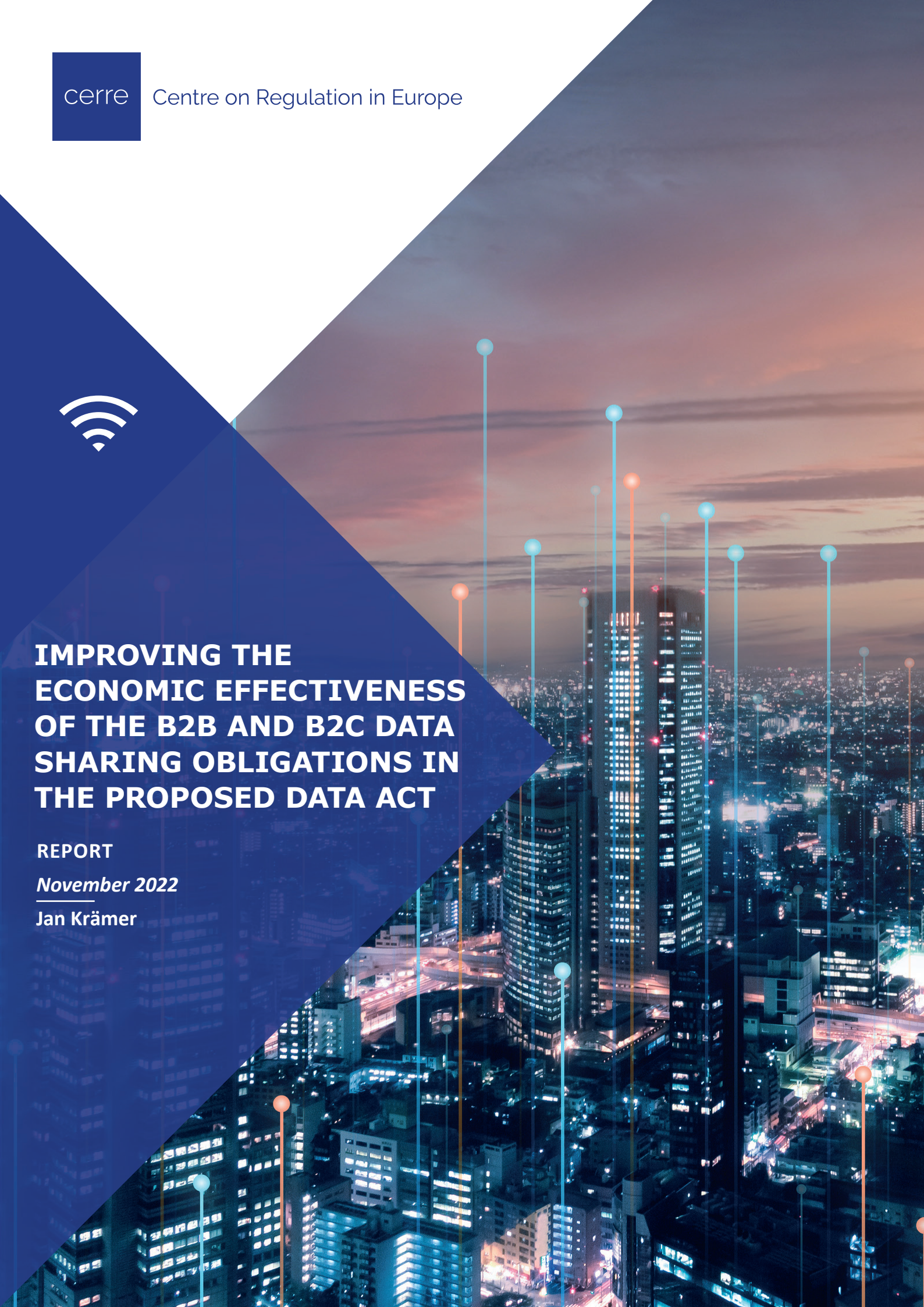
cerre Centre on Regulation in Europe



IMPROVING THE ECONOMIC EFFECTIVENESS OF THE B2B AND B2C DATA SHARING OBLIGATIONS IN THE PROPOSED DATA ACT

REPORT

November 2022

Jan Krämer

As provided for in CERRE's bylaws and procedural rules from its "Transparency & Independence Policy", all CERRE research projects and reports are completed in accordance with the strictest academic independence.

