KU LEUVEN CiTiP

CENTRE FOR IT & IP LAW

CiTiP Working Paper Series

White Paper on the Data Governance Act

Julie Baloup, Emre bayamlıoğlu, Aliki Benmayor, Charlotte Ducuing, Lidia Dutkiewicz, Teodora Lalova, Yuliya Miadzvetskaya and Bert Peeters

CiTiP Working Paper 2021

KU Leuven Centre for IT & IP Law - imec

23 June 2021

White Paper on the Data Governance Act

Julie Baloup[1], Emre bayamlıoğlu[2], Aliki Benmayor[3], Charlotte Ducuing[4], Lidia Dutkiewicz[5], Teodora Lalova[6], Yuliya Miadzvetskaya[7] and Bert Peeters[8]

[1] Julie Baloup contributed to Sections 1, 3, 4, 7 and 8 and coordinated the collaborative writing of the White Paper with Charlotte Ducuing. Julie is a researcher at CiTiP KU Leuven. Email address: Julie.baloup@kuleuven.be.

[2] Emre bayamlıoğlu contributed to Section 4. Emre is a researcher at CiTiP KU Leuven. Email address: emre.bayamlioglu@kuleuven.be.

[3] Aliki Benmayor contributed to section 4 and conducted first-level review of sections 1, 2, 3 and 4. Aliki is a researcher at CiTiP KU Leuven. Email address: aliki.benmayor@kuleuven.be.

[4] Charlotte Ducuing contributed to Sections 1, 2, 3, 4, 5 and 8 and coordinated the collaborative writing of the White Paper with Julie Baloup. Charlotte is a researcher at CiTiP KU Leuven. Email address: charlotte.ducuing@kuleuven.be.

[5] Lidia Dutkiewicz contributed to Sections 2 and 4. Lidia is a researcher at CiTiP KU Leuven. Email address: lidia.dutkiewicz@kuleuven.be.

[6] Teodora Lalova contributed to Section 5. Teodora is a PhD researcher at KU Leuven's Department of Pharmaceutical and Pharmacological Sciences, Clinical Pharmacology and Pharmacotherapy group and at the Centre for IT & IP Law (CiTiP). Her PhD is supported with a scholarship by the Research Foundation – Flanders (FWO), and it is conducted in collaboration with the European Organisation for Research and Treatment of Cancer (EORTC). Email address: teodora.lalova@kuleuven.be.

[7] Yuliya Miadzvetskaya contributed to Sections 7 and 8. Yuliya is a researcher at CiTiP KU Leuven. Email address: yuliya.miadzvetskaya@kuleuven.be.

[8] Bert Peeters contributed to Section 6 and conducted first-level review of sections 5 and 7. Bert is a researcher at CiTiP KU Leuven. Email address: bert.peeters@kuleuven.be.

Table of Contents

Abstract

The White Paper offers an academic perspective to the discussion on the Data Governance Act proposal ("DGA proposal"), as adopted by the European Commission in November 2020. It contains a legal analysis of the DGA proposal and includes recommendations to amend its shortcomings. The White Paper aims to cover the full spectrum of the DGA proposal and therefore offers an in-depth analysis of its main provisions. In conclusion, the authors identify general patterns at work with the DGA proposal, namely, first, the (new) regulation of data as an object and, even more so, as an object of rights. This approach, the authors find, may contribute to exacerbate the risk of contradictions of the DGA proposal with the GDPR on the level of principles. Second, it discusses the relationship of the DGA proposal vis-à-vis the (regulation of) European data spaces and more generally its place in the two-pillars approach of the EC, between horizontal (sector-agnostic) and sectoral regulation of data. Finally, the DGA proposal is identified as a cornerstone of the new EU 'digital sovereignty' policy.

Keywords

Data governance; data rights; data altruism; data sharing service; data intermediary; public sector body; data utility; digital sovereignty; data spaces; neutrality.

Acknowledgment

The authors express their gratitude to Peggy Valcke, Isabelle Huys and Jan Czarnocki for their support and insightful comments on earlier drafts of the White Paper. All errors remain these of the authors. The authors also thank Natalie Bertels for her enthusiastic support for their work.

The White Paper benefited from the support of the following research projects:

- EUHubs4Data. This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 951771.
- TRUSTS - Trusted Secure Data Sharing Space. This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 871481.
- Teodora Lalova's PhD is supported by a scholarship awarded by the Research Foundation – Flanders (FWO), Project No 11H3720N.

Key conclusions

The White Paper offers an academic perspective to the discussion on the DGA proposal, as put forward by the European Commission in November 2020. The paper covers the whole text of the DGA proposal, offering an in-depth analysis of its main provisions and pointing to its main shortcomings, in particular as regards the interplay with the GDPR rules. It also includes recommendations to address identified shortcomings. The DGA proposal lacks legal certainty and the following issues warrant further clarification:

- **Definitions under Art. 2 DGA proposal, especially those of 'data', 'data holder' and 'data user'**

The definition of 'data' is remarkably broad as it extends not only to individual data but also to 'compilations' of them. The definition of 'data' risks being extended to the semantic level of information (the content conveyed by digital means) rather than on its syntactic level (the bits and bytes). This may result in the DGA proposal having an unexpectedly broad scope.

Under the definition of 'data holder', it should be clarified whether 'data subject' refers to 'data subject' in the meaning of the GDPR or not. The 'right to grant access' and the 'right to share' data are core components of the definition of 'data holder' but are neither defined in the DGA proposal nor any other EU legislation. It is unclear whether these 'rights' refer to (i) the lack of legal entitlements to prevent data access and sharing; or to (ii) legal entitlements allowing a 'data holder' to grant access to and/or share data. Also, it should be clarified what having 'data under one's control' means and whether it is a cumulative condition with a 'right to grant access' or 'right to share' data.

To qualify as a 'data user', one has to meet two cumulative conditions: (i) have 'lawful access' to personal or non-personal data; and (ii) be 'authorized' to use data. The issue of what constitutes 'lawful access' and who – and based on what criteria - determines whether the access is lawful should be clarified. Concerning personal data, the question is whether 'lawful access' equals 'lawful basis' within the meaning of the GDPR. It is also unclear what 'lawful access' means in relation to non-personal data consisting of individual data, given that such data is generally considered to not be covered by specific access and/or sharing rights. The question is also how being 'authorised' to use data is different from having a 'lawful access'.

- **Re-use of public sector data that are subject to third parties' rights (Chapter II DGA proposal)**

With the creation of this legal regime, the Commission aims to unlock the potential of re-use of some 'data' deemed to be outside the scope of the Open Data Directive. However, there is a risk of overlap and thus inconsistencies between the DGA proposal and the Open Data Directive. This may arise from the - artificial - distinction made between data and document in the scope of application of the Open Data Directive and those which would be outside, where the latter could therefore be regulated under the DGA.

Public sector bodies are requested to adopt a granular approach towards data re-users, for instance by looking into - but also supervising - the purpose for re-use. While it could indeed fulfil its objective to increase the amount of data made available for re-use, such an approach raises questions as to the responsibilities and liability exposure of public sector bodies. This seems to have been overlooked in

the DGA proposal. This is particularly the case concerning the processing of personal data, where the interplay with the GDPR should be clarified.

The re-user that was granted the right to re-use protected data held by public sector bodies may only transfer such data to third countries under strict conditions. While international transfers of personal data is subject to the GDPR, the DGA proposal introduces rules for international transfers of confidential data and data covered by IP rights. These rules may raise compliance issues with the EU's international trade commitments.

- **Data sharing services regime (Chapter III DGA proposal)**

With the creation of a mandatory legal regime applicable to data sharing services providers, the European Commission aims to foster trust in data sharing and intermediaries to boost the EU digital economy. However, the DGA proposal provides a heavy-handed regime by imposing notification duties and several other operational conditions (such as appointing a legal representative, ensuring neutrality of operations or continuity of service). This raises questions as to the regulatory role of the state in the economy and the proportionality of the chosen instrument in an ecosystem which is still at its infancy.

The DGA proposal needs to set out the exact scope of the data sharing service providers, by laying down specific criteria that providers will need to meet. At the moment, both the included entities and those exempted are vaguely defined.

The obligations and duties imposed on data sharing service providers should be further clarified. It should also be considered whether they conflict with fundamental freedoms protected by the EU Charter, especially the right to conduct business and whether they pass the proportionality test, *i.e*. whether they are necessary, suitable and *stricto sensu* proportionate to attain the aim pursued.

- **Data altruism (Chapter IV DGA proposal)**

With the creation of this legal regime, the Commission aims to ensure that individuals and legal entities trust data altruism organisations to increase data altruism 'for the common good'. However, the interplay with the GDPR rules is unclear. On that basis, the effectiveness of this data altruism regime may be considerably undermined.

The definition of 'data altruism' is riddled with several key terminological ambiguities, related to, *i.e*., the notions of 'consent', and 'general interest'. Data altruism focuses on consent, although consent is only one among several possible lawful grounds for processing personal data - which are not ranked in any particular way - under the GDPR. The legal regime governing data altruism is characterised by the objective to make data available for purposes of 'general interest'. However, the proposal has left unclear how 'general interest' must be understood vis-a-vis the multi-layered notion of 'public interest' in the GDPR.

Although the provisions of the DGA proposal apply to both personal and non-personal data, the rules on data altruism lack clarity and consistency when it comes to non-personal data, which seem to be implicitly overlooked. Hence, data altruism appears to be mainly targeted at the re-use of personal data. This ambiguity must be resolved and clear rules in the context of non-personal data must be established.

The DGA proposal does not define 'data altruism organisation', nor its activities in a sufficient manner. In addition, the complexification of the data value chain with the introduction of a 'data altruism organisation' as a new actor comes with risks to undermine the legal protection afforded to individuals concerning the processing of data relating to them (in the case of personal data). It is questionable whether the proposed data altruism mechanism suffices to fulfil the Commission's objective to grant data subjects control on what is done with 'their' data along the value chain, thus establishing trust. The legislator could get inspiration from empowering mechanisms in place in other contexts (*e.g.* clinical research) to enable individuals to take part in the decision-making process. Moreover, the question of the added value of the data altruism provisions concerns not only data subjects but also data users. Whether these provisions can genuinely increase the re-use of data 'for the common good' is questionable as a result.

- **The European Data Protection Board's competence (Chapter VI DGA proposal)**

There is growing awareness that data protection should not only be considered with regards to data that is clearly personal. On the contrary, increasing amounts of data make combinations of non-personal data more likely to infer or generate personal data, thereby introducing an element of risk to the processing of non-personal data. Likewise, anonymisation proves to be particularly difficult. Instead of elaborating on the competence of the EDPB, the DGA proposal obfuscates the regulatory landscape by introducing separate competent bodies with overlapping competences.

- **Final provisions (Chapter VIII DGA proposal)**

The DGA proposal should provide clarification about the scope of the obligations imposed on the public sector body, the re-user to which the right to re-use the data was granted under Chapter II, the provider of data sharing services and the recognized data altruism organisation given international access to non-personal data by third-country law enforcement authorities.

To ensure harmonized penalties within the EU, the European Data Innovation Board should allow for cooperation between the Member States on this issue.

1 Introduction

In November 2020, the European Commission ("EC"), adopted the Proposal for a Data Governance Act ("DGA proposal").[9] It is its first legislative initiative under the 2020 European Data Strategy that aims to reinforce the single market for data. The objective of the DGA proposal is to set the conditions for enhancing the development of the common European data spaces, as identified in the 2020 European Data Strategy,[10] by bringing trust in data sharing and data intermediaries.[11] In that respect, the DGA proposal lays down an overarching framework comprising horizontal measures relevant for all common European data spaces while leaving room for the application of sector-specific rules, where appropriate.[12]

Data is an essential resource for data-driven innovation, allowing for the development of personalized and inexpensive products and services.[13] While an increasing amount of data is being generated through the use of digital devices and services, the cross-border availability of such data remains too limited due to the lack of a data sharing framework in the EU. As a result, the EC fears that the European economy will increasingly depend on third countries, in particular for the development of the Internet of Things and Artificial Intelligence systems.[14] There is therefore a need to leverage the potential of data for the EU economy and society by fostering data sharing across the European digital single market.

The DGA proposal is part of the general digital strategy of the EC that should materialise in several legislative proposals complementing each other. The DGA proposal is most closely related to the upcoming Data Act expected to be proposed by the EC in 2021. While the DGA proposal deals with the governance framework, the Data Act should introduce new substantive rights on data, in order to solve the question of who is entitled to access and/or control which data.[15] The EC's digital strategy also encompasses two other legislative proposals, released around the same time as the DGA proposal : the Proposal for a Digital Market Act ("DMA proposal")[16] and the Proposal for a Digital Services Act ("DSA proposal").[17] While the DGA proposal is expected to deliver fairer data processing practices and regulate the behaviour of actors engaged in data sharing, at the same time the EC seeks to tackle the data-driven (market) power of 'Big Tech'. This is covered by the DMA proposal that aims to promote effective competition in digital markets. To do so, the DMA proposal is based on 2 pillars : (i) to prevent

[9] European Commission, Proposal for a Regulation of the European Parliament and the Council on European data governance (Data Governance Act), COM(2020) 767 final ("DGA proposal").

[10] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, A European Strategy for Data, COM(2020) 66 final.

[11] Commission Staff Working Document, Impact Assessment Report accompanying the DGA proposal, SWD(2020) 295 final, Section 1.2.

[12] Commission Staff Working Document, Impact Assessment Report accompanying the DGA proposal, SWD(2020) 295 final, p.3.

[13] Commission Staff Working Document, Impact Assessment Report accompanying the DGA proposal, SWD(2020) 295 final, Section 1.1, p.1.

[14] Commission Staff Working Document, Impact Assessment Report accompanying the DGA proposal, SWD(2020) 295 final, Section 2.3, p. 17.

[15] Commission Staff Working Document, Impact Assessment Report accompanying the DGA proposal, SWD(2020) 295 final, p. 6.

[16] Proposal for a Regulation on contestable and fair markets in the digital sector ("Digital Market Act"), COM/2020/842 final, 15.12.2020.

[17] Proposal for a Regulation on a Single Market for Digital Services ("Digital Services Act") and amending Directive 2000/31/EC, COM/2020/825 final.

unfair practices of online platforms having a gatekeeping role, resulting *i.a.* from their control of large amounts of data; and (ii) to facilitate mechanisms for market investigations in the digital sphere.[18] In addition, the DSA proposal aims to clarify the responsibilities and obligations of online platforms, with regard to *e.g*. content provision and moderation[19], through *i.a.* a revision of the e-Commerce Directive.[20]

The adoption of the DGA proposal by the EC is based on the observation that the following prevalent obstacles interfere with data sharing. Firstly, while data intermediaries in the broad sense (such as data marketplaces, platforms, trusts, and personal data intermediaries) can facilitate data sharing (*e.g.* by reducing transaction costs), lack of trust in their services limit their scaling-up potential. Secondly, there are several technical and legal issues related to the re-use of public sector data, especially when data are subject to the rights of third parties. An example can be personal data protection or intellectual property rights. Public sector bodies often do not have the capabilities to design technical mechanisms aimed at finding the right balance between making data available for re-use, while protecting the rights of third parties (*i.e.* "safe reading rooms").[21] Thirdly, while individuals would be increasingly willing to share 'their' personal data "for the common good and research", such initiatives would remain under-developed if there are no data sharing mechanisms in place, such as clear rules and processes at EU or Member State level. The lack of a proper legal environment impedes activities of the organisations conducting such data-sensitive activities. Finally, the EC points to many technical problems that hinder data sharing, such as the lack of cross-sectoral interoperability, the limited ability to obtain reusable data, and the uncertainty about data quality.[22] That is also why, according to the EC, with an increasing digitalisation of the economy and society, there is a risk of uncoordinated legislative intervention among the Member States that may, in turn, lead to fragmentation of the internal market.[23]

In order to tackle these obstacles, the DGA proposal consists in the following 3 main pillars. First, the DGA proposal creates a compulsory notification regime applying to a range of data sharing services. Second, it introduces a voluntary registration regime applying to data altruism services. In this way, the DGA proposal should ensure trust in data sharing and data intermediaries, to the benefit of both these intermediaries and their users (individuals and companies). Third, viewed as a complement to the Open Data Directive which mandates public sector bodies to share the data that they hold, the DGA proposal creates a legal regime for the re-use of public sector data which are subject to the rights of third parties.

[18] Commission Staff Working Document, Impact Assessment Report accompanying the DGA proposal, SWD(2020) 295 final, p. 6.

[19] Commission Staff Working Document, Impact Assessment Report accompanying the DGA proposal, SWD(2020) 295 final, p. 6.

[20] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ("e-Commerce Directive"), OJ L 178/1.

[21] Commission Staff Working Document, Impact Assessment Report accompanying the DGA proposal, SWD(2020) 295 final, p. 12-13.

[22] Commission Staff Working Document, Impact Assessment Report accompanying the DGA proposal, SWD(2020) 295 final, Section 2.

[23] Commission Staff Working Document, Impact Assessment Report accompanying the DGA proposal, SWD(2020) 295 final, point 3.1.

With the DGA proposal, the EC aims to enable the emergence of an "alternative model to data handling practices of the Big Tech companies".[24] This model should "meet new market demands and allow the EU to become more competitive in the data-driven world economy". It should further "be built on a division of functions and the development of common European data spaces as collaborative ecosystems in which data would be usable by a broader range of organisations […] based on a collective governance of data sharing".[25] To prevent fragmentation between the Member States but also between sectors, the DGA proposal establishes a 'European Data Innovation Board', which will be in charge of supporting data-driven innovation.

This White Paper offers an academic perspective to the discussion about the DGA proposal, as adopted by the EC. It provides a critical legal analysis of the DGA proposal, and it formulates recommendations to amend shortcomings that were diagnosed. The White Paper does not discuss the subsequent versions of the text issued during the legislative process,[26] but it refers to them where necessary. Although the White Paper aims to cover the full spectrum of the DGA proposal, the authors focus more specifically on the following items.

Section 2 gives a critical look into some of the definitions of the DGA proposal namely "data", "data holder" and "data user". While they constitute the basic components of the entire text, their interpretation raises fundamental questions.

Section 3 analyses Chapter II of the DGA proposal, which relates to "the re-use of certain categories of protected data held by public sector bodies" ("PSBs") along the following lines. It discusses the unclear normative value of the provisions, which results from a cascade of subsequent 'may' and 'shall' provisions incumbent on the PSBs. Then, it unveils the risk of overlap between the Open Data Directive and the DGA proposal, to the detriment of both texts. This section also looks into the extent to which the DGA proposal constitutes a continuation or, conversely, a breakpoint *vis-à-vis* the PSI Directive as then recast by the Open Data Directive. This concerns two items, namely the modalities under which data should be made available to data re-users on the one hand and the (more or less active) role of the PSBs on the other. Finally, the section discusses the proposed regulation of international transfer of non-personal data held by PSBs to third countries.

Section 4 analyses Chapter III of the DGA proposal relating to the requirements applicable to data sharing services. It first analyses the notion of data sharing services providers, covering data intermediaries and data cooperatives. In that context, inspired by the Horizon 2020 EUHubs4Data Project, it provides a practical example of what would constitute a data intermediary. Second, it looks into the applicable legal regime and critically examine the specific conditions applicable to data sharing services providers, in the light of sector-specific legislation and EU competition law. In particular, the authors analyse the neutrality obligation in its two manifestations, namely the cross-usage of data prohibition and the structural separation obligation. In addition, the authors analyse the obligation for fair, transparent, and non-discriminatory access to their services, and take note of an asymmetric

[24] Commission Staff Working Document, Impact Assessment Report accompanying the DGA proposal, SWD(2020) 295 final, p. 6.

[25] Commission Staff Working Document, Impact Assessment Report accompanying the DGA proposal, SWD(2020) 295 final, p. 11.

[26] At the time of writing, the Council of the European Union discusses the Presidency compromise text of 22.02.2021 (Interinstitutional File: 2020/0340(COD)). The Committee on Industry, Research and Energy of the European Parliament ('ITRE' committee) delivered a Draft Report which includes an amended text of 26.03.2021 (Interinstitutional Fine: C9-0377/2020 - 2020/0340(COD)).

obligation of continuity of service, which could equate data sharing services providers to "public service" providers. Finally, the inclusion of a form of *actio revendicatio* on data entrusted to data sharing service providers is discussed.

Section 5 analyses Chapter IV of the DGA proposal relating to data altruism and the regulation of "data altruism organisations". The analysis is based, where appropriate, on illustrations from health research, which is one of the main areas in which data altruism is expected to take place. It especially discusses core notions of the data altruism regime, such as the notion of 'data altruism consent' and its relation to the 'GDPR consent', and the ' purposes of general interest' including their relation to the notion of 'public interest' in the GDPR. Although the scope of data altruism extends to all types of data, there seems to be an implicit focus on personal data. The analysis also extends to the newly created 'data altruism organisations' and their role in the data value chain, whether the legal regime provided by the DGA proposal for such organisations may genuinely bring trust to data holders and data users and thereby incentivize the creation of a data altruism environment. Since the scope of the GDPR and the DGA proposal somehow overlap with respect to data altruistic behaviours of data subjects concerning 'their' data, the analysis finally questions the added-value of the DGA proposal for data subjects to be empowered, compared to the rights afforded to them by the GDPR.

