediary between data holders and data users, and cannot use the data exchanged for developing other services. This requirement addresses concerns about vertically integrated platforms having a dual role by simultaneously acting as intermediary between businesses and users as well as competing with those businesses in offering their own services.[100] An example is an undertaking that at the same time: (1) provides a marketplace where independent businesses can sell products to consumers, and (2) sells products as a retailer on the same marketplace in competition with the independent businesses. Such situations of vertical integration provide room for practices of self-preferencing, whereby a platform treats its own services more favourably than those of rivals. The *Google Shopping* competition decision and the ongoing *Amazon* competition investigation target such practices. In its *Google Shopping* decision, the European Commission found Google liable for abusing its dominant position in the market for online search by giving its own comparison shopping service more prominent placement in its general search results than rival comparison shopping services.[101] In the *Amazon* investigation, the Commission is concerned about Amazon's preferential access to transaction data of independent businesses who sell on its marketplace to the benefit of Amazon's own retail business that is directly competing with these independent businesses.[102] These risks caused by the vertically integrated nature of platforms are prevented through the neutrality requirement that the proposed DGA imposes on providers of data sharing services.

While this is a welcome development, there seems to be an unlevel playing field between the data sharing services governed by the neutrality requirement in the proposed DGA and big tech platforms that are only subject to requirements against self-preferencing in specific circumstances under

100 See, Crémer, de Montjoye & Schweitzer 2019, p. 61.
101 Case AT.39740 *Google Search (Shopping)*, 27 June 2017.
102 Press release European Commission, 'Antitrust: Commission sends Statement of Objections to Amazon for the use of non-public independent seller data and opens second investigation into its e-commerce business practices', 10 November 2020.

competition law and in the proposed DMA. For instance, the proposed DMA lays down a duty for gatekeeping platforms to refrain from combining personal data across services unless the end-user has provided consent to do so (art. 5(a)) and to refrain from using data generated through business users' activities to compete when data is not publicly available (art. 6(1)(a)). Considering that gatekeeping platforms are not subject to full neutrality requiring structural separation of data sharing services, a question is whether the data intermediaries governed by the proposed DGA stand a chance against big tech platforms who increasingly offer data sharing services targeted at individuals under their own control. An example is the Data Transfer project[103] developed by Apple, Facebook, Google, Microsoft and Twitter, which allows individuals to port personal data across services. Doubts have indeed been expressed about whether data sharing services, and in particular PIMs targeted at natural persons, can succeed on the market as a neutral alternative to the services provided by big tech firms. In the absence of widespread standards to seamlessly integrate personal data from different services and as long as PIMs find no sustainable revenue streams beyond the prevalent business model of the big techs relying on the monetisation of personal data, data sharing services may not have a significant impact on the European data economy.[104] The success of data sharing services depends on the uptake by the market, considering that the proposed DGA merely facilitates voluntary data sharing at the initiative of market players. More far-reaching legislative interventions to assign rights and duties to make data sharing compulsory in certain circumstances are expected in the proposed Data Act that is due to be published in 2021.[105]

While the proposed DGA and DMA are separate instruments promoting their own goals, there should be consistency in the overall policy approach for the EU digital strategy. To achieve such alignment, the imposition of more far-reaching neutrality requirements on gatekeeping platforms to

103 See datatransferproject.dev/.

104 See J. Krämer, 'Personal Data Portability in the Platform Economy: Economic Implications and Policy Recommendations', *J. Competition Law Econ.* 2020, p. 19-28.

105 COM(2020)66 final, 19, p. 13-15 and 20-21. Note that the proposed DMA already includes specific duties for gatekeeping platforms regarding the use of data. Beyond the requirements of art. 5(a) and 6(1)(a) as mentioned in the main text, art. 6(1)(i) lays down a duty to give business users free of charge and real-time access to data generated through the use of a core platform service and art. 6(1)(j) provides for a duty to give third-party search engines access to ranking, query, click and view data on FRAND terms, subject to anonymization.

offer data sharing services under the proposed DMA may be required to mirror the approach taken in the proposed DGA.