The project, within the framework of which this report has been prepared, received the support and/or input of the following CERRE member organisations: Amazon, Arcep, Comreg, IGN, Huawei, and Vodafone. However, they bear no responsibility for the contents of this report. The views expressed in this CERRE report are attributable only to the authors in a personal capacity and not to any institution with which they are associated. In addition, they do not necessarily correspond either to those of CERRE, or of any sponsor or of members of CERRE.

info@cerre.eu – www.cerre.eu

TABLE OF CONTENTS

ABOUT CERRE

Providing top quality studies and dissemination activities, the Centre on Regulation in Europe (CERRE) promotes robust and consistent regulation in Europe's network and digital industries. CERRE's members are regulatory authorities and operators in those industries as well as universities.

CERRE's added value is based on:

- its original, multidisciplinary and cross-sector approach;
- the widely acknowledged academic credentials and policy experience of its team and associated staff members;
- its scientific independence and impartiality;
- the direct relevance and timeliness of its contributions to the policy and regulatory development process applicable to network industries and the markets for their services.

CERRE's activities include contributions to the development of norms, standards and policy recommendations related to the regulation of service providers, to the specification of market rules and to improvements in the management of infrastructure in a changing political, economic, technological and social environment. CERRE's work also aims at clarifying the respective roles of market operators, governments and regulatory authorities, as well as at strengthening the expertise of the latter, since in many Member States, regulators are part of a relatively recent profession.

ABOUT THE AUTHOR

Jan Krämer is an Academic Co-Director at CERRE and a Professor at the University of Passau, Germany, where he holds the chair of Internet & Telecommunications Business.

Previously, he headed a research group on telecommunications markets at the Karlsruhe Institute of Technology (KIT), where he also obtained a diploma degree in Business and Economics Engineering with a focus on computer science, telematics and operations research, and a Ph.D. in Economics, both with distinction.

He is editor and author of several interdisciplinary books on the regulation of telecommunications markets and has published numerous articles in the premier scholarly journals in Information Systems, Economics, Management and Marketing research on issues such as net neutrality, data and platform economy, and the design of electronic markets.

Professor Krämer has served as academic consultant for leading firms in the telecommunications and Internet industry, as well as for governmental institutions, such as the German Federal Ministry for Economic Affairs and the European Commission.

His current research focuses on the role of data for competition and innovation in online markets and the regulation of online platforms.

1. INTRODUCTION

The proposed Data Act (COM(2022) 68 final), henceforth DA, is a central puzzle piece in the Commission's data strategy and the recent legislative efforts to facilitate more free flow of data (including the Data Governance Act, the Open Data Directive, or the Digital Markets Act). The Data Act contains four main parts. The first part (Chapters II-IV) addresses business to consumer (B2C) and business to business (B2B) data sharing. The second part (Chapter V) is concerned with business to government (B2G) data sharing. The third part (Chapters VI & VIII) contains provisions to facilitate switching and interoperability between cloud service providers and data spaces. The fourth part (Chapter VII) relates to international access and data transfers.

This report deals exclusively with the first part, which is considered to be the 'heart and soul' of the Data Act. Moreover, while previous commentators have predominantly adopted a legal perspective when discussing the DA, we specifically take on an economic and technological viewpoint here, and we will largely leaves out possible legal issues, such as the coherence of the DA within the existing or proposed legal framework in the EU.

As explained above, the DA covers a wide variety of issues. However, as diverse as the different parts of the DA are, so are its goals. The overall goal of the DA is to complement the EU's agenda by promoting "**fairness in the allocation of value from data among actors in the data economy and to foster access to and use of data"**.[1] More specifically, the part on B2B/B2C data sharing seeks to "**facilitate access to and the use of data by consumers and businesses, while preserving incentives to invest in way of generating value through data**".[2] Thus, the DA seeks to **unlock data from connected products**, which are exclusively under the control of the product manufacturer, by **empowering users (commercial and non-commercial)** of such products and product-related services "to control how the data generated by their use of the product or related service is used and enabling innovation by more market players."[3] The underlying premise of the B2B/B2C data sharing obligations under the DA is that data holders of data from connected products (also known as **Internet-of-things (IoT) products**) do not make their data available voluntarily, and thereby hinder innovation and competition. Importantly, the impact assessment report for the DA[4] emphasizes that a main goal of the DA is **to promote competition and innovation in aftermarkets** of connected products.[5] This explicitly includes enabling enhanced digital services by third parties, over and beyond those provided as "related services" by the original manufacturer of the connected product, and enabling **competition in repair services**.[6] The Impact Assessment Report even mentions specific examples where such data access problems occur, and which shall be addressed by the DA. In the B2B context, these are braking systems of a tractor, lifts, and factory machines, for which exemplary problems arise due to lack of