Section 6 discusses several issues concerning the new European Data Innovation Board that the EC seeks to establish with the DGA proposal, as well as the competent bodies Member States would be required to designate (Chapter VI of the DGA proposal). In particular, the apparent lack of confirmation of the competences of the EDPB with regards to personal data and anonymisation efforts is discussed, which could lead to an obfuscation of competences between the EDPB and the European Data Innovation Board. With regards to data altruism, this section questions the need for a separate competent body, given the already identified implicit focus on personal data.

Section 7 first addresses the legal regime regulating the access to non-personal data by third country law enforcement authorities, under Art. 30 of the DGA proposal. On the one hand, it analyses the scope and nature of the obligations imposed on entities involved in data sharing activities subject to requests for access issued by foreign law enforcement authorities. On the other hand, it discusses the interplay between this regime and foreign laws with extraterritorial reach designed to get access to sough-after data, such as the US Cloud Act. Second, Section 7 looks into the penalties applicable to infringements of the DGA, under Art. 31 of the DGA proposal.

After analysing some of its specific provisions, the eighth and last section of the White Paper draws general conclusions on the DGA proposal. This section identifies a pattern with the DGA proposal, namely the (new) regulation of data as an object, and even more so, as an object of rights. This approach may contribute to exacerbate the risk of contradictions of the DGA proposal with the GDPR on the level of principles. Second, it discusses the relationship of the DGA proposal vis-à-vis the (regulation of) European data spaces and more generally its place in the two-pillars approach of the EC, between horizontal (sector-agnostic) and sectoral regulation of data. Finally, it identifies the DGA proposal as a cornerstone of the new EU 'digital sovereignty' policy.

2 Definitions

This section focuses on some of the definitions embedded in Art. 2 of the DGA proposal, especially the ones which raise general interpretation issues, namely 'data', 'data holder' and 'data user'.

2.1 A broad definition of 'data'

EU law lacks a uniform definition of data.[27] The DGA proposal adds another layer of inconsistency between various secondary laws, by laying down yet another definition. The DGA proposal defines 'data' as "*any digital representation of acts, facts or information and any compilation of such acts, facts or information, including in the form of sound, visual or audiovisual recording*".[28] The DGA proposal definition of 'data' differs from the often referred-to definition from the ISO, which equates data with "*a reinterpretable representation of information in a formalized manner, suitable for communication, interpretation or processing [...]*", with examples such as weather data or research data.[29] The ISO definition targets data at the syntactic level of information (the bits and bytes).

First, the DGA proposal refers to 'data' as "*a digital representation of acts, facts or information*". It is however unclear what a 'representation of acts [or] facts' means, as these would always consist of information (about such acts or facts). Second, the DGA proposal definition of 'data' is striking in that it comprises not only the "*digital representations of acts, facts or information*" *as such* but also "*compilations*" of them. The notion of compilation is unclear and rarely used to define 'data'. It is unclear whether it refers to databases, defined in EU law as a "collection" of, *i.a.*, data,[30] to datasets, to aggregated data or squarely to content or services in digital form, as the reference to "*sound, visual or audiovisual recording*" suggests? In the latter case, the definition of data would extend to the semantic level of information (the content conveyed by digital means) rather than on its syntactic level. With "*compilations*", the focus may therefore extend beyond individual data, namely a single datum, *as such* to include some (any) content with the sole condition that it would be in a digital form.

Given the obvious pivotal role of 'data' throughout the DGA proposal, the lack of clarity and precise boundaries of the definition is highly problematic and should imperatively be fixed i.e., by bringing it into line with the ISO definition. Or else, the DGA may turn out to be unworkable. Without further justification, there is no reason to broaden the definition of 'data' (namely, to 'compilations') beyond the broadly-shared understanding of this term.

Finally, it should be noted that this broad definition of data includes both personal and non-personal data. They are then regulated as distinct regulatory objects throughout the DGA proposal, despite the strong scholarly arguments raised against this regulatory approach as already experienced in the Free-Flow of Non-Personal Data Regulation.[31] Because of the highly contextual nature of the qualification

[27] On that, see the seminal work of Streinz: Thomas Streinz, The Evolution of European Data Law, in *The Evolution of EU Law*, Craig and de Burca (eds.), Oxford University Press, 3rd ed. 2021 (*forthcoming*).
[28] DGA proposal, Art. 2(1).
[29] ISO/IEC 2382-1:1993, as then replaced by ISO/IEC 2382:2015 standard.
[30] Directive 96/9/EC on the legal protection of databases, OJ L 77/20, Art. 1(2).
[31] Regulation (EU) 2018/1807 on a framework for the free flow of non-personal data in the European Union, OJ L 303/59.

of data as 'personal', it is indeed often difficult to set clear-cut and decisive boundaries between the two types of data,[32] especially when gathered in 'mixed datasets'.

2.2 The problematic notion of 'data holder'

The notion of 'data holder' is a central concept in the DGA proposal. However, it is likely to give rise to numerous interpretation issues. 'Data holder' is defined as "*a legal person or data subject who, in accordance with applicable Union or national law, has the right to grant access to or to share certain personal or non-personal data under its control*".[33]

First, the question is whether the DGA proposal definition of 'data holder' refers to 'data subject' in the meaning of the GDPR, namely the identified or identifiable natural person to whom personal data relates to. Such interpretation would exclude from the 'data holder' definition natural persons who 'hold' non-personal data, unless the DGA proposal assumes a broader meaning of the notion 'data subject'. When the definition of 'data holder' is read in conjunction with other articles (e.g. Article 5(6), Article 7(2)(c), Article 11(3) DGA proposal and the provisions related to data altruism), it becomes obvious that in fact, not all types of 'data holder' can freely share all types of data.[34] These provisions most often refer to 'consent of the data subjects' and/or 'permission' of legal entities. This seems to suggest that sharing of non-personal data by natural persons does not fall under the scope of the DGA proposal and it is left to be regulated elsewhere, i.e., the Free flow of non-personal data regulation.[35] This realization is especially relevant in the context of 'data altruism' (see subsection 5.1.2 below).

Second, it is unclear whether the DGA proposal definition of 'data holder' follows what could be called a 'facts-based' or a 'rights-based' approach. The common sense understanding of 'hold' (or holdership) follows a facts-based approach, especially concerning data. Following this approach, holdership is a factual situation where a person merely 'has' something, whether she would 'possess' it in the case of a tangible object or have access and some factual ability to use it in the case of an intangible one. In contrast, a rights-based approach would suggest that the holder would have legal rights allowing her to conduct certain activities with data, *i.e.* to 'grant access' to it and/or to 'share' it as literally expressed in the DGA proposal definition. The references to 'data holder' throughout the DGA proposal are not consistent in that respect. Chapter II refers to "*protected data* held by *PSBs*"[36] (authors' emphasis), therein following a facts-based approach. Such an approach is in line with the Open Data Directive which bases PSBs' obligations to make documents available for further re-use, on their factual

[32] See Inge Graef, Raphael Gellert and Martin Husovec, Towards a Holistic Regulatory Approach for the European Data Economy: Why the Illusive Notion of Non-Personal Data is Counterproductive to Data Innovation, TILEC Discussion Paper 2018-029, 2018; Joseph Drexl, Legal Challenges of the Changing Role of Personal and Non-Personal Data in the Data Economy in *Digital Revolution - New Challenges for Law: Data Protection, Artificial Intelligence, Smart Products, Blockchain Technology and Virtual Currencies*, Alberto Di Franceschi, Rainer Schulze (eds.), C.H. Beck und Nomos, 2019, 19 - 41.

[33] DGA proposal, Art. 2(5).

[34] As regards 'permission' to re-use data, the EDPB and EDPS also noted that "it is unclear in most cases whether the object of the permission would be the re-use of personal or non-personal data or both", see 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), p. 13.

[35] 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 L 303, 28.11.2018, p. 59–68.

[36] DGA proposal, title of Chapter II and Art. 3(1).

'holdership'.[37] However, this stands in contrast with the *literal* reading of the DGA proposal. There, the 'data holder' definition, which pleads in favour of a rights-based definition of data holdership, refers to the 'right' to grant access to or to share data. The reference in the same Chapter of the DGA proposal to 'third parties' holding certain rights on data (IPRs, commercial confidentiality, statistical confidentiality, or personal data protection)[38] as 'data holders' appears to follow a rights-based approach. As a result, the same data is deemed to be simultaneously held by both PSBs and 'third parties', based on contradictory approaches, which seriously obfuscates the understanding of the DGA proposal.

Should the definition of 'data holder' follow a rights-based approach, as the literal reading suggests, then 'compilations of data' (see definition of 'data' above) could indeed be covered by *i.a.* (intellectual) property rights. However, most individual data within the meaning of the commonly-used ISO definition of data cannot be the object of 'rights to grant access and/or to use'. Such data is generally not considered as property as such, which would typically include rights to grant access and/or share as part of the rights attached to the property. Moreover, it is generally agreed in the scholarship[39] that individual data cannot qualify as a trade secret within the meaning of the Trade Secret Directive.[40] Specific rights to grant access to data and/or to share it are also non-existent as of now. It remains to be seen whether such rights could be created by the upcoming Data Act. As a result of an (assumed) rights-based approach, individual data would be out of the scope of the DGA proposal, which would water down entire sections of the DGA proposal referring to it (see for instance the whole Chapter III on data sharing services).

Assuming a rights-based approach of the definition of data holder leaves another question open, namely whether such an approach would follow a 'positive' or a 'negative' understanding of rights. The 'negative rights-based approach' implies that a party has (non-exclusive) legal entitlements to prevent data access and sharing. The 'positive rights-based approach' implies that a party has legal entitlements allowing her to grant access to and/or share data. The reference to 'third parties' as 'data holders' in Chapter II of the DGA proposal is based on the existence of negative rights, namely rights to prevent data access and/or sharing with the exception of IPRs to grant exclusive rights to exploit data. Based on trade secrets protection or commercial confidentiality, the legal beneficiary of such protection may legally prevent the PSB from making data available for further access and re-use by data re-users but do not have positive rights to i.e. share data. The distinction is far from trivial. While *i.e.* commercial confidentiality to the benefit of party A may legally prevent the PSB from sharing data to data re-users, this does not mean that party A can *ipso facto* grant access and/or share data. Indeed,

[37] The question whether the documents would be burdened by rights held by third parties (such as data protection rights or IPRs) is discussed only at a later logical stage. Directive (EU) 2019/1024 of 20 June 2019 on open data and the re-use of public sector information, OJ L 172/56, see Art. 1.

[38] DGA proposal, Art. 5(13).

[39] The value of data is generally agreed to lie in the *aggregation* of data rather than with individual data. In any case, the value of data is generally not attached to individual data being kept secret, especially in the Big Data context when dealing with 'trivial' data. This is based on this observation that many scholars deny the possibility for such single or individual data to satisfy the condition laid down in Art. 2(1)(b) Trade Secrets Directive and therefore to qualify as 'trade secret' as such. See Josef Drexl, Designing Competitive Markets for Industrial Data – Between Propertisation and Access, JIPITEC, 2017(8), 257-292; Herbert Zech, Data as a Tradeable Commodity, in *European Contract Law and the Digital Single Market: The Implications of the Digital Revolution*, Alberto Di Franceschi (ed.) Intersentia, 2016, 51-80.

[40] Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure, OJ L 157/1.

the *same data* could i.e. also qualify as personal data, which could simultaneously prevent further access to and sharing data to data re-users.

With respect to data subjects, assumed to potentially qualify as 'data holders', 'the right to grant access' raises another question. Such a 'right' is neither defined in the DGA proposal, nor any other data-related legislation at the EU level. The right *of* access is, on the other hand, one of the rights of data subjects (but not of a legal person) under the GDPR.[41] It provides a data subject the right *to access* personal data relating to him or her which have been collected by another person.[42] The scope of the right of access according to the GDPR is therefore entirely different from the so-called right *to grant* access to certain personal or non-personal data.[43] The definition of data holder refers to both EU and national law. It may indeed be theoretically the case that some national legislations do encompass some rights to either grant access to or share certain data, but only in a piecemeal manner. Additionally, linking the data holder definition solely to national laws would risk seriously impairing the ambition of the EC to harmonise the conditions under which data can be exchanged. To conclude, the "*right to grant access to or to share […] data*" as part of the definition of data holder raises many interpretation issues which should be clarified, or else they could seriously hinder the implementation of the DGA.

Then, the 'data holder' definition provides that personal and non-personal data are under the legal person's or data subject's 'control'.[44] (Data) 'control' is referred to throughout the whole DGA proposal. As a way of illustration, the explanatory memorandum provides that the DGA proposal aims at "*empowering natural and legal persons by giving them a better overview of and control over their data*". Rec. 26 also mentions [bringing] "*more control for data holder and data users*". However, the notion of 'control' – even though so often referred to - is neither defined in the DGA proposal nor in any other EU policy and legislative document. Both its normative and regulatory implications remain notoriously unclear when it comes to data. Who can be said to have 'data under control'? Again, should the notion of 'control' be understood under the traditional meaning applicable in a physical environment, in the sense of physical possession of an object (excluding simultaneous 'control' by third parties),[45] or conversely, in the sense of rights to ownership (in line with the 'facts-based' or 'rights-based' approach respectively)? As noted by UNIDROIT's working group on private law and digital assets, not all jurisdictions do share the same understanding of the term 'control', provided that they even define this term at all when it comes to data and digital assets.[46] In other words, there is simply no common understanding of the notion of 'control' concerning data. Also, the question is whether the condition to have 'data under one's control' is cumulative with the other conditions (i.e. to have a 'right to grant access' or 'right to share' data), and how to demonstrate one's 'control' over data.

[41] GDPR, Art. 15.

[42] See for instance: Jef Ausloos, Michael Veale and René Mahieu, Getting Data Subject Rights Right, A submission to the European Data Protection Board from international data rights academics, to inform regulatory guidance, JIPITEC, 20119 10(3) 283-309; Jef Ausloos and Pierre Dewitte, Shattering One-Way Mirrors. Data Subject Access Rights in Practice, International Data privacy Law, 2018 8(1), 4-28.

[43] Ibidem.

[44] Christophe Lazaroand Daniel Le Métayer, Control over Personal Data: True Remedy or Fairy Tale?, SCRIPT-ed, 2015, 12(1).

[45] The notion of 'control' is for instance used as an equivalent of 'possession' in the analogue world by the United Nations Commission on International Trade Law (UNCITRAL), in their Model Law on Electronic Transferable Records of 2018, Art. 11, see :
https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/en/mletr_ebook_e.pdf.

[46] International Institute for the Unification of Private Law (UNIDROIT), Digital Assets and Private Law Working Group, Issues Paper, Study LXXXII – W.G.1 – Doc. 2, November 2020, para 44.

Concerning personal data, this issue can be linked to the question of whether the data holder, under the DGA proposal, coincides with either the data subject or the data controller under the GDPR. On the one hand, the 'data control' narrative is about empowering the data subject with respect to 'his' or 'her' data, based on the rights afforded to them by the GDPR. The 'data control' narrative can however, be seen more as a political objective and motto rather than a description of reality. On the other hand, the data 'controller' is defined within the GDPR as, essentially, the entity being *de facto* in control of the 'why and how' of the personal data processing activities. Both the DGA proposal and the Impact Assessment convey the view that the data subjects are the data holders, thereby presuming (irrefragably?) that they are 'in control' of 'their' data by their sole quality as data subjects.

2.3 The problematic notion of 'data user'

The 'data user' is the counterpart of the 'data holder'. This notion also lacks clarity. Data user means "*a natural or legal person who has lawful access to certain personal or non-personal data and is authorised to use that data for commercial or non-commercial purposes*".[47] It follows that in order to qualify as a 'data user', one has to meet two cumulative conditions: (i) have 'lawful access' to personal or non-personal data; and (ii) be 'authorized' to use data. First, the question arises as to what constitutes 'lawful access' and who – and based on what criteria - determines whether the access is lawful. With regard to personal data, the question is whether it is the same as a 'lawful basis' within the meaning of the GDPR. If so, the next question is if it is sufficient to fulfil one of the lawful basis of Art. 6, and/or Art. 9 GDPR—in case of sensitive personal data, to meet the conditions for lawful access. Or the alternative is that the scope of the lawful access is broader than the scope of the lawful basis for the processing of personal data. Should that be the case, in order to have 'lawful access' to personal data, data users would have to comply with other GDPR provisions such as the principle of lawfulness, fairness, and transparency.

It is also unclear what 'lawful access' means in relation to non-personal data consisting of individual data (see above on the definition of 'data'). As discussed with reference to the data holder definition, such data is generally considered to not be covered by specific access and/or sharing rights. Therefore, it is not clear what a positive interpretation of having lawful access could mean. A lenient interpretation could consist of a negative definition, namely the absence of (proved) unlawful access. Such an interpretation could i.e. relate to the 'Cybercrime Directive' which explicitly regulates the unlawful access to information (shortly known as 'hacking').[48]

Then, it would mean that the data user has to be 'authorized' to use data. Given that a data user has to comply with these two conditions cumulatively, or so it seems, the question is how this authorisation is different from having a 'lawful access'. It seems that 'lawful access' constitutes the first stage while the 'authorization' relates to the following one, namely data use (for commercial or non-commercial purposes). However, such distinction between 'lawful access' and 'authorized use' of data cannot be found in personal data protection law. As a general rule, under the GDPR processing of personal data – defined as "*any operation or set of operations which is performed on personal data or a set of personal data […]*" including collection and use of data – is allowed provided there is a lawful

[47] DGA proposal, Art. 2(6).

[48] Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA, OJ L 218/8 (the 'Cybercrime Directive'), see in particular Rec. 17 and Art. 3.

basis for such processing, The GDPR regulates the processing of personal data based on the notion of 'purpose'. It does not foresee any additional, specific requirement to process ('use') data. It remains therefore unclear how the two legal frameworks interact in this respect and, concretely, what substantiates the 'authorization' of the data user. While the term suggests someone delivering some form of clearance, the other question is whether the data user gets 'authorized' to use data based on the consent of data subjects.

2.4 Conclusion

With the DGA proposal, the EC is deliberately reluctant to regulate rights on data, but at the same time, it appears to assume the existence of such rights. As for personal data, the DGA proposal is not well-aligned with the logic, principles, and rights afforded by the GDPR. As for other data ('non-personal data'), the problem rather lies in the absence of rights on data, at least concerning individual data. This brings about many uncertainties or even inconsistencies which shall be clarified.

The DGA proposal definition of 'data' is remarkably broad, as it extends not only to individual data but also to 'compilations' of them. Not only it is unclear what 'compilation' means, but also this notion is likely to extend the scope of 'data' meaning well beyond its broadly-shared definition understood as individual data consisting in bits and bytes representing some information. The definition of data should be clarified, given its pivotal role in the DGA proposal. Also, the particularly broad understanding of 'data' in the DGA proposal may logically result in the DGA having an (unexpectedly?) broad scope. This may for instance complicate the understanding of what 'data sharing service providers' are and how to distinguish them from other services providers in the digital environment.

Moreover, the DGA proposal should further clearly define what 'right to grant access' and 'right to share' data mean, as core components of the definition of 'data holder'. It should especially clarify whether such rights consist of positive, or negative rights, and what is the legal position of data holder *vis à vis* rights of the third parties to the given data. The interplay with the GDPR should also be clarified with respect to whether and how the 'right to grant access' is related to the data subjects' 'right of access'. Also, it remains unclear whether the notion of 'control' in the DGA proposal definition of data holder refers to the (expected) data subjects' 'control' over 'their' data or the factual control of 'data controllers' under the GDPR. In other words, the question is what the data holder, the data subject, or the data controller may mean within the conceptual framework of the GDPR.

Concerning the definition of 'data user', clarification on the scope and meaning of 'lawful access' is needed for both personal and non-personal data. In particular, with regard to personal data, it should be determined whether 'lawful access' amounts to the 'legal basis' for data processing as stated in the GDPR, or not.

Further explanation on 'data holder' and 'data user' definitions is also needed in the context of 'data sharing' defined as "*the provision by a data holder of data to a data user for the purpose of […] use of the shared data […]*".[49] One could wonder to what extent the data user should know whether the data holder actually has "the right to grant access to or to share data […] under its control". The question is whether the data user's access to data would be 'unlawful' based on the fact that the data holder had such a 'right'. The DGA proposal does not specify what would be the consequences for both parties,

[49] DGA proposal, Art. 2(7).

and for data sharing activity as such, should the data user have known that his access to data is 'unlawful' or 'unauthorized'.

3 Re-use of certain categories of protected data held by public sector bodies

Chapter II of the DGA proposal pursues two goals: first, to unlock the potential of re-use of some 'data' deemed to be outside the scope of the Open Data Directive—those protected by third parties' rights. Second, to lay down the conditions under which such data can be transferred to third countries, with the purpose to protect the rights and interests of the third parties. Chapter II of the DGA proposal applies to public sector bodies ('PSBs'), defined as the State, regional or local authorities, bodies governed by public law, or associations formed by one or more such authorities, or one or more such bodies governed by public law.[50] For example, based on this definition, a city council or a public hospital would qualify as PSBs.