3.4 Need for guidance on how to balance interests protected by separate legal regimes

Apart from questions about the expected success and sustainability of data sharing services as governed by the proposed DGA, it is also important to acknowledge the key responsibilities they are given. Art. 11 requires data intermediaries to put in place procedures to ensure compliance with various legal frameworks related to data sharing, including data protection and competition law as well as requirements applicable to non-personal data. This task is not as straightforward as it may seem. This is best illustrated by giving a few examples of the sometimes overlapping and even conflicting requirements of different regimes that apply in parallel.

An important data subject right whose use data sharing services can further facilitate is the GDPR's right to data portability.[106] There are still open questions as to the scope of this right. For instance, to what extent can the rights of third party data subjects or the intellectual property rights of data controllers stand in the way of the porting of one's personal data?[107] In the absence of further clarification by data protection authorities or courts,[108] data intermediaries are expected to make sure the data exchanges on their platforms strike an adequate balance between these interests. Another example concerns the interaction between the regimes for personal and non-personal data, as already discussed in §2. Despite the choice by the EU to separate legal requirements on the basis of whether data qualifies as personal or not,[109] the notion of personal data seems too dynamic and open-ended to be used as a basis for a new regime for non-personal data

106 Art. 20 GDPR.

107 Art. 20(4) GDPR. See the discussion in: G. Malgieri, ''User-provided personal content' in the EU: digital currency between data protection and intellectual property' *Int. Rev. Law, Comput. Technol.* 2018, p. 118-140; O. Lynskey, 'Aligning data protection rights with competition law remedies? The GDPR right to data portability', *EULR* (44) 2017, p. 814; I. Graef, M. Husovec & N. Purtova, 'Data Portability and Data Control: Lessons for an Emerging Concept in EU Law', *German Law J.* 2018, p. 1359-1398.

108 For non-legally binding guidance, see art. 29 WP, 'Guidelines on the right to data portability', 16/EN WP 242 rev.01 [2017].

109 See FFNPDR. For further discussion, see I. Graef, 'Paving the Way Forward for Data Governance: a Story of Checks and Balances: Editorial', *Technology & Regulation* 2020, p. 25-26.

only.[110] A last example relates to the need to ensure compliance with the competition rules. A concern regarding the exchange of information between rivals is that it may give rise to collusion and act as a mechanism to restrict competition.[111] However, the exact scope for liability is still unclear in the absence of decisions of the European Commission and judgments of the EU Courts on so-called data pooling arrangements.[112] The Commission is expected to provide guidance on the legality of data pooling in its revised Horizontal Guidelines.[113]

The observation here is that the scope of the rules applicable to data sharing are not yet clear-cut and need further interpretation by the respective authorities and courts. Until more clarity is created, the responsibility for implementing important trade-offs are now left to data intermediaries with ex post monitoring by the competent authorities designated at the Member State level. In other words, the enforcement is initially delegated to data intermediaries that can face fines or be required to discontinue their services if a national authority concludes they have breached one of the requirements as laid down in the proposed DGA. The idea of delegated enforcement by data intermediaries is not an unjustified policy choice in itself, especially considering that the neutrality requirement provides an important safeguard against data intermediaries misusing data transactions to achieve own commercial gains in related markets. Our main concern is therefore not that data intermediaries have bad intentions and intentionally act or fail to act in a way that creates competition or data protection concerns. Instead, our message is that more proactive guidance from the EU legislator is welcome to stimulate the exchange of data and let data sharing services truly flourish. In the absence of more legal clarity, data intermediaries may be too careful and restrict exchanges of data that would in fact be desirable or the rise of data sharing services may be lower

110 See Graef, Gellert & Husovec, *EULR* 2019, p. 605-621; M. Finck & F. Pallas, 'They who must not be Identified – Distinguishing Personal from Non-Personal Data under the GDPR', *Int. Data Priv. Law* 2020, p. 11-35. See also the finding based on interviews with platforms in V. Gineikytė, E. Barcevičius & G. Cibaitė, Analytical paper 5 of the Observatory of the Online Platform Economy 'Business user and third-party access to online platform data', July 2020, p. 42: "while in the public discussions on data sharing the main distinction is between personal and non-personal data processing, from the business perspective, this distinction is hard to make."