[1] European Commission, 'Proposal for a Regulation of the European Parliament and of the Council on harmonized rules on fair access and use of data (Data Act)' COM(2022) 68 final, Explanatory Memorandum, 2
[2] Data Act proposal, supra note 1, Explanatory Memorandum, 3
[3] Data Act proposal, supra note 1, Explanatory Meomandum, 13
[4] Commission Staff Working Document, Impact Assessment Report accompanying the Proposal for a Regulation on harmonised rules on fair access to and use of data (Data Act) SWD(2022) 34 final
[5] Impact Assessment, supra note 4, 1
[6] Impact Assessment, supra note 4, 10

data access for (predictive) maintenance services and repair services of third parties. In the B2C context, these are smart dishwashers, cleaning robots, fitness trackers, and smart solar panels, for which a lack of data access may prohibit the development of enhanced "digital solutions (e.g., more efficient energy use)", including solutions that combine data from various devices.

In reverse, it is worth highlighting that a main **goal of the DA does not seem to be to promote competition and innovation in primary markets**, that is, those markets where the data was generated. Recital 28 makes it clear that, while the goal of the DA is to "stimulate the development of entirely novel services making use of the data", it avoids "undermining the investment incentives for the type of product from which the data are obtained, for instance, by the use of data to develop a competing product". From an economic point of view this is at least controversial, and it will be later discussed in more detail in this paper.

Finally, the goal of the DA B2B/B2C data access provision is to establish a horizontal regulation that equally applies to all sectors and defines "**basic rules**" on data use.[7] Clearly, in view of the vast scope of products (and related use contexts) that are covered under the DA, spanning over both B2B and B2C environments, this is a formidable task from an economic point of view. The economic power situation can be very different in B2B versus B2C markets, and sometimes it may thus not be the product user, but rather the product manufacturer that would require stronger data rights.[8] Thus, it is important to keep in mind that, due to its horizontal nature, the DA cannot fix all data access problems in the various product markets that it covers. Such markets may differ in the type of data being generated, in the economic power relationships between the manufacturer and the user, the lifetime value and (business) use of the device, and so forth. There is also a risk of the DA being too specific or ill-guided if it would attempt to achieve more than "basic rules". Thus, it should be understood that the **DA will necessarily need to be complemented by sector-specific regulation in many cases**.[9]

The remainder of the report is structured as follows. Against the backdrop of the DA's stated goals, we will next outline the data access and sharing framework laid out by the proposed DA. In doing so, we will already address some inconsistencies and potential issues, but not yet make recommendations on how to rectify them. Then, in Section 3, we evaluate whether the proposed framework is apt to achieve the goals laid out in the introduction. In particular, we comment on the DA's effectiveness and likely economic consequences. Finally, Section 4 concludes with seven concrete recommendations on how to revise the proposed DA in order to alleviate some of the concerns raised, and to increase its effectiveness in practice.

[7] Data Act, supra note 1, Explanatory Memorandum, 5

[8] Indeed, some observers have noted that the DA may in fact strengthen the rights of manufacturers/data holds vis-à-vis its users, rather than the other way around. See Wolfgang Kerber (2022), 'Governance of IoT Data: Why the EU Data Act will not fulfill its objectives', GRUR International, ikac107, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4080436

[9] In similar spirit, see Data Act, supra note 1, Explanatory Memorandum,.5

2. THE ARCHITECTURE OF THE DATA SHARING OBLIGATIONS UNDER THE PROPOSED DATA ACT

The basic architecture of the DA is that of a core right, a **data portability right**, which is then limited and specified in a number of ways. In addition, the DA imposes manufacturers to conclude **a contract with users** in which it has to disclose which data is being collected, for what purpose, and with whom the data is shared. In this section, we first describe the core data portability right, then the initial user contract, and then address the numerous **limiting factors of the portability right**. The goal of this section is not to lay out the legal framework of the B2B/B2C data sharing obligations under the DA in full detail, but to highlight its main pillars, which may enable or inhibit data sharing.