While the ambition of the EC with the DGA proposal is to foster the re-use of data held by PSBs, the normative value of related provisions is unclear, because provisions using the wording 'may' and 'shall' are intertwined, which is examined in a first sub-section. This is all more problematic since there is an overlap in the scope of application of the DGA proposal with the Open Data Directive, as discussed in the second subsection, which results in a lack of clarity on which obligation(s) is(are) concretely applicable to PSBs. The two following subsections analyse where the DGA proposal follows or, conversely, deviates from the approach of the Open Data Directive. On the one hand, the DGA proposal considers the *purpose* for data re-use, thereby departing from the open data approach of the PSI and then Open Data Directive. On the other hand, the DGA proposal follows a pattern that has been visible throughout the various revisions of the PSI and then Open Data Directives towards requiring PSBs to play a more active role in 'providing' data. This pattern is taken a step further here, with the possible establishment of 'data utilities'. The fifth and last subsection analyses the conditional data flow regime which the EC aims to set up for the international transfer of non-personal data protected by third parties' rights. Not only can it lead to inconsistencies, but it also remains to be further analysed whether such a strict regime complies with the EU's international trade commitments.

3.1 Purpose of the chapter and unclear normative value

The DGA proposal aims to "complement" the Open Data Directive[51] by laying down the conditions for making available data held by PSBs, which falls outside of the scope of the Open Data Directive.[52] It targets data held by PSBs that is subject to the rights of third parties, covering data protected on the ground of commercial confidentiality, statistical confidentiality, protection of intellectual property rights of third parties, and protection of personal data.[53] Data covered by the rights of third parties, allegedly excluded from the scope of the Open Data Directive, is therefore not subject to obligations for PSBs to make them available for re-use to the benefit of third parties, for both commercial or non-

[50] DGA proposal, Art. 2(11).

[51] Directive (EU) 2019/1024 on open data and the re-use of public sector information, OJ L 172/56 ('Open Data Directive'). Adopted in 2019, the Open Data Directive recast the so-called 'Public Sector Information Directive' (or 'PSI Directive) (Directive 2003/98/EC).

[52] Commission Staff Working Document, Impact Assessment Report accompanying the DGA proposal, SWD(2020) 295 final, Section 1.

[53] DGA proposal, Art. 3(1) and (2). Defense and security-related secret data remain outside of the scope.

commercial purposes under this Directive. In contrast, the DGA proposal aims to find ways to make them available for re-use to the extent possible. The Open Data Directive generally mandates PSBs to share the documents that they hold following the 'open data' approach, namely data in an open format that can be freely used, re-used, and shared by anyone for any purpose.[54] In contrast, the ambition of the EC with the DGA proposal is to find a middle ground by doing the following. First, allowing the re-use of data covered by the rights of third parties under more *granular schemes* compared to the open data approach of the Open Data Directive and, second, supporting PSBs in setting out the appropriate legal and technical arrangements to do so.

The extent of the obligations incumbent on PSBs concerning the making available for re-use of data covered by the rights of third parties is not entirely clear. The first unclarity relates to the 'cascade' nature of the legal regime. The DGA proposal states that it does neither release PSBs from respecting third-party rights on data *nor does it create obligations on PSBs to allow re-use of data, beyond the Open Data Directive*.[55] Then, in the case *where PSBs would decide to allow such re-use* ('may' provisions), they should do so pursuant to the conditions of the DGA proposal. These conditions consist of demanding legal and technical measures to protect such data, to the benefit of third parties (as discussed more in detail below).[56] Until that point, there is therefore no obligation incumbent on PSBs concerning the making available of data covered by rights of third parties for further re-use. However, where the re-use of data could as a result not be granted and, in the case of personal data, there is no other legal basis under the GDPR for transmitting them, then the PSBs "*shall* support re-users in seeking the consent of the data subjects and/or permission from the legal entities whose rights and interests may be affected by such re-use, where it is feasible without disproportionate cost for the PSB" (emphasis added).[57] It is hard to imagine how this cascade of 'may' and, then, 'shall' provisions can be sustained. Logically, the 'may' provisions (facultative options) should become 'shall' ones (legal obligations). The second unclarity relates to the nature of the legal obligation for the PSBs to support re-users in seeking the consent of the data subjects and/or permission from the legal entities, in order to allow for the re-use of data. Our understanding is the following. While there is indeed no obligation (*a fortiori* of result) for PSBs to make data covered by the rights of third parties available for re-use by potential data re-users, there are some obligations (of means), namely to take *some measures* in order to facilitate such re-use. The lack of clarity of the legal regime may however as well lead others to conclude, in the opposite direction, that the whole legal regime would be entirely facultative.[58] The normative nature of the legal regime should therefore be clarified. This is all the more required since there is a risk of overlap and therefore inconsistency between the DGA proposal and the Open Data Directive, as analysed in the following sub-section.

[54] Open Data Directive, Rec. 16.
[55] DGA proposal, Art. 3(3).
[56] DGA proposal Art. 5.
[57] DGA proposal, Art. 5(6).
[58] This seems to be the view endorsed by Antoine Petel, Publication de l'Acte sur la gouvernance des données, les propositions de la Commission européenne, Revue Lamy Droit de l'immatériel, 176, 2020, 43-47.

3.2 A risk of overlap and inconsistency between the Open Data Directive and the DGA

The relation between the Open Data Directive and the DGA proposal may not be as clear as the letter of the DGA proposal suggests. The DGA proposal is based on the assumption of a 'black or white' legal situation, where data would either be *in* the scope of the Open Data Directive *or* outside the scope.[59] In the latter case, data may fall under the scope of the DGA. In reality, there is an obvious *grey zone* where 'documents' (in the parlance of the Open Data Directive, see below) are *adapted* by PSBs to be accessed and re-used, according to the Open Data Directive, without infringing the rights of third parties (*i.e.* by deleting or anonymizing sensitive parts of a document). This may be stated in national law transposing the Directive[60] or it may be derived from the guidance from national competent authorities and Courts. With regard to personal data, adapting documents in order to accommodate the rights of data subjects is demanded by the recommendations of the (at the time) Article 29 Working Party.[61] Further, personal data (and potentially other data covered by rights of third parties, depending on national transposition and regulatory practice), should not *necessarily and systematically* be considered to fall outside of the scope of the PSI regime laid down by the Open Data Directive. Article 29 Working Party clarified that in certain circumstances, which are to be assessed on a case-by-case basis, personal data could be made available for re-use, subject to appropriate conditions and safeguards.[62]

The risk of overlap between the Open Data Directive and the DGA proposal is reinforced by the reference to "data" as a subject matter regulated in the DGA proposal. The original PSI Directive of 2003 applied to "documents", defined as "*any content whatever its medium [...]; any part of such content.*"[63] In contrast, the DGA proposal applies to "data" (see sub-section a) above; on the broad and problematic definition of 'data', see Section 2 above). The question is, therefore, whether the term "data" has replaced this of "document" *mutatis mutandis,* or whether the two terms refer to different subject matters. A concrete example may help picture the problem more clearly. Let us consider any document (e.g. a report) covering a reference to the name of an employee (that is, personal data). Such document could be made available for re-use, subject to *i.e.* removal of the name of the employee. In such a case, the question is whether this act of removal of the name of the employee and subsequent making available of the document fall under the Open Data Directive regime or the DGA. In other terms, whether the DGA proposal applies (a) to the document (report) or (b) to the data (employee's name). A literal reading of Art. 3(1) DGA proposal suggests that the accurate answer is (b), namely that the DGA proposal applies to the data covered by rights of third parties (personal data and/or to the information protected by confidentiality or IPRs) which are outside the scope of the Open Data Directive. The obligation for PSBs to act as middlemen and "support re-users in seeking the consent of the data subjects and/or permission from the legal entities whose rights and interests may

[59] See DGA proposal, Art. 3(1) and Commission Staff Working Document, Impact Assessment Report accompanying the DGA proposal, SWD(2020) 295 final, section 4.2.2.

[60] This is for example the case in France. Art. L-312-1-2 of the 'Code des relations entre le public et l'administration' (Code of relationships between the general public and public administration) mandates PSBs to anonymise or occult sensitive information (such as personal data and trade secrets).

[61] See Article 29 Working Party, Opinion 7/2003 on the re-use of public sector information and the protection of personal data - Striking the balance, 2003 and Opinion 06/2013 on open data and public sector information ('PSI') reuse, 2013.

[62] Article 29 Working Party, Opinion 6/2013 on open data and public sector information ('PSI') reuse, 2013, p. 6-7.

[63] Directive 2003/98/EC, Art. 1(1).

be affected by such re-use [...]"[64] could also fit in this understanding. However, other provisions tend to suggest otherwise. Art. 5(3) states that the PSB "*may impose an obligation to re-use only pre-processed data where such pre-processing aims to anonymise or pseudonymise personal data or delete commercially confidential information, including trade secrets*''.[65] If applied to our example, this provision implies that the regulatory subject-matter (namely, the thing that should be made available for re-use) seems to be (also?) the report (the "document", already regulated by the Open Data Directive) rather than the employee's name (the "data").

This theoretical and logical problem has concrete implications for the normative scope of the DGA proposal and for the legal burden put on PSBs. It is indeed unclear at this stage what triggers the obligation for PSBs to comply with Chapter II of the DGA. The question is should PSBs apply Chapter II of the DGA *systematically* when data covered by the rights of third parties are involved, with the ensuing risk of overlapping with the Open Data Directive regime (as implemented in the respective national legislations).[66]

3.3 From open data to purpose-based re-use of data

The DGA proposal introduces a major change to the open data approach laid down in the Open Data Directive in that the purpose for data re-use shall be taken into account, by PSBs, upon their making available. By doing so, the DGA proposal aims to extend the amount of data held by PSBs which can be re-used. However, it brings about several legal questions.

To understand the legal implications of this shift, it is first necessary to understand the limitations to the re-use of documents inherent to open data. The PSI regime is based on open data, and particularly on the making available of data for re-use by different types of re-users (potentially anyone willing to re-use them) for indefinite types of purposes, including both commercial and non-commercial ones. There is no requirement for candidates for data re-use to even *have* a pre-identified purpose in the first place. Based on the market economy principle, the Open Data Directive bets on the expectation that re-users will "*find new ways to use [the data] and create new, innovative products and services*".[67] It is commonplace that such broad re-use of data for yet unknown purposes can expose protected parties to severe interference with their rights and protected interests. With respect to data protection law, the Article 29 Working Party observed that the PSB *can* take into consideration neither the particular re-user(s) nor the intended purpose(s) for re-use, *at the time of the making available of personal data for re-use*.[68] This contradicts the purpose limitation principle at the heart of data protection law in the case of personal data.[69] To assess whether the making available for re-use would not breach data protection law, the Article 29 Working Party considers that the "any person test" should therefore be conducted.[70] The 'any person test' consists of the following. When deciding upon

[64] DGA proposal, Art. 5(6).

[65] The Impact Assessment confusingly mentions the "secondary use of public sector data that is subject to rights of others", Commission Staff Working Document, Impact Assessment Report accompanying the DGA proposal, SWD(2020) 295 final, Annex 2 (section "Results of the consultation process").

[66] Petel's interpretation is that, as per French national law, PSBs are likely to be entitled to *choose* which legal regime would be applicable to them, with a risk of cherry-picking. See Antoine Petel, Publication de l'Acte sur la gouvernance des données, les propositions de la Commission européenne, Revue Lamy Droit de l'immatériel, 2020(176), 43-47.

[67] Open Data Directive, Rec. 8. On this, see Charlotte Ducuing, Data as infrastructure? A study of data sharing legal regimes, Competition and Regulation in Network Industries, 2020, 21(2) 124–142, p. 129-131.

[68] Article 29 Working Party, Opinion 06/2013 on open data and public sector information ('PSI') reuse, 2013, p. 11.

[69] GDPR, Art. 5(1)(b).

[70] Article 29 Working Party, Opinion 06/2013 on open data and public sector information ('PSI') reuse, 2013, p. 11-12.

whether personal data shall be made available for re-use under the Open Data and PSI regime, the PSB shall anticipate the interference with the rights and freedoms of the data subjects for *any possible* purpose and by any person, or in other words in the worst-case scenario. According to Article 29 Working Party, the 'any person' test shall also guide the PSB in designing anonymisation techniques of personal data before making it available for re-use. Because the data could be mixed with *any other* dataset and that *any* data analytics technique could be used, the risk of re-identification of anonymised data is considerable. As a result of the 'any person test', it is very unlikely that personal data can be made available for re-use under the Open Data Directive. The 'any person test' also reduces the possibilities to share anonymised data, because of the high risk of re-identification.

The DGA proposal aims to overcome this obstacle to data sharing, by mandating PSBs[71] to "*support re-users in seeking the consent of the data subjects*", but also "*permission from the legal entities whose rights and interests may be affected by such re-use*".[72] Within the meaning of data protection law, consent of data subjects is purpose-specific.[73] This logically entails that PSBs would look into *particular cases and purposes* of (categories of?) data re-use and that the making available for re-use of data would be purpose-specific. Besides, the PSBs shall be able to "*verify any results of processing of data undertaken by the re-user and reserve the right to prohibit the use of results that contain information jeopardizing the rights and interests of third parties*".[74] When data is confidential, "*the PSBs shall* ensure *that the confidential information is not disclosed as a result of the re-use*".[75] In other words, the PSB shall in this case play a supervisory role *vis-à-vis* data re-users to ensure balance with the rights of third parties. This stands in sharp contrast with prior 'PSI practice' pursuant to the Open Data Directive of making data available 'as they are' without further consideration for the re-user(s) and purpose(s) of re-use.

This regulatory shift begs the question of whether the account paid to *specific* cases of data re-use could give rise to unequal treatment and discrimination between potential re-users. Art. 5(1) DGA proposal mandates PSBs to make publicly available the conditions under which data re-use is allowed. However, it remains to be seen to what extent they can truly design standardized or 'boilerplate' contractual conditions on the one hand while taking into account the specificities of data re-use on the other, or whether the only option would be for them to look into every *ad hoc* case of data re-use. The liability exposure of PSBs in case of illegitimate data re-use remains also an open question. For instance, the problem is to what extent could PSBs be exposed to liability in case of lack of surveillance of data re-users leading to a breach of confidentiality. This also puts into question the relation between the DGA proposal and the GDPR concerning the allocation of responsibilities. Namely, whether the obligations placed by the DGA proposal onto the PSBs concerning the processing of personal data have an influence on their qualification within the meaning of data protection law. Also whether the obligation to support data re-users in seeking consent from data subjects and/or to supervise data re-users results in PSBs qualifying as joint controllers (together with the data re-user). Finally, in how far should the PSB supervise the data re-user in order to be shielded from liability or in other words, what is the nature of the supervisory obligation. Would the conclusion of a non-disclosure agreement with the data re-user suffice to fulfil this obligation or should the PSB also supervise the execution of such

[71] With the assistance of the "competent body", see DGA proposal, Art. 7(1).
[72] DGA proposal, Art. 5(6). On the nature of such obligation, see sub-section 3.1 above.
[73] GDPR, Rec. 32.
[74] DGA proposal, Art. 5(5).
[75] DGA proposal, Art. 5(8).

agreement? The term "ensure" seems to point indeed to an extensive obligation of guarantee. This also points to the changing role of PSBs towards active data intermediaries.

3.4 PSBs turning into data intermediaries: towards data utilities?

The DGA proposal raises the threshold in terms of the active involvement required from PSBs to enable data re-use. It is to the extent that they are incentivised to turn into data intermediaries. The DGA proposal may even foster the emergence of what can be called 'data utilities'.

In this respect, the DGA proposal shall be viewed as a continuation and a deepening of the PSI Directive as revised in 2013[76] and then recast by the Open Data Directive in 2019. The Open Data Directive stipulates the principle that PSBs shall make documents available for re-use "*in any pre-existing format or language*", or in other words 'as they are'. However "*where possible and appropriate, [they shall make them available] by electronic means in formats that are open, machine-readable, accessible, findable and reusable, together with their metadata*".[77] The Open Data Directive introduced a second exception for "dynamic data",[78] which shall be made available for re-use "*immediately after collection, via suitable APIs and, where relevant, as a bulk download*".[79] Thirdly, the Open Data Directive introduced yet another exception for "high-value datasets" to be identified by the EC in implementing acts.[80] Upon identification as "high-value datasets", datasets shall be made available for re-use by PSBs in principle free of charge, and, in a machine readable format via APIs, and provided as a bulk download where relevant. Finally, the Open Data Directive makes it mandatory for the Member States to encourage PSBs to produce and make available documents in accordance with the principle of "*open by design and by default*".[81] While the expression is not defined in the Directive, it logically implies that PSBs shall already consider the possibilities for data re-use *at the stage of data production*.[82] To sum up, from mere making available data produced (somehow incidentally) throughout other activities in the original PSI regime, PSBs have increasingly been requested to become *active* providers of data in the data economy.

The DGA proposal takes this pattern a step further. PSBs are required to further bridge the gap between the *initial* use of data and its *re-use*. This entails to provide and arrange for a secured environment for data re-use, to arrange the anonymisation or pseudonymisation of personal data or delete commercially confidential information, to supervise the re-use of data (by the data re-users) in order to prevent re-use detrimental to the rights of third parties and to ensure that confidential information is not disclosed as a result of the re-use, and, finally, to assist data re-users in seeking consent or, respectively, permission, to re-use personal data or information protected by IPRs or confidentiality.[83] The DGA proposal thereby goes beyond the Open Data Directive as follows. Not only shall PSBs curate data (both technically and legally) with a view to their re-use, they are now also

[76] See PSI Directive as recast by Directive 2013/37/EU, Art. 2(6) and Art. 5.
[77] Open Data Directive, Art. 5(1).
[78] Dynamic data are defined as digital documents "subject to frequent or real-time updates" such as "data generated by sensors", Open Data Directive, Art. 2(8).
[79] Open Data Directive, Art. 5(5).
[80] Open Data Directive, Chapter V. At the time of writing, the EC has not (yet) identified "high-value datasets".
[81] Open Data Directive, Art. 5(2).
[82] See Opinion of the IMCO Committee of the European Parliament for the ITRE Committee of 19 October 2018 […], Rapporteur for opinion: Julia Reda, para II.A.
[83] DGA proposal, Art. 5.

expected to *tailor* such activities to the *specific* data re-use and data re-user purpose for data processing. They shall accommodate *in concreto* the rights and legitimate interests of protected third parties on the one hand (data subjects and holders of IPRs or trade secret rights) and data re-users on the other hand.

The more active role increasingly expected from PSBs raises a number of questions. First, whether PSBs are able to deal with this new role as a data intermediary. PSBs are by definition not data professionals and it may be challenging and costly for them to gather the required legal and technical capabilities, such as a "*secure processing environment*".[84] Additionally, whether it is it *fair* to burden them with such far-reaching obligations, should these indeed constitute *obligations* and not mere *incentives* (on this, see sub-section a) above). Originally, their role under the PSI regime was limited to a mere (passive) making available of documents 'as they are' for further re-use. The underlying idea was that the elaboration or collection of such documents throughout public service activities had been financed by public money and should therefore be shared back with the public. An active role of PSBs shatters this rationale by requiring PSBs to engage proactively in re-use-specific data intermediation characterized by delicate balance to be found between the rights of third parties and those of data re-users. As explained above, this new activity brings about additional legal risks. But at the same time, PSBs have little to gain from this (side) activity since their economic perspectives are curtailed by strict charging regulation.[85] In this case, they may ultimately be trapped into a 'lose-lose' situation, which could also have a chilling effect on their willingness to engage decisively in such data intermediation activities.

It remains to be seen whether the establishment of (a) "competent body(ies)" could alleviate these risks. The DGA proposal mandates the designation of one or several "competent body(ies)" to support PSBs, whether centralized or sector-specific.[86] The competent bodies shall provide technical and legal support for PSBs to comply with their obligations. Member States may even *substitute* PSBs by the competent bodies in compliance with DGA obligations to make data available for re-use.[87] Such entrustment of competent bodies with DGA obligations of PSBs may very well alleviate the feasibility risk. As opposed to PSBs, the competent bodies shall indeed "*have adequate legal and technical capacities and expertise to be able to comply*" with their obligations.[88] Their data activities are expected not to be a mere side activity but to constitute the core of their mandate. Although not regulated in the DGA proposal, *dedicated* funding should logically be consequently allocated to them by the State. The entrustment of competent bodies with such data activities would also logically move the responsibility and liability exposure (discussed above) from the PSBs to them. The entrustment of competent bodies with PSBs' obligations should therefore be welcomed as a logical and fair apportion of responsibilities. It can be viewed as both the recognition and the result of the long-standing shift of the role of PSBs, from passive 'making available of data for further re-use' to active data intermediation for the public interest. This being said, such entrustment is not mandated by the DGA but constitutes an option for the Member States, which they may choose not to activate (i.e. due to financial costs likely to be incurred as a result).

[84] DGA proposal, Art. 5(4)(a).
[85] DGA proposal, Art. 6.
[86] DGA proposal, Art. 7.
[87] DGA proposal, Art. 7(3).
[88] DGA proposal, Art. 7(4).