111 Art. 101 TFEU.

112 See B. Lundqvist, 'Competition and Data Pools', *EuCML* 2018, p. 146-154.

113 The current guidelines are from 2011: Guidelines on the applicability of Article 101 of the Treaty on the Functioning of the European Union to horizontal co-operation agreements (*OJ* 2011, C 11/01).

than hoped due to the unclear scope for liability. These issues can still be tackled during the legislative process or should otherwise be clarified through soft law or guidance documents in order to ensure that the promotion of data sharing services as envisaged by the proposed DGA can achieve its full potential.

4. Conclusions

This contribution has provided a first look at the proposed DGA from the perspective of how the instrument interacts with other regulatory frameworks, including the GDPR, competition law and the proposed DMA. The key point of this analysis is that the proposed DGA is currently characterised by a number of legal uncertainties that can jeopardise the achievement of its objectives (i.e., stimulating the data economy) but also undermine other parts of the EU regulatory framework.

The achievement of its objectives might be at jeopardy because of some of the choices made in the DGA proposal (e.g., bestowing legal responsibility for compliance onto data sharing services), but also because of the uncertainty surrounding the articulation of the proposed DGA with other laws. In this regard, it has been shown that, as things stand, there is quite some uncertainty on the status of mixed datasets and in particular of inextricably linked datasets. Does the application of the proposed DGA without prejudice to the GDPR lead to the exclusive application of the GDPR to these datasets? Similarly, actors regulated under the DMA will enjoy more favourable conditions than the DGA's data sharing services, meaning that the sharing of data might take place under other legal frameworks rather than under the DGA, which can stand in the way of the European data economy reaching its full potential.

From a data protection law perspective this contribution has highlighted a number of issues such as diverging definitions and terminologies between the GDPR and the proposed DGA (e.g., conflict between data subject and data holder), the lack of a clear basis for the processing of personal data under the proposed DGA, and the difficult distinction between what constitutes personal or non-personal data. As far as the latter are concerned, key terms such as inextricably linked mixed datasets are nowhere defined and guidance is lacking for the parallel application of the GDPR and the proposed DGA to a mixed dataset. This lack of guidance may undermine the desired data sharing that the proposed DGA wishes to promote. The

data sharing envisaged by the proposed DGA can also be undermined due to the current uncertainties about the application of the competition rules to data exchanges to be facilitated by the DGA's data sharing services.

The lack of adequate institutions and governance structures had previously been identified as one of the core reasons underpinning the lack of sufficient sharing of data.[114] This is clearly what justifies the proposal for the DGA.[115] While we understand the rationale for specific institutions dedicated to facilitating the sharing of data, we had previously argued that such institutions and governance frameworks needed not be created *ex nihilo* but could build on structures already created by existing regimes (such as within data protection and competition law) and should at least consider their interaction with these existing regimes.[116]

In particular, we would like to observe two things. First, spill-overs from the data protection framework might help dispel the idea that data protection law is 'the elephant in the room of the data economy'. After all, the GDPR is also meant to ensure the free flow of personal data within the EU.[117] In this regard, it is useful to point out that specific GDPR provisions such as those concerning data security or data portability obligations are directly instrumental to enabling a flourishing data economy.[118] Second, these spill-overs would require going beyond general and abstract phrasing that characterises the proposed DGA (i.e., "this Regulation is without prejudice to…").[119] As things currently stand, the compatibility of the proposed DGA with the rest of the EU *acquis* looks like a mere afterthought that is left to market players to figure out. To make sure the proposed DGA (and new data sharing policies in general)[120] achieves its objectives, the interaction with other parts of the EU *acquis* should ideally be considered upfront during the legislative process or otherwise be addressed in a proactive manner through soft law or guidance documents before its entry into force.

114 Duch-Brown, Martens & Mueller-Langer, *JRC Technical Reports* 2017, p. 36.
115 COM(2020)66 final, 19, p. 12-13.
116 Graef, Gellert & Husovec, *EULR* 2019, p. 618.
117 Art. 1(1) and recital 170 GDPR.
118 See, Graef, Gellert & Husovec, *EULR* 2019, p. 619-620.
119 Art. 1(2) proposed DGA.
120 See, Graef, Gellert & Husovec, *EULR* 2019, p. 618.