2.1 Right to Real-Time Data Portability for Generated Data

The B2B/B2C data sharing obligations under the proposed DA are, in principle, an **enhanced data portability right** in the spirit of Article 20 GDPR (cf. Recital 31).[10] The core provision is provided by Article 4(1) of the proposed DA:

> Article 4(1): *Where data cannot be directly accessed by the user from the product, the data holder shall make available to the user the data generated by its use of a product or related service without undue delay, free of charge and, where applicable, continuously and in real-time. This shall be done on the basis of a simple request through electronic means where technically feasible.*

The data access right is enhanced vis-à-vis Article 20 GDPR in at least two important ways. First, the data portability right encompasses not only personal data, but also **non-personal data**. Consequently, data access rights in the DA are not limited to a 'data subject' but extend more generally to a 'user', who – according to Article 2(5) – is "a natural or legal person that owns, rents or leases a [connected] product or receives a [related] service". Thus, it explicitly includes business users of connected products.

Second, data generated shall be made available "**continuously and in real-time**", whereas Article 20 GDPR is designed as a one-off data transfer. One-off data transfers have been recognized as having limited effectiveness in the digital economy, where data are generated at a fast pace.[11] Moreover, continuous and real-time data portability necessitates to share data in a more structured format, for instance, via APIs, which should also be conducive to its effective use. Thus, **the DA also enhances portability of personal data**.

[10] Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), [2016] OJ L 119/1, Article 20(1) states that: "The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided [..], and Article 20(2) GDPR complements that "the data subject shall have the right to have the personal data transmitted directly from one controller to another, where technically feasible."

[11] See Jan Krämer, Pierre Senellart, and Alexandre de Streel (2020), 'Making Data Portability more Effective in the Digital Economy', CERRE Policy Report, https://cerre.eu/publications/report-making-data-portability-more-effective-digital-economy/

Similar as under Article 20(2) GDPR, 'users' under the DA also have the **right to authorize a third party** to access their data directly from the data holder:

> *Article 5(1): Upon request by a user, or by a party acting on behalf of a user, the data holder shall make available the data generated by the use of a product or related service to a third party, without undue delay, free of charge to the user, of the same quality as is available to the data holder and, where applicable, continuously and in real-time.*

Article 5(1) is important, because those users who generated the data will frequently not have the resources, capabilities, and economic incentives to re-use that data, and therefore need to be able to relay such data efficiently to third parties. Interestingly, the language of Article 5(1) is not symmetric to that of Article 4(1) as it alludes explicitly to the data access having the "same quality as is available to the data holder", where this is not the case in Article 4(1). One should assume, however, that there is per se no material difference in the scope of data which shall be accessible and the technical access conditions established by Article 4(1) and 5(1). Albeit, as we will point out later, the economic access conditions differ significantly depending on whether data is accessed by the data user or a third party authorized by the data user.

Generally, the core access rights under Article 4(1) and 5(1) of the DA, that is, that users of connected products are entitled to obtain the data that they co-generated through their usage of the product is laudable. It builds on the notion that data that is co-generated by a user and a provider of a service or product, through the use of that service or product, shall be freely available for use to all co-generators, and not just the party that has a de-facto control over the data. Such an **inalienable right** was first established by Article 20 GDPR in the context of personal data and is now logically extended to the context of non-personal data. At the same time, as detailed above, the DA also enhances the possibility of personal data portability over and beyond the status quo under GDPR through continuous, real-time access. In the same spirit, similar provisions for enhanced, real-time, and continuous data portability of 'end users' and 'business users' have also been included for 'gatekeepers' under the Digital Markets Act (DMA) with respect to their core platform services.[12]

2.2 Contractual Agreement Between User and Data Holder

Another key element of the DA is the requirement of a contract between the manufacturer/data holder[13] of the connected product with the user (business or consumer) before purchase, rent, or lease. Indeed, the data holder is not allowed to use any non-personal data generated by the use of the product or related service without such a contract (Article 4(6)). In conjunction with the GDPR in

[12] See Article 6(9) and 6(10) of the Regulation (EU) 2022/1925 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act), [2022] OJ L 265/1

[13] Indeed, the Data Act is often not precise in distinguishing between the manufacturer of a connected product on the one hand and the holder of the data, on the other hand (see, e.g., Axel Metzger and Heike Schweitzer (2022), 'Shaping Markets: A Critical Evaluation of the Draft Data Act', https://ssrn.com/abstract=4222376). At least five different actors of relevance should be distinguished in practical scenarios concerning sharing scenarios under the DA: (i) the manufacturer, (ii) the distributor/seller, (iii) the data holder, (iv) the user and (v) the third party who may obtain data. However, even more actors may exist, e.g., because the buyer of connected product may not be identical to its user. We acknowledge this impreciseness in the text, and that it would require more careful positioining. At the same time, we do not resolve this tension here and presume for the most part that the manufacturer and data holder are the same (or two closely linked and economicaly aligned) entitities.