Interestingly, the entrustment of competent bodies with such far-reaching competencies would also establish them as data utilities, in the sense of data intermediaries acting in the general interest. Beyond the DGA, a growing pattern towards entrusting (some) public authorities with (a range of) roles as data intermediaries for general interest purposes can be observed on behalf of policy-makers, both at the EU and national level. In its Data Strategy, the EC emphasizes many times the need to have EU "data infrastructures". It has also further attempted to support the emergence of a European federation of 'data hubs' to support the Common European Data Space as part of the Research and Innovation Programme.[89] This initiative led to the creation of "EUHubs4Data", the "European federation of Data Driven Innovation Hubs". EUHubs4Data is an EU-funded private initiative, rather than a public authority, which is aimed to constitute the supporting federation for data services and data sharing in order to break data silos. It is expected to provide the underlying open, neutral, and *sustainable* infrastructure for data hubs to rely on across the EU,[90] which may bring it closer to a 'data utility' at some point. At the national level, a recent example can be found with the Flemish plan for the economic post-Covid relaunch. The plan includes the creation of a data utility company ('data nutsbedrijf'), which shall act as a neutral third party to support data sharing by public and private entities in the data economy.[91] France has set up a data public service ('service public de la donnée') in 2016,[92] in charge of the centralised making available of 'reference data', deemed to constitute an essential infrastructure, to the benefit of both public and private entities.[93] The DGA stands in line with this broader pattern in the EU, which should be further analysed.

3.5 The regulation of international transfer of non-personal data held by PSBs and possible inconsistencies

The DGA proposal introduces a legal framework to regulate international transfers of certain categories of non-personal data held by PSBs. This regime aims at increasing trust in data sharing by ensuring the protection of data rights holders' interests as well as public policy objectives such as public health.[94] However, it remains to be seen whether it is in line with the EU's international trade commitments.

For the purposes of international transfers, the DGA proposal distinguishes between two categories of non-personal data held by PSBs, namely 'commercially sensitive' data and 'highly sensitive' data, each category being subject to specific conditions.[95]

First, transfers of non-personal 'commercially sensitive' data notably covering trade secrets and content protected by IP,[96] are subject to either an adequacy or an accountability system. Under the

[89] See the call: https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/dt-ict-05-2020.
[90] See EUHubs4Data website: https://euhubs4data.eu/#
[91] Vlaamse Veerkracht, Relanceplan Vlaamse Regering, 2020: https://www.vlaanderen.be/publicaties/relanceplan-vlaamse-regering-vlaamse-veerkracht
[92] Loi n° 2016-1321 du 7 octobre 2016 pour une République numérique (1), Art. 14.
[93] See the website of the "Service public de la donnée", https://www.data.gouv.fr/fr/reference.
On this, see Maxime Boul, Réflexions sur la notion de donnée publique, Revue française d'administration publique 2018/3, 2018(167), 471-478 and Céline Beguin-Faynel, Rapport de synthèse, Elise MOURIESSE (dir.), L'open data : une évolution juridique ?, Revue générale du droit, Etudes et réflexions 2018.
[94] DGA proposal, Rec. 14 and 19.
[95] DGA proposal, Rec. 15 and 19.
[96] DGA proposal, Rec. 15.

adequacy system, transfers to third countries may take place based on implementing acts of the EC declaring that the relevant third-country provides appropriate safeguards for the use of data.[97] Where no implementing act was adopted, the transfer may take place under an accountability system. In this case, the re-user shall undertake obligations in the interest of protecting the data. In that respect, the re-user shall ensure that, even after the data is transferred to the third country : (i) the data is re-used in compliance with IP rights; and (ii) when the data is considered confidential, that the confidential information is not disclosed as a result of the re-use. In addition, the re-user shall accept the jurisdiction of the court of the Member State of the PSB for the judicial settlement of disputes.[98]

It could be argued that the foreseen mechanism of adequacy decisions to be issued by the EC may lead to a ban or serious restrictions of international transfers of 'commercially sensitive' data as adequacy systems have significant drawbacks such as the length of the process and the influence of the political factor which may translate into a very limited implementation of the system.[99] Also, even though the DGA proposal provides for an accountability system in cases of absence of adequacy decision, the obligation for the re-user to bear responsibility for the protection of the data, even after the data is transferred to the third country, may have a 'chilling effect' on international transfers. It shall also be noted that the DGA proposal shall clarify who shall the re-user commit to, whether it is the PSB that granted the right to re-use or the third party holding rights on the data.

Second, non-personal 'highly sensitive' data, for instance certain datasets held by actors in the public health system, may be subject to stricter conditions to be transferred to third countries, in the case such transfer could jeopardize public policy objectives.[100] This type of 'highly sensitive' data should be defined by Union law, for instance in the context of relevant sectoral legislation (such as European Health Data Space).[101]

The conditions attached to the transfer of such data to third countries should be laid down in delegated acts adopted by the EC and may include limitations as regards the re-use of data in third countries, categories of persons that are entitled to transfer such data to third countries or who can access the data in the third country.[102] In exceptional cases, these acts could also include restrictions on transfers to third countries to protect the public interest.[103] In the latter case, it may amount to a ban on international transfers of such 'highly sensitive' data.

In addition, this regime implies that 'highly sensitive' data shall be defined according to the EU legislative procedure in order for the EC to be allowed to adopt delegated acts laying down the conditions relating to international transfers of such data. This suggests that all protected non-personal data held by PSBs that have not yet been identified as 'highly sensitive' and subject to the relevant

[97] Namely that the legal, supervisory and enforcement arrangements of a third country : (a) ensure protection of intellectual property and trade secrets in a way that is essentially equivalent to the protection ensured under Union law; (b) are being effectively applied and enforced; and (c) provide effective judicial redress (DGA proposal, Art. 5(9)).

[98] DGA proposal, Art. 5(10).

[99] As it can be noted with regard to the adequacy mechanism under which personal data may be transferred to third countries, in accordance with Chapter V of the GDPR.

[100] DGA proposal, Art. 5(11) and Rec. 19.

[101] DGA proposal, Art. 5(11) and Rec. 19.

[102] DGA proposal, Art. 5(11) and Rec. 19.

[103] DGA proposal, Art. 5(11).

delegated act may thus be considered as 'commercially sensitive' data and transferred to third countries according to the adequacy or the accountability systems.

The rationale for creating this legal framework to regulate international transfer of protected non-personal data is allegedly the protection of trade secrets, IP rights as well as public policy objectives.[104] It may however raise compliance issues with regard to the EU's trade commitments, notably under the General Agreement on Trade and Services ("GATS") that governs international trade in services and aims at liberalizing cross-border flow of services, including digital services.[105]

In its schedule of specific commitments under the GATS,[106] the EU committed to grant market access[107] and national treatment[108] with regard to the sector of computer and related services, covering data processing services[109] and for the four modes of supply of a service covered by the Agreement,[110] including cross-border trade. It follows that the EU shall not adopt or maintain measures that hinder the access to data processing services (market access) and shall accord foreign providers of data processing service treatment no less favorable than it accords to its own like service providers (national treatment).

In the event that the implementation of the conditional data flow regime would lead to a *de facto* impossibility to transfer non-personal data held by PSBs to third countries, cross border trade with regard to data processing services would not be ensured which would constitute a breach of the market access obligation. In addition, foreign data processing operators would not be able to offer their services unless the processing takes place in the EU. As a result, they might be forced to invest in EU based facilities to access the market. Foreign operators could thus be subject to a less favourable treatment as the implementation of the regime could modify the conditions of competition between EU and foreign operators, to the detriment of the latter.[111]

[104] DGA proposal, Rec. 14 and 15.

[105] Under Article I. 3(b) of the GATS, the GATS cover any service in any sector except services supplied in the exercise of governmental authority.

[106] Under the GATS, some obligations such as the market access and the national treatment obligations, may apply only to the extent that specific commitments have been taken by a WTO Member. These commitments are stated in a 'schedule of specific commitments'. For the EU, see WTO, GATS/SC/157, 2019.

[107] GATS, Art. XVI(1):"With respect to market access through the modes of supply identified in Article I, each Member shall accord services and service suppliers of any other Member treatment no less favourable than that provided for under the terms, limitations and conditions agreed and specified in its Schedule".

[108] GATS, Art. XVII(1): "In the sectors inscribed in its Schedule, and subject to any conditions and qualifications set out therein, each Member shall accord to services and service suppliers of any other Member, in respect of all measures affecting the supply of services, treatment no less favourable than that it accords to its own like services and service suppliers."

[109] Except MT (unbound) and, for some specific services LV and SK with regard to market access and except MT (unbound) with regard to national treatment; see EU schedule of specific commitments, WTO, GATS/SC/157, 2019, p. 58-62, available here : https://docs.wto.org/dol2fe/Pages/SS/directdoc.aspx?filename=q:/SCHD/GATSSC/SC157.pdf&Open=True.

[110] There are different means through which services are supplied. The GATS covers the four following modes of supply : cross border trade, consumption abroad, commercial presence and presence of natural persons. Indeed, under Article 1 (2) of the GATS, the trade in services is defined as the supply of a service : (a) from the territory of one Member into the territory of any other Member; (b) in the territory of one Member to the service consumer of any other Member; (c) by a service supplier of one Member, through commercial presence in the territory of any other Member; Page 286 (d) by a service supplier of one Member, through presence of natural persons of a Member in the territory of any other Member.

[111] As Art. XVII (3) states that "Formally identical or formally different treatment shall be considered to be less favourable if it modifies the conditions of competition in favour of services or service suppliers of the Member compared to like services or service suppliers of any other Member."

The GATS however contains the General Exceptions provision that allows WTO Members to depart from their commitments.[112] In this respect, measures in breach of the obligations to grant market access and national treatment may be justified if they are (i) necessary to (a) protect public policy objectives[113] (e.g. environment, health); or (b) secure compliance with laws or regulations that are not inconsistent with the provisions of the GATS;[114] and (ii) provided that such measures are not applied in a manner that would constitute a means of arbitrary or unjustifiable discrimination between countries where same conditions prevail, or a disguised restriction on trade in services.[115]

It could be argued that the measures regulating international transfers of non-personal data held by PSBs may be justified, on the one hand, as securing compliance with IP and trade secrets laws concerning 'commercially sensitive' data and, on the other hand, as protecting public policy objectives such as public health concerning 'highly sensitive' data.

However, it should be stressed that the assessment of a measure inconsistent with a WTO Member's commitments by the WTO adjudicating bodies on the basis of this General Exceptions provision is carried out according to a strictly trade-oriented interpretation.[116] As result, little room is left for domestic regulatory intervention that aims at protecting societal and political values and may incidentally affect international trade.[117]

While no definitive conclusion can be drawn at this stage, it remains to be seen whether and if so, to what extent, the conditional data flow regimes introduced by the DGA proposal to frame international transfers of non-personal data held by PSBs may be conflicting with international trade rules.

3.6 Conclusion and recommendations

Just like for other parts of the DGA proposal, the lack of clarity of some provisions appears to be a major hindrance. Concerning chapter II of the DGA proposal, the normative value of the provisions raises questions as to the (extent of the) obligations that the PSBs shall comply with, with a view to making more data available for re-use. In order to make the provisions workable, the text should be made more clear.

Chapter II of the DGA proposal is expected to constitute a continuation and a complement to the Open Data Directive. However, there is a serious risk of overlap and therefore of inconsistencies between the two legal frameworks, which appears to arise from the - artificial - distinction made between data and document in the scope of application of the Open Data Directive and these which would be outside, where the latter could therefore be regulated under the DGA. It is recommended to choose another trigger for the application of the DGA.

In order to foster the re-use of data, PSBs are requested by the DGA proposal to adopt a granular approach towards data re-use(rs), for instance by looking into - but also supervising - the *purpose* for re-use. Such an approach departs from the 'open data' obligations in the PSI and then Open Data

[112] GATS, Art. XIV.
[113] GATS, Art. XIV(a).
[114] GATS, Art. XIV(c).
[115] GATS, Chapeau to Art. XIV.
[116] Svetlana Yakovleva, Privacy protection(ism) : the latest wave of trade constraints on regulatory autonomy, University of Miami Law Review, 2020(416), 416-519.
[117] Ibidem.

Directive. While it could indeed fulfil its objective to increase the amount of data made available for re-use, such an approach raises questions as to the responsibilities and liability exposure of PSBs, something which seems to have been overlooked in the DGA proposal. This is particularly the case concerning the processing of personal data, where the interplay with the GDPR should be clarified.

Following earlier trends visible in the PSI and then Open Data Directive, the DGA proposal aims to turn PSBs into increasingly active data intermediaries, to the point that the DGA could result in the creation of what was called here 'data utilities'. The possible emergence of data utilities (or at least the idea to have such data utilities) can be observed on behalf of policy-makers at the EU and national level beyond the DGA proposal. This can be related to the 'digital sovereignty' political motto. As a new data governance mechanism, the emergence of 'data utilities' should be scrutinised more closely, to assess its potential for fair political governance of the data economy.

The EC finally proposes to regulate strictly the conditions under which non-personal data (protected by third parties' rights) may be transferred to third countries to the extent that compliance with EU's international trade commitments may be questioned. This issue should be thoroughly discussed and clarified before any final adoption of the text. It is also worth recalling here that the debatable distinction made between 'personal' v 'non-personal' data is likely to seriously impair the implementation of the text by PSBs and data re-users.

4 Data sharing services

A major area of regulation under the DGA proposal is the introduction of "data sharing services" ('DSS') in Chapter III. The DGA proposal regulates "data sharing services" under a mandatory compliance regime, applicable to all organisations engaging in a set of specific activities.[118] The rationale for this rather heavy-handed regulation is explained as the need to increase trust in data sharing and lower transaction costs by creating a notification regime for the providers of DSS. In this perspective, specialised data intermediaries, independent from the so-called "Big Tech" platforms, are believed to facilitate the emergence of new data-driven ecosystems. Given the cross-border nature of data sharing, a highly harmonised legislative environment establishing a European model of data sharing with trusted data intermediaries is regarded as imperative. The purpose of the instrument is "*to ensure that data sharing services function openly and collaboratively while empowering natural and legal persons by giving them a better overview of and control over 'their' data*".[119]

DSS providers are expected to bring transaction costs down by combining data sources and matching users and suppliers.[120] So far, DSS are scarce and limited in market value. The regulation proposed by the EC seems to be strongly inspired by the experience gathered—and by the problems encountered—with the major online platforms and marketplaces. As for now, there is however no empirical evidence that the same phenomena would occur in data trading platforms as noted by Fries.[121] It remains to be

[118] DGA proposal, Art. 9.

[119] DGA proposal, p.7, Detailed explanation of the specific provisions of the proposal, Chapter III.

[120] Heiko Richter and Peter R. Slowinski, The Data Sharing Economy: On the Emergence of New Intermediaries, International Review of Intellectual Property and Competition law, 2019(50), 4-29, p. 10.

[121] Martin Fries, Data as counter-performance in B2B contracts, In *Data as Counter-Performance - Contract Law 2.0? - Münster Colloquia on EU Law and the Digital Economy*, Sebastian Lohsse, Reiner Schulze and Dirk Staudenmayer (eds.), Nomos, 2020 ; Alina Wernick, Christopher Olk and Max Van Grafenstein, Defining data intermediaries - A clearer view through the lens of Intellectual Property Governance, TechReg (special issue: Governing data as a resource), 2020, 65-77.

further analysed whether the regulatory framework laid out by the proposed text will solve the identified problems.

The first sub-section discusses the scope *rationae personae* of the legal regime, namely the types of data sharing service providers subject to the authorisation regime of the DGA proposal: data intermediaries on the one hand, and data cooperatives on the other hand. The second sub-section then analyses some of the obligations and conditions laid down by the DGA proposal for DSS.

4.1 Data sharing service providers

Based on the definition provided in Art. 2, Art. 9 DGA proposal prescribes categories of activities that qualify as DSS and thus become subject to the compliance regime provided under the DGA proposal. These categories, namely "data intermediaries" and "data cooperatives", are examined below.

4.1.1 Data intermediaries

Art. 9 DGA proposal identifies two groups of data intermediaries. The first group are the services between legal persons and potential data users that may include bilateral or multilateral exchanges of data, or the creation of platforms or databases enabling the exchange or joint exploitation of data, as well as the establishment of specific infrastructure for the interconnection of data holders and data users.[122] The other group are services between data subjects—who seek to make their personal data available—and potential data users.[123] The DGA proposal does not give a precise definition of these services with specified criteria, but rather provides examples.[124] It adopts a comprehensive approach to regulate the activities of a broad range of service providers in the data ecosystem.

Rec. 22 of the DGA proposal intends to provide some guidance to identify what services or activities qualify as DSS. It is stated that the DGA proposal should only cover services that have as a "main objective the establishment of a business, a legal and potentially technical relation"[125] between data holders (including data subjects on the one hand, and potential users on the other) and that aim to mediate data transactions. As the recital provides, these services should be aiming to intermediate between an indefinite number of data holders and data users. Those who collect data from external sources to offer services—without establishing a direct relationship between data holders and data users, *e.g.*, advertisement or data brokers, data consultancies—are excluded.[126]

It could be argued that, rather than explaining or elaborating on the actual provisions, Rec. 22 aggravates the existing uncertainty by introducing new conditions and exceptions. For instance, it is not possible to infer from Art. 9 that DSS are limited to services aiming at "*intermediating between an indefinite number of data holders and data users*". Nothing in Art. 9 points to that direction of

[122] DGA proposal, Art. 9(1)(a).
[123] DGA proposal, Art. 9(1)(b).
[124] The DGA proposal has been criticised for failing to specify the modalities under which DSS providers shall provide assistance to individuals in exercising their rights under the GDPR, see the 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), para. 121.
[125] DGA proposal, Rec. 22.
[126] Recitals speak of further exempted entities such as services that focus on the intermediation of content, in particular on copyright-protected content; platforms developed in the context of objects and devices connected to the Internet-of-Things; consolidated tape providers.

interpretation. A coherent approach would be to include elements defining DSS in the articles and use recitals to concretise and contextualise abstract norms.[127]

Data intermediaries: EUHubs4Data[128] as a use case

To explore how the regulation of data intermediaries under the DGA proposal may concretely apply to the data sharing ecosystem, the EU-founded research project EUHubs4Data can be used as an example.

Digital Innovation Hubs ('DIHs') are support facilities that help companies becoming more competitive by improving their business and production processes as well as products and services by providing easy access to the latest digital innovations.[129] However, under the current landscape the DIHs' capabilities are not fully exploited as a DIH's influence area is constrained to a regional level and a DIH's catalogue of services is limited to its areas of expertise and technical domain. This contributes to the unevenness of the level of digitalisation in Europe. To fully exploit the benefits that DIHs may bring to the industry, the establishment of a framework for continuous collaboration and networking is thus needed.

Against this background, theEUHubs4Data project aims at fostering cross-border and cross-sector data sharing by creating a European Federation of DIHs that will build and manage an online catalogue of datasets and data-driven services offered by its members. In practice, potential users will be able to perform a search on the online catalogue. After selecting a dataset or a data-driven service, they will be re-directed to the ordering system of the DIH offering such dataset or service to conclude the transaction. The online catalogue will thus function as a platform connecting potential users, *i.e*. legal entities or natural persons who wish to access datasets or data-driven services for commercial or scientific purposes, with holders of these datasets and data-driven services. To a certain extent, this online catalogue/platform would constitute a means to enable data exchange and could thus be regarded as a DSS under the DGA proposal that covers "*making available the technical or other means to enable*" intermediation services.[130] It would follow that the Federation, which would manage the online catalogue/platform, could be considered as a DSS provider.

In addition, it is expected that the DIHs could allow their local potential users to access datasets and data-driven services held by other member DIHs of the Federation, providing for technical means to enable the data exchange. To ensure a secure data exchange, it is foreseen that the Industrial Data Space ('IDS')[131], a Reference Architecture model consisting in a distributed network of connectors (communication server for sending and receiving data), will be implemented. Thus, IDS connectors deployed by DIHs would enable the sharing of data, executing the data exchange process following the

[127] Regarding exempted services, Art. 14 further states that "not-for-profit entities whose activities consist only in seeking to collect data for objectives of general interest, made available by natural or legal persons on the basis of data altruism" shall be exempted (see also Rec. 22).

[128] For further information, please see here: https://euhubs4data.eu/.

[129] For further information, see European Commission, Joint Research Centre, Kalpaka, A., Sörvik, J. and Tasigiorgou, Policy Report on Digital Innovation Hubs as policy instruments to boost digitalisation of SMEs, A practical handbook & good practices for regional/national policy makers and DIH managers, 2020, available at : file:///C:/Users/u0140804/Downloads/final-onlineversion-dih-(handbook).pdf.

[130] DGA proposal, Art. 9(1)(a).

[131] Fraunhofer, in cooperation with the International Data Space Association, Reference architecture model for the industrial data space, 2017, available at: https://www.fit.fraunhofer.de/content/dam/fit/en/documents/Industrial-Data-Space_Reference-Architecture-Model-2017.pdf.

model of a distributed sharing platform. In this case, the local DIH could be considered as a DSS provider as it would act as a technical enabler.

As a result, both the future Federation and the DIHs may be subject to the conditions for providing DSS as examined in Section 4.2 below.

4.1.2 Data cooperatives

As a separate category of DSS providers, the DGA proposal introduces the novel concept of "data cooperatives". The 2020 European Data Strategy refers to personal data cooperatives as novel neutral intermediaries in the personal data economy. They are meant to empower individuals to exercise their rights under the GDPR, by providing oversight and transparency over the use of personal data entrusted to them.[132] As understood, the concept refers to entities established to facilitate the collaborative pooling of data by individuals or organisations for their mutual economic, social or cultural benefit.[133] From an economic perspective, data cooperatives aim to rebalance the asymmetric relationship between data subjects and those who use data to develop services and products.

The DGA proposal defines *data cooperatives* services as services supporting data subjects or legal entities as members—namely individuals and/or small businesses such as one-person companies and micro, small and medium-sized enterprises— by providing guidance to strengthen their negotiating position before consenting to data processing.[134] Among the tasks entrusted to data cooperatives are improving the terms and conditions offered to data subjects by data user organisations and solving disputes affecting several data subjects within a group. It is also contemplated that data cooperatives could have an intermediary role in terms of providing know-how on data sharing to small businesses.[135] They are expected to establish mechanisms to exchange views on purposes and conditions of data processing that would best represent the interests of data subjects or legal persons.

The DGA proposal is unclear on what the notion of 'data cooperative' concretely entails in terms of legal form and type of organisation. As the article in the proposed text on data cooperatives refers to "membership", this could suggest that they are envisaged as a non-profit type of organisation such as associations or cooperative societies. Yet, the DGA proposal provides no clear guidance about the legal form and the nature of this newly enacted entity, in contrast for instance with the clear requirement for data altruism organisations to be not-for-profit in order to be registered as such (see Section 5 below). In this respect, there is also no link made to 'European Cooperative Society' as a recognised legal form at the EU level. Cooperatives, as part of the European social model and the Single Market, have received strong recognition and support in various key EU documents. Under the EU acquis, the European Cooperative Society (ECS) aims to reduce existing cross-border obstacles for cooperatives and facilitate operation across European borders. It complements the legislation on European Companies (Societas Europaea or SE) laying out the general framework for a European public limited company.[136] However unlike companies, members of ECSs do not control the organisation according

[132] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, A European strategy for data, COM(2020) 66 final p.10.

[133] See for instance, MiData https://www.midata.coop/en/home/; SalusCoop https://www.saluscoop.org; Holland Health Data Cooperative http://hhdc.nl; The Good Data Cooperative https://www.thegooddata.org.

[134] DGA proposal, Art. 9(1)(c) and Rec. 24.

[135] DGA proposal, Rec. 24.

[136] Council Regulation (EC) N° 1435/2003 of 22 July 2003 on the Statute for a European Cooperative Society (SCE), OJ L 207/1.

to their capital contribution but the management is based on the principle of "one member, one vote".[137]

It could be argued that the objectives and activities defined for data cooperatives in the DGA proposal are to a great extent compatible with the general framework provided for ECS. Though it is not clear from the proposal what is exactly meant by "data cooperative", and it is not possible to tell whether the legislature contemplates an entity directly within the ECS framework or whether the term is used in a rather generic sense.[138]

A further point to note, neither the provisions nor the recitals of the DGA proposal provide any guidance in terms of the collective exercise of the data subjects' rights provided under the GDPR.[139]

4.2 Conditions for providing data sharing services: an emerging regulatory framework

As mentioned above, an entity falls under the status of a DSS provider when it pursues activities satisfying one of the categories provided in Art. 9. Under Art. 10 DSS providers are subject to notification duties, upon which they may start providing DSS that are subject to strict conditions laid down in Art.11.[140]

Concerning Art. 11 in particular, the fact that the DGA proposal does not refer to "obligations" but rather to "conditions for providing data sharing services" means that in terms of sanctions, the DSS provider could be prohibited from providing services in case of a breach. This interpretation can be confirmed by the reading of Art. 13, as the competent authority monitoring compliance with Art. 10 and 11 can request DSS providers, where appropriate, to cease or postpone providing services, should a breach be substantiated. These provisions reinforce the view of a very stringent legal regime for DSS providers.

The following subsections look more closely into some of the specific obligations and conditions that DSS providers are subject to.

4.2.1 The obligation to appoint a legal representative

The DGA proposal requires that providers of data sharing services that are not established in the EU appoint a legal representative in one of the Member States in which the data sharing services are

[137] Nevertheless, the Statute for ECS allows for membership status with limited voting rights.

[138] For the lack of clarity in terms of nature and obligations of data cooperatives, see 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), para.128-130.

[139] Rec. 24 of the DGA Proposal acknowledges that "*the rights under Regulation (EU) 2016/679 can only be exercised by each individual and cannot be conferred or delegated to a data cooperative*". Based on this, EDPB-EDPS Joint Opinion takes the view that any powers to be conferred to data cooperatives to negotiate the terms and conditions of consent to be given by a data subject would either give rise to unclarity or contradict the GDPR. The Joint Opinion asserts that the "terms and conditions" for the processing of personal data were those enshrined in the GDPR and, therefore, they could not be amended or superseded by means of a contract, 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), para. 131.

[140] DSS providers are required to submit a notification to the competent authority referred to in Article 12. More importantly, DSS providers may start activity upon notification, subject to the conditions laid down in Art. 9 to14 and this will empower them to provide data sharing services in all Member States.

offered.[141] It should be considered that this obligation may lead to additional costs for foreign service providers which would have to mandate someone in the EU to carry out this mission. To a certain extent, this could raise the question whether such an obligation may disproportionately affect foreign data processing operators, in particular foreign SMEs.

4.2.2 "Neutrality" of data sharing service providers

In order to "bring trust and more control for data holders and data users in data sharing services", the DGA proposal imposes "*neutrality of data sharing service providers as regards the data exchanged between data holders and data users*".[142] Being "neutral'' has so far been a constitutive element of the limited liability regime provided for information society services that act as "intermediaries" under the e-Commerce Directive.[143] The e-Commerce Directive, as interpreted by the relevant case law of the Court of Justice of the European Union ("CJEU"), suggest that for a service to be "neutral", and consequently escape liability, it needs to be of a mere technical and automatic nature, passive. This translates into the service provider not actively interfering with the information submitted or stored to gain knowledge or control over them.

It seems that the EC has borrowed the e-Commerce Directive "neutrality" concept, but for a different purpose: not addressing the liability of DSS providers, but as mentioned above, to bring trust in data intermediaries and data sharing. It could be argued that the EC was inspired by its experience with "Big Tech" platforms. Indeed, it has long been debated whether these platforms act as "intermediaries" or have a more active role in handling content on their platforms.[144] This time, with the DGA proposal, the EC seems eager to define the status of DSS providers in advance to pre-empt any similar debate.

The breadth of the neutrality requirement and the extent to which the e-Commerce Directive precedent is to be followed is however not entirely clear. On the one hand, it could be argued that a line similar to the e-Commerce Directive suggests that DSS providers should not be involved in the data exchanged at all and retain a passive role. But Rec. 22 suggests that DSS providers should be allowed to make adaptations to the data exchanged, to the extent that this improves the usability of the data by the data user, where the data user desires this, such as to convert it into specific formats, within the conditions laid down in Art. 11(4).

To bring trust and further foster data sharing, the DGA proposal implements the "neutrality" principle by prohibiting cross-usage of data, and by requiring providers to place their DSS in a separate legal entity (structural separation). Additionally, the procedural requirements of fairness, transparency and non-discrimination for access to the service, discussed in the following sub-section, are also aimed at ensuring neutrality of services, from the perspective of data holders and users.

[141] DGA proposal, Art. 10(3).
[142] DGA proposal, Art. 11(1) and Rec. 26.
[143] This covers services that act as "mere conduits", "caching" and "hosting services".
[144] See for example, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of Regions, "Tackling Illegal Content Online: Towards an enhanced responsibility of online platforms", COM(2017) 555 final, section 9 onwards.

Cross-usage of data prohibition

The DGA proposal provides that a DSS provider may not "*use the data for which it provides services for purposes other than to put them at the disposal of data users*".[145] In recent years there have been growing competition law concerns arising from cross-usage of data, namely that data collected on a given market could be used by a company to develop or to increase its market power on another market in an anti-competitive way.[146] Already in 2010, the French Competition Authority emphasized that cross usage of data can, in certain circumstances, have foreclosing effects.[147] Similarly, in its report of 2015, the UK Competition and Markets Authority mentioned the possibility of tied sales, whereby a company owning a valuable dataset ties access to it to the use of its own data analytics services. Although potentially pro-competitive in certain circumstances, such leveraging market power can also reduce competition by giving a favourable position to that company that owned the dataset over its competitors on the market for data analytics.[148]

There is however a difference to be made here. National competition authorities have examined such behaviours by dominant entities or former monopolies with privileged access to data and issued their decisions in the context of competition law investigations under Art. 102 TFEU for abuse of dominance. With the DGA proposal, the EC seemingly wants to pro-actively tackle the potential anti-competitive cross-usage of data, regardless of the (outcome of) competition law analysis. Art. 11(2) DGA proposal, which prohibits the use of the metadata collected from the provision of the data sharing service for other purposes, seems to have a similar *ratio legis*.

The DMA proposal contains a similar proscription on the cross-usage of data, prohibiting gatekeepers from combining personal data from their core platform services with data from other sources (including other services offered by the gatekeeper).[149] However, "gatekeepers" are defined as providers of core platform services that enjoy a significant position of power and act as an important gateway for business users to reach end users.[150] Arguably, DSS providers are not yet in a comparable position with "gatekeepers" and therefore should not be subject to similar restrictions as those in the

[145] DGA Proposal, Art. 11(1).

[146] Autorité de la concurrence and Bundeskartellamt, Competition Law and Data, 10th May, 2016, https://www.bundeskartellamt.de/SharedDocs/Publikation/DE/Berichte/Big%20Data%20Papier.pdf?__blob=publicationFile&v=2, p. 20.

[147] French Competition Authority, Opinion 10-A-13 on the cross-usage of customer databases; available at: https://www.autoritedelaconcurrence.fr/sites/default/files/commitments//10a13.pdf (in French). Similar concerns in relation to data have been raised by the Belgian Competition Authority, in the National Lottery case which used data acquired in running one activity to help launch another product in a competitive market. See: Decision No. BMA-2015-P/K-27-AUD and BMA-2015-P/K-28-AUD, Stanleybet Belgium NV/Stanley International Betting Ltd and Sagevas SA/World Football Association SPRL/Samenwerkende Nevenmaatschappij Belgische PMU SCRL (cases MEDE-P/K-13/0012 and CONC-P/K-13/0013) (September 2015).

[148] Competition and Markets Authority, The Commercial Use of Consumer Data (2015), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/435817/The_commercial_use_of_consumer_data.pdf, p. 90.

[149] DMA proposal, Art. 5(a).

[150] The DMA Proposal defines gatekeepers as "providers of core platform services which have a significant impact on the internal market, operate a core platform service which serves as an important gateway for business users to reach end users and enjoy an entrenched and durable position or it is foreseeable that it will enjoy such a position in the near future" (DMA proposal, Art. 3).

DMA proposal. Whereas DSS providers are yet to be established,[151] "gatekeepers" in the sense of the DMA proposal already enjoy considerable (market) power.

Structural separation requirement

DSS providers are further obliged to be placed in a separate legal entity.[152] The rationale behind the provision seems again to be the risk of cross-data usage. Companies would therefore need to avoid combining similar activities, i.e. offer data-sharing services in addition to their standard services that may also involve some kind of data handling. It could be argued that combining data-sharing and other data handling activities under one legal entity may allow these companies to take advantage of the third-party data they hold as data-sharing providers for the benefit of their own services,[153] or to use that third-party data to adjust their behaviour on a given product market. Such behaviour could be problematic under competition law rules, if certain conditions are met.

However, as far as competition law breaches are concerned, establishing a separate legal entity would not shield the company from potential liability. Conversely, one key criterion is the level of control exercised to that separate legal entity. In that regard, the legal form of the separate legal entity is important (whether for example, it would be a wholly-owned subsidiary or an affiliate). [154] Furthermore, assuming neutrality of DSS providers would be interpreted in line with the e-Commerce Directive (*i.e.* have a neutral, passive role), a structural separation obligation may be rendered redundant, to the extent it only seeks to address the potential competition law harms arising out of cross-usage of data.

Structural separation can be found in competition law, but only as an *ex post* remedy imposed on rare occasions in order to address competition law concerns raised by a competition law authority in an investigation. It can also be found in sector-specific regulation of utilities, *e.g.* transport or energy law, as an *ex ante* obligation or remedy, or in other words as a preventive measure in order to avoid potential harm (to competition). In these cases, however, structural separation is justified by the legal exclusivity (or monopoly) that the incumbent once enjoyed and that may prevent the liberalisation process by granting the incumbent an advantage inherited from history. This is not the case for DSS providers which, as already mentioned, are only emerging and remain on a rather small scale yet.

Structural remedies, including legal, functional or structural separation, are also foreseen by the DMA proposal. However, in that case, such measures may only be imposed as a last resort, "*where there is*

[151] Heiko Richter and Peter R. Slowinski, The Data Sharing Economy: On the Emergence of New Intermediaries, International Review of Intellectual Property and Competition law, 50, 4-29, 2019, p. 15.

[152] DGA proposal, Art. 11(1).

[153] A parallel could be drawn with the example of Amazon that acts both as a marketplace and as a retailer, in competition to independent sellers using its platform. In November 2020, the EC sent a Statement of Objections to Amazon alleging breach of competition law rules on the basis of Amazon systematically relying on non-public business data of independent sellers who sell on its marketplace, to the benefit of its own retail business. A necessary precondition therefore is for the company (that also acts as an intermediary) to be in a competitive relationship with the third-party company, whose data it holds. See the EC press release here: https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2077 (last visited 23rd May 2021).

[154] Andriani Kalintiri, Revisiting Parental Liability in EU Competition Law, European Law Review, 2018, ISSN 0307-5400. Also available at http://eprints.lse.ac.uk/id/eprint/87251.

no equally effective behavioural remedy or where any equally effective behavioural remedy would be more burdensome for the gatekeeper concerned than the structural remedy".[155]

The DGA proposal goes a step further by imposing structural separation as a condition for a DSS provider to be allowed to provide DSS services. It has been argued that, while structural or functional separation can address some alleged anticompetitive activities undertaken by dominant platforms, experience demonstrates that separation requirements are difficult to administer and can harm innovation.[156] If that holds true for dominant platforms, then *a fortiori* it will apply for DSS providers, which are yet to be established.

It must be acknowledged, however, that the EC presents neutrality as a *sine qua non* condition for data holders and data users to trust DSS services. Trust is an essential factor to harness the potential market of data intermediation services. However, one could wonder whether a blanket structural separation obligation will indeed serve the EC's aims, or if, alternatively, it needs to be restricted only to competition law-sensitive situations where a company's activities and the intermediation activities concern the same or complementary markets, as defined under competition law, as in those two situations the risk of potential behaviour coordination and cross-data usage is higher.

4.2.3 Fair, transparent and non-discriminatory procedure for access to the service and continuity of provision of service

In addition, DSS providers shall "ensure that the procedure for access to its service is fair, transparent and non-discriminatory for both data holders and data users, including as regards prices".[157] Aimed at ensuring that DSS providers act as neutral intermediaries, such behavioural conditions can, again, be found as ex post remedies in competition law or as ex ante obligations for utility providers in sector-specific regulation. For instance, in order to ensure a smooth transition of the liberalisation of railway services, namely from legal monopoly to market conditions, railway infrastructure managers are bound by similar obligations vis-à-vis railway undertakings.[158]

Moreover, DSS providers shall also "ensure a reasonable continuity of provision of [their] services".[159] In contrast to the above, continuity of provision of services does not constitute a typical remedy in competition law. Continuity of provision of services implies a(n) ("reasonable", in this case) obligation to provide services. Such a far-reaching obligation can barely—if ever—be found in commercial and economic law. In contrast, it constitutes one of the cornerstones of "public service". In France, the continuity of public services has long been recognised by the Constitutional Court as vested with constitutional value, based on the 'continuity of the State' argument.[160] To put it another way, continuity of service is precisely based in France on the exceptional character of public service activities as opposed to traditional economic ones conducted by profit-driven private entities. The continuity of

[155] DMA proposal, Art.16(2).
[156] Richard J. Gilbert, Separation: A Cure for Abuse of Platform Dominance?, Information Economics and Policy, Volume 54 (March 2021) 100876.
[157] DGA proposal, Art. 11(3).
[158] See Directive 2012/34/EU of 21 November 2012 establishing a single European railway area (recast), OJ L 343/32, especially Chapter II, Section 4.
[159] DGA proposal, Art. 11(6).
[160] Constitutional Court (Conseil Constitutionnel), Decision 79-105 DC, 25th July 1979.

service condition is therefore surprising here, since it applies to service providers that are not recognised as 'public service' providers (or other similar phrasing).

In sum, the bundle of conditions discussed in both sub-sections 4.2.2 and 4.2.3, combined, are particularly stringent. Some of these conditions resemble the farthest-reaching measures that can theoretically be found as ex post remedies in competition law (structural separation being rarely imposed in practice) and that are typical of sector-specific obligations imposed on utilities providers in the liberalisation process (from legal monopoly to competition). The stringency of the conditions is all the more since they come as a cumulative bundle – rather than, i.e., as a toolbox (as can be found in electronic communications law). For its part, the continuity of service condition goes even a step further and seems more akin to typical public service principles.

This raises the question of whether obliging DSS providers to comply with the above obligations, as well as the additional ones under Art. 11 DGA proposal,[161] conflicts with DSS providers' freedom to provide business. Art. 16 of the EU Charter of Fundamental Rights (EU Charter) guarantees economic initiative and activity.[162] As Art. 11 DGA proposal essentially dictates how DSS providers shall structure and organise their business, it could be argued that the protection ensured by Art. 16 EU Charter is engaged in this case.

Public authorities may legitimately subject the freedom to conduct a business to a broad range of interventions that may limit the exercise of economic activity in the public interest. However, under Art. 52(1) EU Charter, any limitation on the exercise of the rights and freedoms recognised by the EU Charter must respect the essence of those rights and freedoms, as well as the principle of proportionality.[163] The ECJ has recognised that putting in place measures that are complicated and costly to implement constituted a disproportionate interference with an operator's freedom to conduct business.[164] But the interference needs to be such, to affect the core content of the freedom to conduct a business so that business activity is prevented from being carried out.[165] Arguably, that threshold could be met here given the cumulative effect of the obligations imposed on DSS providers.

Interestingly, the Impact Assessment does not refer to the impact of Art. 11 on the DSS providers' freedom to conduct business, while the DGA proposal itself recognises that "*the notification framework for data intermediaries would touch on the freedom to conduct a business, as it would place certain restrictions in the form of different requirements as a prerequisite for the functioning of such entities*".[166] The DGA proposal therefore only links Art. 10 relating to the notification framework with the freedom to conduct a business.

---

[161] These include the following: ensuring interoperability of the data; putting in place procedures to prevent fraudulent or abusive practices in relation to access to data from parties seeking access through their services; putting in place adequate technical, legal and organisational measures to prevent transfer or access to non-personal data that is unlawful under EU law; ensuring a high level of security for the storage and transmission of non-personal data; putting procedures in place to ensure compliance with the EU and national rules on competition.

[162] Article 16 provides that "[t]he freedom to conduct a business in accordance with European Union law and national laws and practices is recognised". The freedom to pursue a business is a corollary of the right to property (Article 17 EU Charter) and has also been considered by the ECJ as a general principle of EU law.

[163] Case C-283/11, *Sky Österreich*, Judgment of 22 January 2013, ECLI:EU:C:2013:28, paras. 46-48.

[164] Case C-70/10 , *Scarlet Extended,* Judgment of 24 November 2011, ECLI:EU:C:2011:771, paras. 48 onwards.

[165] Sky Österreich*, supra*, ft 163, para. 49.

[166] DGA proposal, Section 3, page 7.

4.2.4 The *actio revendicatio* on data: a stick of the bundle of property rights?

The DGA proposal indirectly regulates an aspect that had been typically discussed in the field of property law. The EC essentially proposes to create an *actio revendicatio* for data holders and data users entrusting the data sharing service provider with 'their' data.[167] The provider shall indeed "*have sufficient guarantees in place that allow data holders and data users to obtain access to their data in case of insolvency*". Because data are not protected by ownership rights and do not constitute property in most jurisdictions, natural or legal persons entrusting a third party with the storage of 'their' data (*i.e.* in the case of a cloud computing service contract) do not benefit from the right to revendicate them in case of insolvency or bankruptcy, except where specific provision state otherwise.[168]

This provision thereby aims to protect data holders and data users with respect to 'their' data by providing them with one 'stick of the bundle' of property rights, without having to engage in a sensitive "all or nothing" discussion on whether there should be ownership rights in data. Here, however, the *actio revendicatio* seems to be purely contractual, in the sense that it exists only subject to a contractual relationship between a data holder or data user on the one hand, and the DSS provider on the other. This can be praised to constitute a pragmatic solution to a problem already experienced in other related markets (such as cloud computing and the supply of digital content to consumers), to bring trust to emerging data sharing service providers. With this provision, the EC thereby regulates a property-related issue *indirectly* via the regulation of data intermediaries' governance. By doing so, the EC dispenses itself from engaging in a tricky discussion on a full-fledged property regime for data.

4.2.5 Conclusion

As far as Chapter III is concerned, the DGA proposal provides a heavy-handed regime. As such, it raises many questions as to the regulatory role of the state in the economy and the proportionality of the chosen instrument. The choice of a strict regime accompanied with various duties becomes all the more questionable when we take into account that in much more mature ecosystems (such as online platforms), the EU legislator had until now deemed it sufficient to enact transparency and minor accountability measures (e.g., in the Platform-to-Business Regulation,[169] dealing with the relationship between platforms and business users). This being said, the situation is likely to change significantly with the DSA and DMA proposals.