relation to personal data, this is supposed to bestow control over data use to the user. However, as we lay out below, there is reason to question this empowerment. Henceforth, we shall refer to this as the **initial user contract.**

Additional requirements of the contract between the user and the manufacturer/data holder are laid out in Article 3(2), and include predominantly transparency obligations on (a) "the nature and volume of the data likely to be generated by the use of the product or related services", (b) " whether the data is likely to be generated continuously and in real-time", (c) "how the user may access those data;" (d) who else can access the data and for which purpose, and (e) the identity and contact address of the data holder, including information on how to request data access and how to lodge a complaint.

In general, Article 3(2) is reminiscent of the information that a data controller would need to provide to a data subject before acquiring 'informed consent' for the processing of personal data under the realm of the GDPR. Consequently, one could argue that the Data Act opts for a "**consent -based" architecture** for the processing of non-personal data, in a similar way as the GDPR does for the processing of personal data. As far as the processing of personal data is concerned, the data holder under the DA would of course additionally have to obtain consent or another legal basis for data processing under the GDPR. Thus, in many settings the 'user' under the DA would have to 'consent' to the processing of both personal and non-personal data in a relatively similar way. Albeit legally still two separate 'consents' would be required for personal and non-personal data, practically these could be obtained in one process. **As the distinction between personal and non-personal data becomes increasingly complex in practice, a coherent approach to the use and portability of both types of data may be viewed positively**.

However, whether the consent-based mechanisms of GDPR, and now its logical extension to non-personal data under the DA, truly empowers users of connected products is, at least, questionable. Much has been written about this in the context of personal data, and generally the same criticism applies now to the DA. In particular, the **DA starts from the premise that there is a strong imbalance of bargaining power between the manufacturer/data holder and the user**, whereby the data user is considered the weaker part. This will generally apply in B2C situations and often also in B2B situations. In this case, due to the imbalance of bargaining power, a user cannot truly negotiate the terms of the contract on equal footing with the data holder, and is prone to just accept the contract being offered, giving 'consent' away too easily in expectation of the ability to use the product. While the initial user contract surely contributes to more transparency about the data collection and processing of the connected product – which may be seen as an achievement in its own right – it is **not likely to empower the user** in an economically significant way.

One may argue that such required transparency could strengthen competition between manufacturers of connected products with respect to more user-friendly data collection or data access practices. But this would only be true if there is indeed already strong competition between such products. In this case, and if users are really concerned about their data collection and data access rights, then we would expect that firms would already compete in this dimension (that is, be transparent about data collection and offer consumers favourable access terms) irrespective of the

provisions in the DA. Hence, **transparency alone cannot be expected to significantly change the competitive dynamics beyond the status quo**.

It is important to note, however, that the DA also puts restrictions on the data holder. By Article 4(6), the data holder "shall not use such data generated by the use of the product or related service to derive insights about the economic situation, assets and production methods of or the use by the user that could undermine the commercial position of the user". As Recital 25 explains, this is to protect users in markets where the data holder and the user may engage in additional business negotiations, over and beyond the initial user contract. However, Article 4(6) is not limited to business users and equally applies in B2C relationships. Due to its vagueness and potentially broad scope, this provision also contributes to legal uncertainty and could therefore undermine innovation and investment incentives in IoT products.

Moreover, the initial user contract also does not alleviate other existing legal or economic uncertainties that arise over the life span of the usage of the connected product. Almost by definition – due to their 'connectedness' – the firmware running on IoT products and the software of related services can be and will be frequently updated 'over the air'. Thereby, it is very likely that the data collection and thus also the data access possibilities change over time. By contrast, **the initial user contract seems to assume a static environment**, where the scope of data collection and the processing of the data is fixed and invariant over time, **whereas in reality the scope, scale and purpose of data collection are changing over time**. Further, the DA assumes that product use and acceptance of the initial user contract are inevitably coupled. But what if a user rejects the initial user contract? Can the product still be 'used'? What if a user accepts the initial user contract, but data collection or processing conditions have significantly changed since? Can the product be returned and under which conditions? The DA does not address these obvious questions and may thereby raise rather than lower economic and legal uncertainty. These issues are not per se new, and arise for every product or service that can be altered after purchase. However, these after-sales issues are only central to the DA because of the centrality of the user contract in the architecture of the DA.