On that basis, it is first imperative that the DGA proposal ensures legal certainty. To that end, in order to determine the true scope of the DSS providers, there is a need for a set of specific criteria that providers will need to meet. At the moment, both the included entities and those exempted are vaguely defined. For example, it is hard to clarify which entities the DGA proposal refers to as '*services established as a business entity aiming to assist data users and data holders and/or data subjects*'. Similarly, it is also not clear whether qualifying as a non-profit organisation is sufficient to be excluded

[167] DGA proposal, Art. 11(6).

[168] For instance, Luxembourg passed a law in order to enable parties entrusting (cloud computing) service providers with 'their' data ("incorporeal, non-fungible movables") to have a right to claim such data in case of insolvency of the service provider, Loi du 9 juillet 2013 portant modification de l'article 567 du Code de commerce [Law of 9 July 2013 Amending Article 567 of the Commercial Code]. On another note, the Supply of Digital Content Directive creates a right for consumers to retrieve from the trader the digital content upon termination of the contract, Art. 16(4), Directive 2019/770 of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services, OJ L 136/1.

[169] Regulation (EU) 2019/1150 of the European Parliament and of the Council of 20 June 2019 on promoting fairness and transparency for business users of online intermediation services, OJ L 186/57.

from the scope of the DSS regime. The broad and unclear definition of 'data' (see Section 2 on definitions) hereby plays an important role as well.

The EU legislator should also ensure that obligations and duties imposed on DSS providers are clearly defined. It should also be considered whether the measures proposed by the Commission conflict with fundamental freedoms protected by the EU Charter, especially the right to conduct business, and whether they pass the proportionality test, i.e. whether they are necessary, suitable and *stricto sensu* proportionate to attain the aim pursued, given the fact that the market for data sharing services is only emerging and not yet at scale. In this respect, the 'continuity of service' obligation is particularly demanding and seems to implicitly consider DSS providers as public service providers.

Finally, as far as specific provisions are concerned, such as the neutrality requirement, the exact scope of the obligation needs to be set out. It should also be considered whether it conflicts with other requirements under the DGA proposal. That could be the case for example with the obligation, under Art. 11(9), to ensure compliance with EU and national competition law. If DSS providers need to scan the data they receive to ensure that they do not facilitate companies sharing competitively sensitive information (such as information on prices, supply volumes, trading terms, etc.) current and future, their neutrality status could be jeopardised.

5 Data altruism

The DGA proposal introduces the notion of "data altruism" in Chapter IV and the *possibility* (rather than the obligation) for organisations to register[170] as a 'data altruism organisation' recognised in the EU—subject to conditions laid down in the DGA proposal. By doing so, the EC aims to ensure that individuals and legal entities trust data altruism organisations in order to increase data altruism 'for the common good'. Data altruism is defined as "*the consent by data subjects to process personal data pertaining to them, or permissions of other data holders to allow the use of their non-personal data without seeking a reward, for purposes of general interest, such as scientific research purposes or improving public services*".[171]

The first sub-section critically discusses the elements contained in the data altruism definition, i.e. what is data altruism consent, specifically what is the interplay with the GDPR rules, the existing unclarities regarding the application of data altruism to personal and non-personal data, and the notion of 'purposes of general interest" in the DGA proposal. The second sub-section focuses on the data altruism organisations and examines the question of bringing trust in them as a new intermediary in the data value chain.

Throughout this section, the White Paper pays particular attention to the case of (health) research, as the majority of existing examples of data altruism tools and the discourse surrounding data altruism per se focus predominantly on scientific research in the area of health. Looking into (health) research is also a means to discuss data altruism more concretely than solely based on an abstract notion.

[170] "*Each Member State shall designate one or more competent authorities responsible for the register of recognised data altruism organisations and for the monitoring of compliance with the requirements*" of Chapter IV (DGA proposal, Art. 20).
[171] DGA proposal, Art. 2(10).

5.1 Elements of definition and scope of application of data altruism

This section presents a detailed discussion about three key crucial elements of the data altruism definition, namely consent, the uncertainties related to the application of the newly proposed mechanism to personal and non-personal data, and, finally, the concept of 'purposes of general interest', yet undefined in the DGA proposal.

5.1.1 Data altruism consent

*"Data altruism means **the consent**…"* (Art. 2(10) DGA proposal)

The DGA proposal and additional communication surrounding it claim that "data altruism" consent is the same consent as the one foreseen under the GDPR.[172] However, this seemingly simple statement gives rise to several questions relating to the alignment between the two legal frameworks and to the risk of bringing – or *extending* – the uncertainty surrounding the different 'GDPR consent types' to the DGA and its data altruism consent.[173] This particularly concerns the GDPR notion of 'broad consent' and the obscurity surrounding what consent should be attached to, whether 'purpose' or 'processing activity'.

While stating that data subjects should consent to "*specific purposes of data processing*", Rec. 36 DGA proposal also seems to allow for a 'broad consent' for research *in the same terms as the GDPR* (Rec. 33), namely "*to data processing* in certain areas of research *of parts of research projects as it is often not possible to fully identify the purpose of personal data processing for scientific research purposes at the time of data collection*" (authors' emphasis). However, the DGA proposal does not give further guidance as to the usability of broad consent, which is currently very restricted by the interpretation of the EDPB, according to which it "*does not disapply the obligations with regard to the requirement of* specific *consent*"[174] (authors' emphasis).

Moreover, the provisions of the DGA bring uncertainty as to the already complicated understanding of the notions 'purpose' and 'processing activity'. Although, according to the GDPR, and as reiterated in Rec. 36 DGA proposal, consent is attached to "*one or more specific* purposes"[175] (authors' emphasis), Art. 22(3) DGA proposal states that data subjects can give consent to and withdraw consent from "*a*

[172] Pursuant to Rec. 38 DGA proposal, the 'data altruism' consent should follow the requirement established in Art. 7 GDPR. See also the Commission Staff Working Document, Impact Assessment Report accompanying the document Proposal for a Regulation of the European Parliament and of the Council on European data governance (Data Governance Act), p. 28: "*In line with the rights conferred by the GDPR, these mechanisms for data altruism would* be based on consent under Article 7 GDPR *and build on the portability right provided by Article 20 GDPR. In line with the GDPR, they should also provide for individuals to withdraw consent for the processing of their data*." (authors' emphasis)

[173] The lack of clarity as regards the notion of 'consent' employed in the DGA proposal was noted by the European Parliament Committee on Industry, Research and Energy (ITRE). In the recently published draft reports with amendments from the ITRE committee, there are many proposals that attempt at making the link with GDPR much clearer than the current DGA proposal. See AMENDMENTS 300 - 499 - Draft report European data governance (Data Governance Act) EN 27-04-2021 ITRE_AM(2021)691468 PE691.468v01-00

[174] Art. 6(1)(a) GDPR establishes that consent must be given in relation to 'one or more specific purposes'. According to the EDPB, the requirement for specific consent 'aims to ensure a degree of user control and transparency for the data subject'. To reply with the element 'specific', data controllers much apply: 1) purpose specification, 2) granularity in consent requests, and 3) clear separation of information related to obtaining consent for data processing activities from information about other matters. EDPB Guidelines 05/2020 on consent under Regulation 2016/679, p. 13-14. Note, however, that these guidelines, first expressed by the Article 29 Working Party, have never been tested before the European Court of Justice.

[175] GDPR, Art. 6(1)(a) and Art. 9(2)(a).

specific data processing operation". Several processing operations can be performed for one specific purpose, and reciprocally, one processing operation can serve multiple purposes. For example, in a clinical trial, one processing operation can be performed to answer a research question and to comply with a legal obligation.[176] In this context, the question is whether Art. 22(3) DGA proposal should be understood as an endorsement of granular consents *within one project*, for which initially data subjects have provided a 'broad consent'.[177] Alternatively, the DGA proposal might be interpreted as providing (also?) data subjects with the opportunity to give and withdraw broad consent for a *series of scientific projects that serve one purpose*.[178] Finally, another possible interpretation of Art. 22(3) DGA proposal would be that it endorses the new "step-based approach" of the CJEU in its recent case law on (joint) controllership. Although still new and with a number of questions open, this approach seems to back a processing activity-(or operation-)based understanding of consent.[179]

The recent report on the assessment of the EU Member States' rules on health data in research in relation to GDPR pointed out that stakeholders indicated high interest in further EU level action to create "*a more level, and* above all more understandable*, playing field for research*".[180] Particularly acute in the health sector, the interpretation issues raised by the GDPR constitute one of the main examples of lack of "understandability". The DGA proposal, unfortunately, does not seem to bring more clarity to these issues, but further exacerbates them. The lack of clarity and the uncertainty that it entails are likely to burden the data altruism organisations in the first place, since they are in charge of collecting and organising consent. This may also have a chilling effect on the willingness of one to be recognised as a data altruism organisation, which runs against the objectives of the DGA.

The DGA proposal does introduce one additional element, not foreseen in the GDPR: the European data altruism consent form. The form is established with the aim to bring *"additional legal certainty to granting and withdrawing of consent, in particular in the context of scientific research and statistical use of data (...)*".[181] Some advantages of having such a consent form may be foreseen. For instance, studies have shown that privacy policies or terms and conditions (i.e. the current standard of consent

[176] EORTC contribution to the EMA Discussion Paper for Medicines Developers, Data Providers, Research-Performing and Research-Supporting Infrastructures entitled "The General Data Protection Regulation: Secondary Use of Data for Medicines and Public Health Purposes Discussion Paper for Medicines Developers, Data Providers, Research-Performing and Research-Supporting Infrastructures", p. 8.

[177] In its Guidelines 05/2020 on consent under Regulation 2016/679, the EDPB states: "*When research purposes cannot be fully specified, a controller must seek other ways to ensure the essence of the consent requirements are served best, for example, to allow data subjects to consent for a research purpose in more general terms and for specific stages of a research project that are already known to take place at the outset.* As the research advances, consent for subsequent steps in the project can be obtained before that next stage begins*. Yet, such a consent should still be in line with the applicable ethical standards for scientific research*." (authors'emphasis). According to some authors, such as Dara Hallinan, Guidelines 05/2020 then appear to endorse rolling granular consents for each stage of a specific project. Dara Hallinan, "Broad consent under the GDPR: an optimistic perspective on a bright future", Life Sci Soc Policy, 2020, 16(1).

[178] On this topic, see in particular EORTC contribution to the EMA Discussion Paper for Medicines Developers, Data Providers, Research-Performing and Research-Supporting Infrastructures entitled "The General Data Protection Regulation: Secondary Use of Data for Medicines and Public Health Purposes Discussion Paper for Medicines Developers, Data Providers, Research-Performing and Research-Supporting Infrastructures", p. 8.

[179] Charlotte Ducuing, Jessica Schroers, The recent case law of the CJEU on (joint) controllership: have we lost the purpose of 'purpose'?, Computerrecht Tijdschrift voor Informatica, Telecommunicatie en Recht, 2020(6), 424 – 429.

[180] European Commission (2021), Assessment of the EU Member States' rules on health data in the light of the GDPR, p. 80-81.

[181] DGA proposal, Rec. 39.

requests) are rarely read and hard to digest.[182] Data subjects often face a cognitive limitation to understand what exactly they consent to.[183] Having a uniform document (the European data altruism consent form) might be hoped to improve the level of readability and understandability of individuals so that they give genuinely informed consent. It is also commendable that the proposal foresees that the informed consent form will be tailored to specific sectors and for different purposes.[184] However, at this stage, it is difficult to see how the form on its own would fulfil the objectives outlined in Rec. 39, *i.e.*, to contribute to "additional *transparency for data subjects that their data will be accessed and used in accordance with their consent and in full compliance with the data protection rules*" (authors' emphasis). The consent form appears to be simply a(n obvious) means to *comply with* already-existing obligations of the GDPR.

5.1.2 Data altruism for personal… and non-personal data?

"Data altruism means the consent (…) to process (…) ***personal data*** *or permission (…) to allow the use of (…)* ***non-personal data*** *(…)" (Art. 2(10) DGA proposal)*

Data altruism relates to both personal and non-personal data. However, the dedicated Chapter IV hardly includes any reference to non-personal data, with the respective provisions leaning heavily into personal data and leaving many questions unanswered with regards to non-personal data.

The definition of data altruism seems to clearly specify that 'consent' is given by data subjects, whereas legal persons can allow the use of non-personal data via 'permissions'.[185] However, Rec. 38 emphasises *only* the importance of consent,[186] to the detriment of "permission", referred to only once in Chapter IV.[187] It might be questioned, then, whether the European data altruism consent form, foreseen in Art. 22, would also be used as a "permission" form for legal persons. Rec. 39 seems to suggest so: *"(…) a European data altruism consent form should be developed. (…) It could also be used to streamline data altruism performed by companies and provide a mechanism allowing such companies to withdraw their permission to use the data*." If not, it appears that the focus of the provisions contained in Chapter IV falls mostly on the re-use of personal data. This view is confirmed by the reading of preparatory documents and public consultations, which discuss mainly – where not *solely* – altruism concerning personal data.[188] This is particularly the case concerning the EC's preparatory work on the European

[182] Aleecia M. McDonald and Lorrie Faith Cranor, The cost of reading privacy policies, A Journal of Law and Policy for the Information Society, 2008, 4(3), 543-568.

[183] Alessandro Acquisti, Idris Adjerid, and Laura Brandimarte, Gone in 15 seconds: the limits of privacy transparency and control, IEEE Secur. Priv., 2013, 11(4), 72–74;, Frederik Zuiderveen Borgesius, Informed consent: we can do better to defend privacy, IEEE Secur. Priv., 2015, 13(2), 103–107.

[184] DGA proposal, Art. 22(2).

[185] This is also the understanding of the European Data Protection Board, see Statement 05/2021 on the Data Governance Act in light of the legislative developments, adopted on 19 May 2021, p. 5

[186] DGA proposal, Rec. 38: *"(…)*Typically *data altruism would rely on consent of data subjects*" (authors' emphasis).

[187] DGA proposal, Art. 19(3).

[188] See for instance the EC consultation on a European Strategy for Data (2020), available at : file:///C:/Users/u0140804/Downloads/DataStrategy_16_06_2021_EN_draft.pdf, and the European Commission, A European Strategy for data. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. COM/2020/66 final, available at: https://ec.europa.eu/info/sites/info/files/communication-european-strategy-data-19feb2020_en.pdf , p. 13. In the public consultation launched by the EC, data altruism is symptomatically introduced as the mechanism "about making it easier for individuals to allow the use of the data they generate for the public good, if they wish to do so, in full compliance with the GDPR and namely on the basis of consent as a legal basis", see PwC, Response to EC consultation on a European

Health Data Space.[189] In that respect, it is important to bear in mind that stakeholders have so far been confronted *only* with the idea of data altruism as related to personal data shared by individuals. The unclear way in which the provisions in Chapter IV in the DGA proposal are drafted does not do much to dispel this idea. Moreover, the current wording of the DGA proposal does not address the question whether and how natural persons who might wish to make non-personal data under their control available for re-use (e.g., in the scope of citizen science activities[190] or agriculture) could achieve this in practice. Theoretically, such sharing should be possible - as long as one accepts a broader meaning of the notion 'data subject' (see section 2) - because the definition of 'data holder' refers to both legal persons and *data subjects*[191] (authors' emphasis). However, the definition of 'data altruism' appears to limit the use of 'permission' solely to legal entities.[192] Should it then be assumed that the only way for individuals to engage in altruistic data sharing for the purpose of, e.g., citizen science projects, would be to set up separate legal entities? If the answer is yes, would this approach not be a barrier to emerging phenomenons, such as biohacking? After all, the main motivation for participating in such activities is the freedom with which one could do it, in contrast to traditional research environments. In view of the foregoing, it is recommended that the notion of data altruistic 'permission' for data re-use is further clarified to cover the full spectrum of relevant situations, namely natural persons controlling non-personal data.

This being said, regulating data altruism concerning non-personal data should be praised for facilitating altruistic initiatives by companies, at least theoretically. While there is indeed no legal regime *specifically* regulating the use of non-personal data and in particular no ownership rights in data (see also Section 4 on *action revendicatio*), save in sector- and data-specific cases,[193] legal persons permitting the use of 'their' non-personal data for purposes of general interest might fear that, upon making data available, they may not be able to make sure that data are indeed processed for such purpose(s) - and such purpose(s) *only*. By requiring data altruism organisations to "ensure that the data is not to be used for other purposes than those of general interest for which it permits the

Strategy for Data (2020), available at https://www.pwc.com/gx/en/about/assets/pwc-response-to-consultation-on-the-eu-data-strategy.pdf, p. 11.

[189] See in particular the study European Commission, DG Health, Food and Safety. "Assessment of the EU Member States' rules on health data in the light of the GDPR (2021), p. 214. As part of the employed mixed-method design, a survey was sent to key stakeholders, in which data altruism was introduced as follows: "Some MS have put in place system to foster data altruism (sometimes referred to also as data donation), through which *patients* can make available data concerning themselves for researchers to use" (emphasis added).

[190] Citizen science is typically defined as "voluntary engagement in science" (see Luca Ceccaroni et al. (2021) Citizen Science, Health, and Environmental Justice. In: Katrin Vohland et al. (eds) The Science of Citizen Science. Springer, Cham.). In recent years, the opportunities for citizen contribution have grown exponentially – from air-quality testing to DNA sequencing (see Andrea Wiggins and John Wilbanks (2019). The rise of citizen science in health and biomedical research. The American Journal of Bioethics, 19(8), pp. 3–14). Also relevant in this context, is the discussion about so called 'biohacking' – an umbrella term for people who conduct biology experiments outside of traditional research environment. The community's interests are divergent: from genetically modifying plants or the human body, to creating cheap drugs, or making fascinating art (see Teodora Lalova, Burning Down the House: Talking (Bio)Hackers, CiTiP blog, 4 August 2020, available at: https://www.law.kuleuven.be/citip/blog/burning-down-the-house-talking-biohackers/).

[191] DGA proposal, Art. 2(5)

[192] DGA proposal, Art. 2(10), see "permissions of other data holders to allow the use of their non-personal data" (authors' emphasis). See also European Data Protection Board, Statement 05/2021 on the Data Governance Act in light of the legislative developments, adopted on 19 May 2021, p. 5.

[193] For instance, pharmaceutical legislation includes data protection / exclusivity (see Directive 2001/83/EC) so that clinical data generated to get marketing authorization may not be used for the purpose of assessing the market authorization applications of subsequent competing companies. Such legal protection is applicable to both personal data and non-personal data.

processing", the DGA proposal[194] should thus allow data holders to trust that 'their' data will not be used beyond their permission.[195] Incidentally, it should be noted that this provision introduces a new notion of "purpose" for the processing of non-personal data, as of yet unseen in EU law save in some sector-specific legislation,[196] although Rec. 36 clarifies that legal persons could give permission for "a range of purposes not defined at the moment of giving the permission", which is obviously much broader than the "specific purpose" within the meaning of the GDPR.

5.1.3 The notion of 'general interest' in the DGA proposal

*"Data altruism (…) for **purposes of general interest**" (Art. 2(10) DGA proposal)*

The DGA proposal provides that data subjects and other data holders can make data available for 'purposes of general interests',[197] and gives the examples of healthcare, combating climate change and improving mobility as notable examples of such purposes.[198] This raises two main questions.

First, as regards the link between the notion of 'general interest' in the DGA proposal and this of 'public interest' in the GDPR. The notion of general interest is reminiscent of the notion of "public interest" in the GDPR, where it is provided as a possible legal basis for the processing of personal data.[199] Are both terms designed to refer to the same notion and, if so, how do they interact? The DGA proposal does not use the exact same terminology as the GDPR. Typically, objectives of 'public interest' within the meaning of the GDPR are to be stated in EU or national law.[200] In the scope of the GDPR, for instance, this implies that choices made in Member States' laws can have a considerable impact on the legal basis.[201] As for the DGA proposal, the choice to use the term "general" (instead of "public") has not been explained in any of the documents that accompany the legislative proposal. Quite on the contrary, the Impact Assessment refers to "*public* interest" when it comes to data altruism (authors' emphasis).[202] It might be that the *general* interest in the context of data altruism concerning personal data coincides with *public* interest within the meaning of the GDPR.[203] Should that be the case, it could potentially lead to misconceptions concerning the legal basis for processing personal data, namely consent (as per the definition of 'data altruism' in the DGA proposal) on the one hand and a legal provision in EU or national law substantiating the "public interest" at stake pursuant to Art. 6(1)(e)

[194] DGA proposal, Art. 19(2).

[195] The interpretation of Art. 19 DGA proposal is however not straightforward. Indeed, it could alternatively be interpreted so that it is (also?) for the data altruism organization to 'permit' the processing of data by users.

[196] In the case of pharmaceutical data, the protection afforded under Directive 2001/83/EC is purpose-specific, in the sense that clinical data are protected for the purpose to get market authorization.

[197] Data altruism organisations must be legal entities constituted to meet objectives of general interests (Art. 16(a) DGA proposal), they must report to competent authorities annually on the way in which the general interest purposes for which data is collected have been promoted during a given financial year (Art.18(2)), they should ensure that the data is not used for other purposes than those of general processing for which they permit the processing (Art. 19(2)), etc.

[198] DGA proposal, Rec. 35.

[199] GDPR, Art. 6(1)(e).

[200] See e.g. Art. 6(3) of the GDPR, pursuant to which the basis for processing in the public interest shall be led down by Union or Member State law to which the controller is subject.

[201] See EDPB Document on response to the request from the European Commission for clarifications on the consistent application of the GDPR , focusing on health research (2021), p. 5.

[202] Commission Staff Working Document, Impact Assessment Report accompanying the DGA proposal, SWD(2020) 295 final, p. 72.

[203] This seems to be the view of the Committee on Industry, Research and Energy ('ITRE') of the European Parliament, as appears from the reading of its draft report on the DGA proposal (Angelika Niebler, PE691.139v03-00), 28.04.2021. The draft report of the ITRE committee suggests to change "general interest" for "public interest" throughout the text in order to "match the language of DGA to the established regime of the GDPR",p. 99.

GDPR on the other. It could mean that basing data altruism (solely) on the consent of data subjects (in the case of personal data) is inappropriate and legally inconsistent. Moreover, as noted by Mészáros and Ho, the GDPR speaks of different levels of public interest which could be put in an attempted order - from the perceived lower ('public interest') to the perceived higher ('substantial public interest', as under Art. 9(2)(g) GDPR concerning sensitive personal data).[204] As a result, it is not clear where, if at all, "general interest", as employed by the DGA proposal, would fall in this order, given that data altruism is expected to apply to sensitive personal data such as health data.

A second issue relates to the need – unforeseen in the DGA proposal - to substantiate the notion of 'general interest' in order to make it workable. On the one hand, the DGA proposal is expected to be adopted as an EU Regulation, so it should in principle be directly applicable, with no further implementation being required by Member States. This would tend to suggest that no further measure is expected to substantiate the "general interest". This interpretation seems to be backed by Rec. 35 which elaborates on what shall be deemed to qualify as "purpose of general interest". On the other hand, the notion is extremely broad and thus practically unworkable without further substantiation. Additionally, both notions of "public interest" and "general interest" are generally agreed to be *political* in essence and thus to require political choices and direction, be it at the EU or Member State level pursuant to their respective competencies.

Then, the question is who should be entitled to further substantiate the purposes of "general interest" within the meaning of the DGA proposal. While necessarily requiring[205] a concrete mechanism by which a legal entity would be recognised as "constituted to meet objectives of general interest" (within the meaning of Art. 16(a) DGA proposal), the DGA proposal is entirely blind as to how to operationalise it. Would it be for the EC to decide, as part of the implementing acts with which it will develop the European data altruism consent form, although it does not appear to fit in the scope? Or, in light of the above paragraph, would it fall rather in the competence of Member States? It could be for 'competent authorities for registration' to be established by Member States pursuant to Art. 20 DGA proposal to decide, or, alternatively, for the respective national public authorities in charge of registering companies and not-for-profit organisations and/or to recognise their general interest (or other related terminology as per national law) value (e.g. for tax purposes). This raises not only practical questions of responsibility allocation, but also questions of principle regarding competences, whether at EU or Member States level. While it could seem legitimate for the Member States to claim competence in that respect, national diverging implementations could result in a high level of fragmentation. It could also result in forum shopping practices, since the registration of an organisation in one Member State would lead *ipso facto* to its recognition as a 'data altruism organisation' throughout the whole EU. This risks impairing the main objective of the data altruism provisions, namely to bring trust so that data subjects and other data holders are inclined to engage in data altruistic behaviour. In any case, and all the more given the *political character* of objectives of general interest, it seems necessary to decide clearly on whether the notion of 'purposes of general interest' should indeed be substantiated (or implemented) and if so by whom and how.

[204] János Mészáros and Chih Hsing Ho, Big data and scientific research: The secondary use of personal data under the research exemption in the GDPR, 59 Hungarian J. Leg. Stud., 2018, 403–419, p. 408.

[205] See Art. 22(2) of the DGA proposal: "*The European data altruism consent form shall use a modular approach allowing customisation for specific sectors and* for different purposes" (authors' emphasis).

5.2 Data altruism organisations

The DGA proposal introduces a new intermediary in the data value chain – the data altruism organisation. First, although this notion is crucial to Chapter IV, it is undefined which raises interpretation issues. The second sub-section discusses to what extent the DGA proposal achieves its main aim with the recognition of data altruism organisations, namely to bring trust along the data value chain.

5.2.1 The lacking definition of data altruism organisations(' activities)

Rec. 38 specifies that "*Data altruism organisations […] should be able to collect relevant data directly from natural and legal persons or to process data collected by others*." However, the proposal defines neither the 'data altruism organisation' nor its activities, *i.e.* what such organisations actually do. Consequently, it is likely that implementation issues will arise, as the DGA proposal sets off to *regulate* such activities. Considering i.e. the requirement for data altruism organisations to place data altruism activities under a legally independent structure, separate from all other activities,[206] it is imperative to know what the precise scope of 'data altruism activities' entails. On the one hand, these activities seem to be limited to the gathering of consents and permissions by data subjects and 'other data holders', respectively. On the other hand, it seems likely that these activities would also include certain forms of data processing, such as the storage of data, which is the logical prerequisite of making data available to users. However, the DGA proposal does not provide a clear specification about these matters in its binding provisions.[207]

5.2.2 Bringing trust along the data value chain

The emergence of an intermediary necessarily calls for a clarification of responsibilities along the data value chain, so that actors (data subjects and other data holders, as well as data users) can trust the data altruism organisation and the overall data altruism system. It is also a matter of legal certainty of the respective obligations of the actors. The DGA proposal does attempt to do so, but some questions remain open.

From the perspective of the data user, negotiations are expected to be facilitated with a data altruism organisation (as a one-stop-shop) rather than with a crowd of data subjects and/or data holders. In this respect, the data altruism organisation could be compared to a clearinghouse, such as in the

[206] DGA proposal, Art. 16(c).

[207] Processing of "relevant" data by the data altruism organisations is mentioned only in Recital 36 DGA proposal, according to which data altruism organisations should *i.a.* process data "within a secure processing environment", defined as "the physical or virtual environment and organisational means to provide the opportunity to re-use data in a manner that allows for the operator of the secure processing environment to determine and supervise all data processing actions, including to display, storage [sic.], download, export of the data and calculation of derivative through computational algorithms". The contents of this recital cannot be found in any binding legal provision of the proposal. It is worth noting, however, that the Council's version of the DGA proposal does provide more specification in legally binding provisions (in particular Art. 19.2 b)) and specifically refers to "storage" of data. See: Council of the European Union, Proposal for a Regulation of the European Parliament and of the Council on European data governance (Data Governance Act) - Presidency compromise text, Brussels, 22 February 2021 (OR. en), Interinstitutional File: 2020/0340(COD). See the new Article 19(2b) *"The entity shall take measures to ensure a high level of security for the storage and processing of data that it has collected based on data altruism."*

context of intellectual property rights as a particular mechanism to conclude license agreements with an intermediary in-between. This however raises the question of whether the data user can trust that the data has indeed been lawfully collected and processed. Should this not be the case (*e.g.*, in case of data collected unlawfully), the data user could fear being in breach of the GDPR. On the other hand, from the perspective of the data subjects (and of the data holders), the question is rather whether they can trust that 'their' data will indeed be processed only under the conditions and for the purposes that they consented upon or gave permission for.

It is against this general background that the *'policing obligation*' of the data altruism organisation shall be understood, namely the obligation to "*ensure that the data is not to be used for other purposes than those of general interest for which it permits the processing*".[208] As explained in the Impact Assessment, data altruism organisations can (shall) play the role of "supervisors and enforcers" of the data altruism scheme, which verify and *police* to some extent [authors' emphasis] the relevant safeguards (consent, revocability, purpose restriction, etc).[209]

This begs the question, however, how such "policing" should take place in concrete terms, similar to the questions raised with respect to the policing role of PSBs (see Section 3). The term "ensure" seems to suggest a high standard obligation of guarantee but the DGA proposal does not clarify what it entails in terms of responsibility and liability exposure for the data altruism organisation. Then the question is whether the mere fact that the data user processes data for purposes other than of general interest suffices for the data altruism organisation to be found in breach of its 'policing obligation'. Further, it remains unclear whether this policing obligation has an influence on the qualification of the data altruism organisation under the GDPR? For instance, would the data altruism organisation be found to qualify as a (joint?) data controller for the data processing activities conducted by the data user, knowing that the data altruism organisation is also the one gathering consent from data subjects?[210]

It is also questionable whether the policing obligation of Art. 19(2) DGA proposal suffices to fulfil the objective of the European Commission to grant data subjects some control on what is done with 'their' data *along the data value chain* and thereby bring them trust. The EDPB and the EDPS, in their Joint Opinion on the DGA proposal, warn that the DGA may end up decreasing the (arguably 'healthy') distrust of citizens towards organisations that want to get access to 'their' personal data. The DGA proposal creates a sort of label for data altruism organisations, but without sufficient substance in terms of obligations and supervision.[211]

---

[208] DGA proposal, Art. 19(2).

[209] Impact Assessment on enhancing the use of data in Europe. Report on Task 1 – Data Governance, SMART 2020/694, p.25.

[210] The EDPS and the EDPB more generally recommend that the DGA defines the roles of each type of actors with respect to data protection law, see 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), p. 11. This being said, the EDPS and the EDPB assume that the data altruism organisation would qualify as a controller within the meaning of the GDPR (see p. 39). However, they do not clarify for which purpose they would qualify as such, whether for their own purposes (namely to conduct data altruism activities) or (additionally?) as joint controller with the data user with respect to his/her purposes for data reuse.

[211] 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), p. 42. See in particular paragraph 177: *"The EDPB and EDPS underline that the fact that there is almost no requirement from a legal, technical and organizational point of view to become a "Data Altruism Organisation recognised in the Union" (or a "data sharing provider") is problematic. For instance, an organisation, entitled pursuant to Article 15(3) of the Proposal to "refer to itself as a 'Data Altruism Organisation recognised in the Union' in its written and spoken communication" ('labelling effect'), will most probably collect personal data leveraging citizens' expectations in particular on full data protection compliance by the same organisation."*

Except for the policing obligation discussed above (and for the transparency measures in Art. 19 which mainly implement GDPR provisions), the DGA proposal does not provide for the safeguards applicable to the data altruism organisations to be *passed on* and made applicable to data users. For instance, while data altruism organisations shall be not-for-profit, this requirement is not applicable to data users. Putting in place a limitation as regards the business structure of data users (such as to be only not-for-profit) could, of course, unnecessarily limit a large proportion of research activities, namely those conducted by commercial companies, and we do not argue for this here. However, the not-for-profit structure of data altruism organisations could then be merely *deceiving* to data subjects who may be induced to expect data users to also be not-for-profit and may not be fully aware of the risks attached to sharing their data with the subsequent chain of actors. One way to address this would be the implementation of specific transparency obligations towards data subjects, in addition to those mandated by the GDPR. For instance, in addition to information on recipients or categories of recipients,[212] data subjects could be informed about the risks, and/or the nature of the business structure of data users (i.e. whether non-for-profit or not) and of their activities. Finally, although Rec. 36 DGA hints that data subjects should stay informed about the use of data they made available, this does not materialise in the relevant Art.19 (safeguard requirements) and has therefore unclear legal value (if at all).

Finally, ethical oversight – which is often used as a safeguard in research - could be another way to establish trust in data subjects/holders and data users.[213] The DGA proposal does list, *inter alia*, "*oversight mechanisms such as ethics councils or boards*" as a safeguard for data subjects engaging in data altruism, although only in a recital, not in the body of the text, and without any concrete specification.[214] It is therefore no more than a paper tiger. First, due to the lack of a concrete specification – and thus legal obligation – within the legally binding provisions of the DGA. Additionally, and should this 'requirement' be vested with legal value (*quod non*), many questions remain as to its concrete implementation. With respect to, *e.g*. health research, the question is whether these ethics councils are supposed to refer to the existing ethics research committees, or whether they should rather consist of in-house ethics boards as part of the data altruism organisations themselves. In case it is the latter, what will be the guarantees for the boards' independence and impartiality. The same question then arises as for the not-for-profit character of data altruism organisations, namely: how would this requirement be passed on or at least have some influence on the data users.

5.3 Conclusion

By critically evaluating the provisions relating to the newly proposed data altruism mechanism, this section made the following main findings.

First, the definition of 'data altruism', as discussed above, is riddled with several key terminological ambiguities, related to, *inter alia*, the notions of 'consent', and 'general interest'. The interplay with the existing data protection rules is not clear-cut. Data altruism focuses on consent, although consent is only one among several possible lawful grounds for processing personal data - which are not ranked in any particular way - under the GDPR. The DGA proposal does not bring clarity in relation to pre-

[212] GDPR, Art. 14(1)(e).

[213] For a detailed discussion on the ethics of data donation and the associated legal and regulatory challenges, see e.g., Jenny Krutzinna, Luciano Floridi (eds.), Ethics of Medical Data Donation. Philosophical Studies Series, vol 137. Springer, Cham. (2019) https://doi.org/10.1007/978-3-030-04363-6_1

[214] DGA proposal, Rec. 36.

existing interpretation issues (*e.g.*, broad consent or the understanding of how consent is to be attached to the notions 'purpose' and 'processing activity'). More clarity is required, beyond merely employing the concept of 'data altruism' consent. In addition, the legal regime governing data altruism is characterised by the objective to make data available for purposes of 'general interest'. However, the proposal has left unclear how 'general interest' must be understood vis-a-vis the multi-layered notion of 'public interest' in the GDPR. Moreover, the DGA proposal does not seem to reckon the inherently political character of this notion. It remains therefore unclear and undiscussed who and how should be in charge of further substantiating it. Finally, although the provisions of the DGA proposal apply to both personal and non-personal data, the rules on data altruism lack clarity and consistency when it comes to non-personal data, which seem to be implicitly overlooked. Hence, data altruism appears to be mainly targeted at the re-use of personal data. This ambiguity must be resolved and clear rules in the context of non-personal data must be established.

Second, the DGA proposal does not define 'data altruism organisation', nor its activities in a sufficient manner. To ensure a workable data altruism mechanism, the notion of 'data altruism activity' should be expressly defined. Additionally, by setting up and regulating data altruism organisations, the DGA proposal creates a new type of intermediary in the data value chain with the aim to bring trust in the data value chain and thereby incentivise data altruistic behaviours. On the one hand, data users need a clear allocation of responsibilities and legal certainty. On the other hand, the complexification of the data value chain comes with risks to undermine the legal protection afforded to individuals concerning the processing of data relating to them (in the case of personal data), which should therefore be acted upon. In order to do so, data altruism organisations are assigned a 'policing' obligation with regards to the data entrusted to them. However, this 'policing' obligation has not been specified in concrete terms and it is questionable whether it suffices to fulfil the EC's objective to grant data subjects control on what is done with 'their' data along the value chain, thus establishing trust. The legislator could get inspiration from empowering mechanisms in place in other contexts to enable individuals to take part in the decision-making process. For example, in the clinical research context, a growing body of evidence shows that patient involvement provides value for all stakeholders.[215] Lessons can therefore be learned from existing initiatives and guidance,[216] and be translated into best practices for the data governance context. Such mechanisms would genuinely go beyond the provisions of the GDPR and could perhaps enable data subjects to have indeed some form of 'data control', namely some control

[215] See e.g. Anton Hoos A, James Anderson J, Marc Boutin M, Lode Dewulf, Jan Geissler, Graeme Johnston, Angelika Joos, Marilyn Metcalf, Jeanne Regnante, Ifeanyi Sargeant, Roslyn F. Schneider, Veronica Todaro, Gervais Tougas, et al. Partnering with patients in the development and lifecycle of medicines—a call for action. Therapeutic Innovation & Regulatory Science,. 2015, 49(6), ;49:929-939;. Paul Wicks, Maria Lowe, Susan Gabriel, Slaven Sikirica, Rahul Sasane, Stephen Arcona Wicks P, Lowe M, Gabriel S, Sikirica S, Sasane R, Arcona S. Increasing patient participation in drug development. Nat Biotechnol. 2015;33:134-135. Parsons S, Starling B, Mullan-Jensen C, Tham SG, Warner K, Wever K; Needs Assessment Work Package of European Patients' Academy on Therapeutic Innovation (EUPATI) Project. What the public knows and wants to know about medicines research and development: a survey of the general public in six European countries. BMJ Open. 2015;5:e006420. Supple D, Roberts A, Hudson V, et al. From tokenism to meaningful engagement: best practices in patient involvement in an EU project. Research Involvement and Engagement 2015.

[216] See e.g.; Geissler J, Ryll B, Leto di Priolo S, Uhlenhopp M, 'Improving Patient Involvement in Medicines Research and Development: A Practical Roadmap', Therapeutic Innovation & Regulatory Science (2017). Klingmann I, Heckenberg A, Warner K, Haerry D, Hunter A, May M, See W, 'EUPATI and Patients in Medicines Research and Development: Guidance for Patient Involvement in Ethical Review of Clinical Trials', Frontiers in Medicine (2018), 5, available at: https://www.frontiersin.org/articles/10.3389/fmed.2018.00251/full.

on what is done with 'their' data, something that the EC aims to bring to data subjects through, *inter alia,* data altruism,[217] but which remain mere words in the current state of the DGA proposal.

Eventually, one is left to wonder whether the notion and regulation of 'data altruism' in the DGA proposal does indeed have an added-value, namely whether the DGA proposal provisions can achieve their goal to bring trust to the various stakeholders and thereby increase data altruism. In its opinion on the European Strategy for Data, the EDPS does already question by anticipation the added value for data subjects of the notion of 'data altruism', relying on the consent of individuals, compared to the rights and safeguards granted by the GDPR for the processing of personal data.[218] The objective of the EC with the DGA proposal is to increase the trust of individuals in order to stimulate altruistic behaviours, which is generally confirmed by the analysis of the concrete provisions of the DGA proposal. The question of the added-value of the data altruism provisions in the DGA proposal concerns not only data subjects, but also data users. Whether these provisions can genuinely increase the re-use of data 'for the common good' is questionable as a result.

6 European data innovation board and competent authorities

In this section, two particular issues are discussed with regards to the new supervisory authorities that the EC intends to set up under the DGA. Section 6.1 discusses the European Data Innovation Board, in particular with regards to a potential overlap between its competences and those of the EDPB in so far as it also covers personal data processing. Section 6.2 discusses the supervisory competence on data altruism. Where the focus seems to be on enabling data altruism with regards to personal data, competences would not necessarily be attributed to data protection authorities.

6.1 European data innovation board: an addition to the regulatory landscape

Chapter VI of the DGA proposal aims to establish a European Data Innovation Board under the form of an expert group, consisting of representatives of all Member States, the EDPB, relevant data spaces, and other representatives of competent authorities in specific sectors.[219] Its tasks would consist of advising the EC in developing a consistent practice of PSBs and competent authorities under the DGA, as well as advising the EC with regards to the prioritisation of cross-sector standards and the enhancement of the interoperability of data. Finally, the Board would facilitate cooperation between national competent authorities under the DGA through capacity-building and the exchange of information.

In the Impact Assessment, the EC discusses the choice of forming the European Data Innovation Board as either an informal expert group, a formal expert group, or an independent body. The Impact Assessment also states that the EC has explored the option of bringing the required functions under the remit of the EDPB.[220] This possibility has however not been discussed further, given that this would

[217] "This initiative can make the difference for the data economy by creating trust in data sharing and incentivising the development of common European data spaces, where natural and legal persons are in control of the data they generate.", DGA proposal, p. 6.
[218] EPDS Opinion 03/2020 on the European Strategy for Data, p. 14.
[219] DGA proposal, Art. 26.
[220] Commission Staff Working Document, Impact Assessment Report accompanying the DGA proposal, SWD(2020) 295 final, Section 1, p. 29.

imply reforming the decision-making body in the EDPB, which is currently composed of representatives of national data protection authorities. This in turn would imply amending the provisions of the GDPR.[221] If this option were to be taken under consideration, the EC states that additional expertise would then also be required within the EDPB regarding competition law, sector-specific data access and usage regimes, as well as regarding technical knowledge of technical sharing and usage regimes.

It is not a surprise that the EC has (briefly) considered bringing the functions of the European Data Innovation Board under the remits of the EDPB. Data protection is relevant to many data transactions or data sharing mechanisms. In that sense, it should at least be considered whether placing supervisory competence under the auspices of a singular competent body may be to the benefit of all stakeholders involved, not in the least data subjects. Ensuring sufficient oversight and expertise with regards to the processing of personal data, inference of personal data from non-personal data, and anonymisation of personal data is paramount in order to ensure effective data protection. As the EDPS notes in its Opinion on the European Strategy for Data, practice shows that a combination of non-personal data *"may infer or generate personal data, i.e. data relating to an identified or identifiable individual*",[222] thereby introducing an element of risk to the processing of non-personal data. On top of this, it should be considered that it has proven difficult to effectively anonymise personal data,[223] as it is difficult to predict whether a risk of re-identification might exist or come into existence at any time in the future.[224]

While the current proposal aims to unlock access to (personal) data held by PSBs and to facilitate data sharing services as intermediary services between data subjects and data users, it hardly addresses the potentially increased risk to data protection. Instead, just like with the inconsistency it may create between the text of the DGA and the GDPR (see Sections 2, 5, and 8 of the White Paper), it risks creating a multitude of competent bodies where the boundaries of respective competences are obfuscated. The current DGA proposal provides that the European Data Innovation Board would advise and assist the EC in developing a consistent practice of PSBs and competent bodies with regards to processing requests for the re-use of data covered by the rights of third parties[225] and of requirements applicable to data sharing providers.226 As the re-use of data covered by the rights of third parties includes the re-use of personal data, there is a possible overlap with the competence attributed to the EDPB by Art. 70 GDPR, which states the EDPB is to advise the EC on any issue related to the protection of personal data.