Finally, it is also conceivable that it is the user who could have more bargaining power relative to the manufacturer/data holder. This could be the case in some B2B scenarios, for instance, when an original equipment manufacturer (OEM) uses the product of a small or medium enterprise (SME). In this case, the user can negotiate favourable data collection and data access terms also without the help of the DA. Hence, in both scenarios – with economically weak and with economically strong users – **the initial user contract is not likely to change the status quo with respect to competition or user's bargaining power** from an economic point of view.

2.3 Restrictions to the User's Data Portability Right (Free Flow of Data)

While Sections 2.1 and 2.2 have laid out the two primary new rights for users of connected products, particularly a new data portability right, in this section, we outline the numerous restrictions that the DA proposes to limit the extent of the free flow of data when users choose to exercise their new data portability right.

2.3.1 Restrictions on the type of connected products

The DA applies in principle to all physical products that "obtain, generate or collect, by means of their components, data concerning their performance, use or environment and that are able to communicate that data via a publicly available electronic communications service" (Recital 14) and their 'related services', that is, digital services and software that are "incorporated in or interconnected with a product in such a way that its absence would prevent the product from performing one of its functions" (Article 2(3)). This is a potentially very far reaching scope, as more and more products in the future will become part of the '**Internet of Things**' and thus fall under the scope of the DA. However, it is important to note that digital services alone (that is, those that are not invariably tied to a physical product such as electronic communications services) are not in the scope of Chapters II-IV of the regulation.

Moreover, the DA does not distinguish between consumer goods and commercial goods/smart machinery. Recital 14 explicitly mentions that covered products include "vehicles, home equipment and consumer goods, medical and health devices or agricultural and industrial machinery". This is consistent with the specific products mentioned in the DA Impact Assessment Report.

In addition, "**virtual assistants**" are specifically mentioned as falling under the scope of the DA (Article 7(2)), as they provide an "interface to play content, obtain information, or activate physical objects connected to the Internet of Things" (Recital 22). As we will point out below, this is remarkable, as other types of interfaces, fulfilling the same purpose, are not covered by the proposed regulation.

The B2B/B2C data sharing provisions of the DA also excludes specific "connected products". First, by Article 2(2), products whose primary function is the "storing" or "processing" of data are excluded. What is probably meant are servers and more generally IaaS cloud computing services. It is understandable that such **basic computing infrastructure is excluded** from the DA, as they typically only provide the backbone infrastructure to another user-facing "connected product", which then falls under the scope of the regulation.

What is more contentious is that, according to Recital 15, products that are "primarily designed to display or play content, or to record and transmit content", such as "personal computers, servers, tablets and smart phones, cameras, webcams, sound recording systems and text scanners" are outside of the scope of the DA. This is in part surprising, because some of the named products are either clearly connected user-facing tangible products with 'related services' (such as webcams or text scanners), or may also serve as an interface to IoT products in a similar way as virtual assistants (tablets or, smart phones, for instance). The fact that virtual assistants may also come with a screen (as in the case of Amazon Echo Show), or that smart phones also include virtual assistants (such as Siri, Google Assistant, or Alexa) further complicates the distinction. Moreover, generally the lines between personal computers, mobile devices, and other devices belonging to the Internet of Things are becoming increasingly blurred. For example, singleboard computers like a Rasperry Pi, are commonly used in IoT installations, but can also be used as a regular PC. In reverse, 'smart devices' are able to fulfill more and more functionalities and run their own operating systems, like smart watches, smart glasses, or smart refrigerators with screens. In fact, some of the devices which are excluded and some of the devices which are included in the scope of the DA may even run on the same underlying operating

system which allows similar access (or non-access) to the data collected by the device.[14]Consequently, **the line drawn in the DA between "virtual assistants" and other similar type of user-facing connected products seems arbitrary and not future-proof.** Likewise, the line drawn between connected products that supposedly record "content" (according to Recital 15 this includes "webcams") and connected products that record any other physical aspect of the world (such as fitness trackers that record heart rates) is not comprehensible nor practical.

If a distinction is to be drawn, it should not be done on the product level, but rather with respect to the type of data which are collected and can (or cannot) be accessed, which we discuss next.

2.3.2 Restrictions on the scope of data that can be accessed

Only raw data generated by use

Recital 14 states that the access rights in the DA are limited to data that "represent the digitalisation of user actions and events", while "information derived or inferred from this data" is excluded from the scope of the Regulation. Therefore, the scope of data to be accessed is potentially very limited. It is limited to **raw data generated through the use of the product.** In this spirit, it is very similar and thus coherent to the notion of "provided data" (which includes observed data, but not derived data) that is subject to data portability under Article 20 GDPR. Thus again, the DA aligns well with the existing legal framework for access to and portability of personal data.

In this way, the DA also strikes a balance between innovation incentives for the data holder on the one hand, and a user's stipulated right to access co-generated data as well as the unlocking of data on the other hand. Innovation incentives still exist with respect to additional services and derived information, which use the raw data as input, as those services and insights do not have to be shared.

In practice, it is often difficult to delineate the boundary for data generated by the user.For example, a device may already record environmental data (such as weather data) without the user having to "engage" with the product. Recital 17 makes clear that user action is not required for the data to fall under the scope of the regulation, and even data that is collected by the device in "standby mode" is subject to user accessibility. Consequently, **all raw data generated through the use of the product, whether actively provided by the user or not, should fall under the scope of the regulation, and this is also what the proposed data act stipulates**.

Nevertheless, in many scenarios it will remain difficult to exactly delineate the difference between raw data and data derived from the raw data in the context of Internet of Things. In the narrow sense, raw data is collected by sensors or human-computer interfaces (HCI). But usually the raw (sensor, HCI) data is immediately processed in the device to derive a status (for example, a temperature reading derived from the conductivity of a metal). The user may ultimately only be interested in the status of the device (especially in a repair context), but this may not be considered raw data. In reverse, the true raw data (the physical readings from the sensor, for instance) may not even be available to the

[14] For example, harmonyOS, Yocto or Zephyr as well as other Android forks are such IoT operating systems that may run on many IoT devices. See, e.g., https://medium.com/huawei-developers/harmonyos-4bfe31c99be7 or https://thenewstack.io/oniro-distributed-os-unites-a-fragmented-internet-of-things/

manufacturer, as it has been immediately processed. Recital 17 clarifies that "diagnostics data" falls under the scope of the regulation as it was collected as a by-product of the user's action. Data shall be available in the same form and format as generated by the *product*. However, the same recital also stipulates that no software process must be involved. **As the product itself may already be running software (firmware, operating systems, apps) it is not clear where to precisely draw the line between raw data and processed data.**

No trade secrets

In addition to the limitation to raw data, the DA also acknowledges limitations of the scope and extent of the data to be made available under the realm of **trade secrets** in Article 8(6). Generally, the DA stipulates that it does not interfere with the Trade Secrete Directive, nor with IP law (Rectial 28). Nevertheless, some commentators from the legal domain have noted that there may be a potential tension between the goals of the DA (unlocking data) and especially trade secret law, as the latter can potentially be construed as very far-reaching,[15] covering essentially all data, including raw data, that the data holder deems to have a commercial value and is worth protecting.

2.3.3 Restrictions on the type of firms which have to make data available

Generally, as a horizontal regulation, the DA applies to all manufacturers and data holders of connected products. However, **exceptions apply for micro and small-sized enterprises (but not for medium-sized enterprises)** according to Article 7(1).[16] Such an exception based on size is generally laudable, as otherwise small firms are disproportionally affected by the burden to comply with the regulation, which hinders their competitiveness and innovativeness. Such concerns have been raised previously in particular to the application of GDPR, which, by contrast, applies irrespective of the size of the data controller.

2.3.4 Restrictions on the use of accessed data

In addition to the limitations on the scope of data that can be accessed, the DA further limits the use of the accessed data, as it **may not be used to develop a "competing product"** by Articles 4(4) and Article 6(2)(e). This **no-competition clause** is a **stark limitation** from an economic point of view[17], especially since competition is a well known driver of innovation. The provision is an embodiment of the implicit goal that the DA is supposed to strengthen competition and innovation in aftermarkets, but not in primary markets (cf. introduction). The logic behind this restriction is highlighted in Recital 28, which states that the no-competition clause is necessary to preserve the incentives of the manufacturers to develop products that collect data. However, it is important to point out that this restriction on data use is made in addition to the restriction in data scope (cf. 2.3.2), which was also done in an effort to balance innovation incentives between the data holder and the data recipient. Thus, the DA pursues a balancing of innovation incentives (manufacturer/data holder vs. data recipient) in several dimensions, but does not make clear why such cumulative potection of the data

[15] See, e.g., Max Planck Institute for Innovation and Competition (2022), 'Position Statement on the Data Act', para 106 and 284, https://www.ip.mpg.de/en/research/research-news/position-statement-on-the-eu-data-act.html

[16] In Section 4 we recommend to exclude also medium-sized enterprises from having to provide access.