Considering that the application of the DGA may result in more personal data (and data which have been anonymised) being processed in the EU, it is unfortunate that its provisions do not create more clarity with regards to the monitoring of the protection of the fundamental rights of European citizens. Instead, the current proposal creates confusion as to the respective competences of different competent authorities. Not only does it fail to expressly confirm the competence of the EDPB with

[221] Most notably Art. 68 68 GDPR, that regulates the composition of the EDPB.

[222] EDPS, Opinion 3/2020 on the European strategy for data, p. 8.

[223] It should further be noted that it is currently somewhat unclear what the threshold for anonymisation under the GDPR entails. While the Article 29 Working Party in its Opinion 05/2014 on Anonymisation Techniques, 2014 (WP126) states that effective anonymisation should be '*irreversible'*, this has been heavily criticized as effectively precluding any form of anonymization (p. 5 and 7).

[224] See for example: Michèle Finck and Frank Pallas, They who must not be identified – distinguishing personal from non-personal data under the GDPR, International Data Privacy Law, 2020, 10(1), 11-36.

[225] DGA proposal, Art. 27(a).

[226] DGA proposal, Art. 27(b).

regards to the processing of personal data (including the anonymisation of personal data), but it also attributes to a separate body, competences that may overlap with those of the EDPB.

Judging by the information the EC provides in the Impact Assessment, it would appear that the idea of attributing the competences of the new European Data Innovation Board to the existing EDPB has effectively been ruled out. While there may be valid reasons why competences under the DGA should reside with a different body than the EDPB, this idea seems to have been dismissed solely on the basis of reasons of practicality. One could argue, however, that there may very well be valid arguments to try to avoid a fragmented and obfuscated supervisory landscape with regards to data and data sharing.

6.2 Data altruism competent authorities

There is a similar issue with regards to the competences of data protection authorities, particularly with regards to data altruism. As discussed in Section 5, the provisions on data altruism seem to be mainly directed at enabling the use of personal data on the basis of a data subject's consent. The current proposal directs the Member States to designate a competent authority to monitor and supervise compliance of data altruism organisations with the conditions laid down in Chapter IV of the DGA proposal.[227] As discussed in Section 5, these conditions include, inter alia, an information duty of the data altruism organisations with regards to the purposes of processing and the limitation of processing to the permitted purposes of general interest. With regards to personal data, these obligations under the DGA proposal seem only to materialise already existing obligations under the GDPR. Even though it does specifically state that the GDPR remains fully applicable with regards to the processing of personal data, the DGA proposal does not attribute competence to monitor compliance with its obligations to data protection authorities. At the same time, nothing in the DGA proposal seems to suggest that Member States could not, at their own discretion, entrust their data protection authorities with the monitoring of data altruism organisations. It seems likely that many Member States would choose to place this task in the hands of data protection authorities, yet nothing in the DGA proposal prevents Member States from taking a different approach. In the particular case of data altruism organisations, the DGA proposal does provide that competent authorities responsible for the register of recognized data altruism organisations are to undertake their tasks in cooperation with the data protection authorities. More specifically, they shall first seek an opinion or decision by the data protection authority for any questions requiring an assessment of compliance with the GDPR.[228] Nonetheless, there remains an element of uncertainty under the current proposal, for instance with regards to the transparency requirements under the DGA and information requirements under the GDPR. Given the predominant focus of data altruism on personal data, it would be advisable to include monitoring and supervision of data altruism under the competence of national data protection authorities and the EDPB.[229]

6.3 Conclusion

There is growing awareness that data protection should not only be considered with regards to data that is clearly personal. On the contrary, increasing amounts of available data make apparently non-

[227] DGA proposal, Art. 20-21.
[228] DGA proposal, Art. 20(3).
[229] Note that this is also the explicit request of the EDPS and EDPB: 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), p. 44.

personal data more likely to allow inference of personal data. Likewise, anonymisation proves to be particularly difficult. Against this backdrop, it is unfortunate that the provisions of the DGA proposal do not provide clarity with regards to the competence of the EDPB, but rather obfuscate the regulatory landscape by introducing separate competent bodies with overlapping competences. While there may be valid reasons for not introducing the new competences under the DGA to the already existing EDPB, the decision seems to be predominantly (if not entirely) based on matters of practicality.

The potential for obfuscation of respective competences of supervisory bodies is best illustrated by the provisions on data altruism. Where the provisions of data altruism seem to primarily be targeted at providing support for sharing personal data out of altruistic motives, the supervision on the organisations that would organise such data sharing should reside with data protection authorities.

7 Final provisions of the DGA proposal

Chapter VIII of the DGA proposal sets out rules on the access to non-personal data by third country law enforcement authorities, as well as on penalties applicable to infringements of the Regulation. First, this section points out the lack of clarity on the scope and nature of the obligations imposed on operators involved in data sharing activities subject to requests issued by third country law enforcement authorities. Second, it questions how EU rules regulating access to non-personal data by foreign law enforcement authorities would interplay with foreign laws with extraterritorial reach, specially designed to get access to sought-after data. Third, this section calls for further guidance on penalties applicable to infringement of the DGA proposal, in order to prevent diverging practices across the Member States.

7.1 International access to non-personal data by third country law enforcement authorities

The DGA proposal sets out rules on transfer or access by third country law enforcement authorities to non-personal data falling under the scope of the DGA.[230] Although these rules aim at protecting the rights and interests of EU businesses, it remains to be seen how such protection would be ensured in practice. Notably considering third country legal acts with extraterritorial reach designed to get access to sought-after data.

As a result of the broad use of electronic communications, investigation, and prosecution of crime relies increasingly on cross-border access to and transfer of data.[231] The mutual legal assistance treaty is the standard legal instrument used by States to cooperate in gathering evidence for criminal investigations and prosecution. However, the system is often rendered inefficient due to its slowness. As a result, governments increasingly try to bypass this system by legally compelling companies that do business in their jurisdiction to provide data no matter where that data is located.[232]

[230] Article 30 of the DGA proposal.

[231] Access to Electronic Data for Criminal Investigations Purposes in the EU, Sergio Carrera and Marco Stefan, No. 2020-01, February 2020.

[232] Access to Electronic Data by Third-Country Law Enforcement Authorities Challenges to EU Rule of Law and Fundamental Rights, Sergio Carrera, Gloria González Fuster, Elspeth Guild, Valsamis Mitsilegas, Centre for European Policy Studies (CEPS), Brussels, 2015; Law Enforcement Access to Data Across Borders: The Evolving Security and Rights Issues, Jennifer Daskal, JOURNAL OF NATIONAL SECURITY LAW & POLICY, Vol. 8:473.

To regulate access to EU non-personal data by foreign enforcement authorities, the DGA proposal lays down strict conditions. The DGA proposal obliges the relevant entity[233] to take "*all reasonable technical, legal and organisational measures*" in order to prevent the transfer of or access to non-personal data held in the Union where such transfer or access would be in conflict with Union or national laws.[234] In particular in the case of data covered by intellectual property rights, trade secrets, and contractual commercial confidentiality.

While those measures may constitute a legitimate requirement to preserve valuable data in the EU, the lack of clarity with regard to the nature of such measures entails risks of legal uncertainty. Indeed, operators in the data sharing ecosystem may need guidance with regard to what would be considered as a 'reasonable' measure and what type of technical, legal, and organisational measures are to be adopted. One may wonder what stands behind technical measures and whether they are limited to security by design measures. The same is true for legal measures expected from private entities. Is it safe to assume that they refer to codes of conduct or self-certification schemes? While we consider that flexibility of the legal framework and a case-by-case assessment are an advantage, we also strongly believe that for the sake of consistency and legal certainty, the current version of the DGA proposal calls for more clarifications on the type of measures mentioned under Art. 30(1).

In addition, the DGA proposal would benefit from further insights of EU lawmakers on the distinction between 'adequate measures' mentioned under Art. 11(7) and 'reasonable measures' under Art. 30(1), if any.[235] This inconsistency of vocabulary may stem from the wording used in the previous version of the DGA proposal made public in October 2020.[236] The homogeneity of the vocabulary throughout the whole text of the DGA proposal would facilitate the interpretation and ease the compliance burden. It should also be considered that it might be challenging for non-EU operators to comply with these obligations as they might be under a conflicting obligation to cooperate with their national law enforcement authorities in accordance with the applicable national law. Although *de jure* these obligations are not discriminatory, as they apply equally to EU and non-EU operators, they might *de facto* affect the latter disproportionally.

The DGA proposal provides for two exceptions allowing transfers of non-personal data upon request of third country law enforcement authorities. First, when the request is based on an international agreement such as a mutual legal assistance treaty. Secondly, when procedural guarantees are in place in the third country that issued the request.[237] In addition, the addressee of the request shall provide 'the minimum amount of data permissible[238] and inform the data holder about the request, except

[233] PSBs, the re-user to which the right to re-use the data was granted under Chapter 2, the provider of data sharing services and the recognized data altruism organisation.

[234] Article 30(1) of the DGA proposal.

[235] Under article 11(7) the DGA proposal requires that providers of data sharing services put in place 'adequate technical, legal and organisational measures' to prevent transfer or access to non-personal data that is unlawful under Union law.

[236] Under the previous version of the DGA proposal made publicly available in October 2020, article 5(7) relating to the conditions for re-use, article 10(i) relating to the requirements for data sharing providers and article 17(d) relating to the requirements for lawful data altruism activities stated that the relevant entity shall have 'adequate safeguards' in place 'including of a technical, organisational and legal nature, that prevent them from responding to requests from authorities of third countries with a view of obtaining access to non-personal data relating to companies established in the Union and Union public administration, unless the request is based on a judicial decision from the Member State in which the company to which the data relate is established.

[237] Article 30(3)(a,b,c) of the DGA proposal.

[238] Article 30(4) of the DGA proposal.

cases where this would undermine the effectiveness of the law enforcement activity.[239] These obligations allegedly aim at securing the interests of EU businesses, preserving their control over 'their' data.

In any event, when subject to a request for transfer or access, the relevant entity shall ask the opinion of the relevant competent bodies[240] or authorities[241] to determine whether the conditions are met to provide access or transfer the relevant data to the law enforcement authority.[242]

It shall be noted that the objective of ensuring a comprehensive protection of EU non-personal data covered by IP rights, trade secrets, or commercial confidentiality, will only be reached if providers of cloud computing services, which are not regulated under the DGA proposal, are subject to the same type of obligations.

Finally, it remains to be seen how the DGA will interplay with the US CLOUD Act that obliges U.S. data and communication companies to provide to U.S. authorities stored data on any server, including abroad, when requested by warrant issued by authorities. Under certain circumstances, such requests might be denied if they violate the legal framework of the foreign country where the data is stored. Back in 2019 the EDPB and EDPS came to the conclusion that the compatibility of the US CLOUD Act with the GDPR raises a problem.[243] The US Cloud Act provides for the possibility for service providers to "intercept or disclose the contents of a wire or electronic communication in response to an order from a foreign government" which is in violation of the EU data protection rules. It remains to see whether the same contradiction will raise with respect to the DGA.

7.2 Penalties applicable to infringements of the DGA proposal

The DGA proposal mandates Member States to adopt the rules on penalties applicable to infringements of this Regulation (Art. 31). The DGA proposal states that the penalties provided for shall be effective, proportionate, and dissuasive (ibid.). However, it is not yet known what the benchmark and the criteria are for guaranteeing the compliance with the principle of proportionality. The EC's proposal would benefit from further insight as to how penalties should be calculated.

It is important to prevent diverging practices across Member States. The DGA proposal obliges Member States to inform the EC of any rules and measures they might undertake (ibid.). Nevertheless, a more structured and institutionalized cooperation is required for ensuring homogeneity across the EU like the EDPB in case of data protection questions. It remains to be seen whether the European Data Innovation Board, foreseen in Art. 26 and discussed in Section 6 above, would become such a forum for developing consistent practices across the EU, including with respect to penalties applied.

[239] Article 30(5) of the DGA proposal.
[240] Concerning the PSBs and the natural or legal person to which the right to re-use the data was granted under Chapter 2 of the DGA proposal.
[241] Concerning the providers of data sharing services and the recognized data altruism organisations.
[242] Article 30(3) of the DGA proposal.
[243] EDPB-EDPS Joint Response to the LIBE Committee on the impact of the US Cloud Act on the European legal framework for personal data protection, Brussels, 10 July 2019.

7.3 Conclusion

Under Chapter VIII of the DGA proposal, clarification is needed, first, on the scope of the obligations imposed on the PSB, the re-user to which the right to re-use the data was granted under Chapter II, the provider of data sharing services and the recognized data altruism organisation in view of international access to non-personal data by third country law enforcement authorities. Second, to ensure harmonized penalties within the EU, the European Data Innovation Board should allow for cooperation between Member States on this issue.

8 General comments on the DGA proposal

The White Paper provided an overview of the DGA proposal, thereby engaging into quite specific lines of argumentation about the novelties put forward by the EC. Drawing on the above sections, this section identifies and critically discusses overall general patterns of the DGA proposal.

8.1 Data as an object of rights – conflicting with the GDPR?

A clear pattern that can be identified in the DGA proposal is that data is considered as an object, that could be 'sold' or 'donated' (even though the term 'data donation' was not retained). Data is even considered as an object *of regulation*, namely as the object of rights, which visibly transpires from the definitions. The definitions of 'data holders' and 'data users' appear to rely on the pre-existence of rights *on* data. Such an approach endorses the commodification of data, namely the process by which data is increasingly viewed as a tradeable commodity. In this respect, the Impact Assessment symptomatically refers on several occasions to the 'data sovereignty' of data providers concerning 'their' data,[244] which seems to endorse that data providers would have a form of exclusive control over such data. The aim of the EC by doing so is to create a 'fair data economy'. Data should be made exchangeable and tradeable, but in a 'fair' manner, *i.a.* by the intermediation of trustworthy intermediaries which would be prevented from tipping into monopolies or by incentivising the use of data 'for the common good'. Such a new approach in EU legislation is worth observing, as it departs quite significantly from previous regulation of 'data'.

However, it also raises a number of questions. As identified in section 2, there are no or barely any such things as 'rights on data', at least when it comes to individual data, namely single datum. Expected to be adopted by the EC in 2021, the Data Act may provide such rights, which should therefore be followed with scrutiny. Also and as discussed on many occasions throughout the White Paper, this approach of the DGA proposal may potentially conflict with the GDPR. The GDPR finds its foundation in the fundamental right to the protection of individuals when data relating to them are processed. Such protection is based on a general prohibition of processing personal data unless a number of requirements are satisfied. In particular, data should be processed (which includes the collection or the coming into existence of the data) only to the extent necessary (data minimization principle) for the achievement of a legitimate and specific purpose (purpose limitation principle). On the other hand, the DGA proposal strives for *more* sharing and re-use of data, including personal data. While the DGA proposal reckons the prevalence of the GDPR in case of contradiction, the White Paper has demonstrated that, in many instances (see for instance concerning Section 2 on definitions, Section 5

[244] Commission Staff Working Document, Impact Assessment Report accompanying the DGA proposal, SWD(2020) 295 final, p. 26, 70 and 73.

on data altruism, and Section 6 on the European Data Innovation Board and other competent authorities), enhanced data sharing goals of the DGA and data processing principles of the GDPR may be hard to reconcile in practice.

8.2 On the regulation of European data spaces

The DGA proposal was conceived to support the establishment of the common European data spaces, that constitute concrete arrangements in which data sharing and/or data pooling can happen beyond one single Member State,[245] in crucial sectors and domains of public interest. The DGA proposal eventually introduces a legal framework that brings safeguards and, in turn, trust in the sharing of data. However, it does not regulate the creation and functioning of the common European data spaces themselves, that are expected to be established or supported under EU funding programmes, such as the Digital Europe Programme and the Connecting Europe Facility 2 (CEF).

Some comments were made to highlight the shift of focus of the DGA proposal from setting explicitly conditions necessary for the functioning of European data spaces to other data related issues. Indeed, the link between the DGA proposal and European data spaces is not apparent. 'Data spaces' are referred to only once in the body of the DGA proposal, concerning the European Data Innovation Board in which they should be represented (see Section 6 above). Against this background, it is possible that a complementary or additional framework will be necessary to tackle the functioning of the common European data spaces. In this respect, the DGA proposal may have missed the opportunity to introduce rules to regulate data spaces as such.

In addition, in its European Data Strategy, the EC clarified that it aims to create a European data space that will enable businesses in the EU to operate on the scale of the Single Market. At the same time, as each sector has its own specificities, cross-sectoral action towards a European data space needs to be accompanied by the development of sectoral data spaces in strategic areas such as agriculture, mobility, and health.[246] It is however not clear how the DGA proposal is positioned in this two-pillars approach. On the one hand, the DGA proposal lays down sector-agnostic provisions with the aim to regulate the governance of data exchange in all sectors, such as with the regulation of data sharing service providers. On the other hand, other provisions appear to relate directly to sectoral data spaces identified in the European Data Strategy, such as the "Common European data space[s] for public administrations" when it comes to Chapter II of the DGA proposal on PSBs or "personal data spaces" when it comes to Chapter IV of the DGA proposal on the regulation of data altruism organisations.

8.3 The DGA proposal as a tool to assert EU's digital sovereignty

The lack of EU data governance mechanisms has constituted a core advantage for the rise of the Chinese and US competitors with regard to the first wave of innovation that was based on personal data collection and use. In particular, the US model relying on the industry self-regulation allowed

[245] Commission Staff Working Document, Impact Assessment Report accompanying the DGA proposal, SWD(2020) 295 final, p. 3.

[246] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, A European Strategy for Data, COM(2020) 66 final, Section 3.

companies like Facebook and Google to grow and further dominate the market by collecting troves of data, notably personal data, across the globe.

The EU must now seize the opportunity of the emerging second wave of innovation based on industrial data, notably data generated by IoT, to set its own standards.[247] As stated by Commissioner Breton, the EU missed the battle for personal data to the US and now it shall not lose the battle for industrial data as a means to boost competitiveness with other global players in the field of data-driven innovation.[248]

Against this background, the DGA proposal is a means to assert the EU's digital sovereignty. The introduction of a data governance framework will allow the EU to exercise control over its data and, in turn, to contain China and the US in their fight for global technological and industrial dominance.

In accordance with its 'open strategic autonomy',[249] the EU's digital strategy to build a strong data economy is twofold. On the one hand, the EU needs openness and international cooperation with regard to data governance. On the other hand, the EU needs to gain control over its data to level the playing field in the data economy.

Against this background, the wording of the DGA proposal follows the spirit of the EU Data Strategy in its attempt to preserve access to EU data for European entities. In particular, a set of restrictions with regard to non-personal data held in the EU are imposed in order to ensure that such data remain in the EU and, thus, benefits the EU's data economy. Indeed, while the explicit data localisation requirements laid out in earlier DGA drafts [250] were removed, the DGA proposal still contains restrictions on transferring 'commercially sensitive' and 'highly sensitive' data to non-EU countries and introduces a requirement of legal representation in the EU for providers of data sharing services and data altruism organisations that are not established in the EU. The DGA proposal would benefit from further insight into how the Commission envisages striking a fair balance between the objective of ensuring preferable operating conditions for EU-based entities and the need to comply with EU's international trade commitments.

The EU is often identified as one of the most important actors in the field of digital regulation. The concept of the "Brussels effect" advanced by Anu Bradford[251] became particularly obvious with the GDPR setting data protection standards for the rest of the globe. The "Brussels effect" primarily consists of the EU's power to promote its rules and practices leading to the Europeanization of legal frameworks of third countries.[252] Time will show whether the EU succeeds in transferring its own data sharing rules and vision of trust worldwide as set out in the 2020 European data strategy. It is, however, without a doubt that the EU seeks to promote its standards and values around the globe by participating in discussions in multilateral fora and cooperating with like-minded partners to decide on

[247] Commission Staff Working Document, Impact Assessment Report accompanying the DGA proposal, SWD(2020) 295 final.
[248] S. Stolton and V.Makszimov, "Von der Leyen opens the doors for an EU data revolution", EURACTIV, 20.02.2020, available at: [https://www.euractiv.com/section/digital/news/von-der-leyen-opens-the-doors-for-an-eu-data-revolution/].
[249] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Europe's moment: Repair and Prepare for the Next Generation, COM(2020) 456 final.
[250] A draft version of the DGA proposal was made public in October; available at : https://mydata.org/wp-content/uploads/sites/5/2020/11/datagovernanceact_oct28_leak.pdf
[251] Anu Bradford, The Brussels Effect, Northwestern University Law Review, Vol. 107, No. 1, 2012, Columbia Law and Economics Working Paper No. 533, available at : https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2770634
[252] Ibid.

future norms regulating the data economy. In the foreseeable future we will also see whether it will preserve its position as a digital regulation leader and trendsetter. DGA will be its important tool in this.