[17] See also Bertin Martens, 'A mutual exhaustion rule on data rights to overcome the paradox of pro- and anti-competitive provisions in the EU Data Act', forthcoming.

holder (limiting the scope of data and prospects of competition) is justified, especially in light of other existing legal protections available to the manufacturer/data holder, such as trade secrets, patents, and copyright protection. In sum, the balancing done in the data act, over and beyond the existing legal innovation protection framework, seems to be tilted strongly in favour of the data holder (seemingly in an effort to protect innovation inventives to develop IoT devices and to collect data), and not in favour of the data recipient (in an effort to unlock data and to stimulate third-party innovation based on device-generate data). Yet, the main goal of the DA is precisely to stimulate data-driven innovation by third parties.

2.3.5 Restrictions on the recepients of accessed data

Further, the DA is very clear on the fact that the **accessed data may not be ported to gatekeepers** designated under the Digital Markets Act (DMA). The DA justifies this by contending an "unrivalled ability of these companies to acquire data" (Recital 36). However, this argument seems a little short sighted and does not properly acknowledge the trade-offs in precluding gatekeepers access to the data made available under the DA. First, especially because of their existing data expertise, gatekeepers under the DMA are likely have both the ability and incentives to use raw data ported to them under the DA for data-driven innovation, and this innovation potential may otherwise not be leveraged. For example, Martens[18] points to the case of in-car operating systems (OS), such as Apple's CarPay and Alphabet's Android Auto, which many car users favour over the OEMs OS. To date, the applications provided through these gatekeeper OS are limited, in part due to limitations in data access. In this case, the DA could improve the data access for gatekeepers, leading to more innovation and benefits for users. Moreover, in many of the product markets covered by the DA gatekeepers are (currently) not in a dominant position, and hence are not in a position to leverage such data otherwise.

However, one may also argue that precisely because gatekeepers are not dominant in many connected products markets (especially in a B2B context), it is even more important to keep such markets open and preclude gatekeepers from access. Yet, if that was the goal, it is questionable whether the DA suffices or is the right place to address this. Gatekeepers are not generally prevented from accessing data, nor from entering IoT markets. They can solicit data holders directly for data, they can also serve as data holders for manufactures, and they can also be manufactures/data holders of own IoT products as well (and often already are, such as for voice assistants, smart home products, fitness trackers, etc). Further, the DMA already contains restrictions on data use and re-combination for core platform services of gatekeepers. The list of core platform services currently already includes virtual assistants (also covered by the DA), and could be extended to other IoT 'related services' in the future in case some of these markets tip and gatekeepers become dominant there. Thus, safeguards to ensure open competition seem better placed as part of the DMA than as part of the DA.

2.3.6 Restrictions for authorised third parties seeking to access data

Finally, restrictions on use are also put in place for any third party that is authorised by a user to access the user's data directly from the data holder.

[18] Martens, ibid.

Purpose authorisation by users

The **third party can only use the data for the specific purposes which have been agreed upon with the user**, who authorized the third party (Article 6(1)). This is reasonable and a required safeguard in order to protect the user, who should remain in control. The third party shall also not "coerce, deceive or manipulate the user in any way" (Article 6(2)(a)) to obtain such data. According to Recital 34, this includes "dark patterns" by which users may be nudged to disclose data to a third party. However, and interestingly, neither Article 6(2) nor the Recitals mention financial rewards in this context, which would be the most obvious means by which a third party could entice a user to disclose data to it. By contrast, Article 5(2)(a) of the DA explicitly forbids gatekeepers to "solicit or commercially incentivise a user in any manner, including by providing monetary or any other compensation, to make data available to one of its services". Thus, the DA is well aware of such financial rewards, but excludes them only when the third party is a gatekeeper. Thus, **it seems that financial rewards paid by the third party (other than a gatekeeper) to a user for obtaining data are generally feasible within the framework of the DA**.

Need to contract with the data holder

Even after being authorised by a user, the third party must still agree with the data holder on a contract concerning the "terms for making the data available" and such terms need to be "fair, reasonable and non-discriminatory" and derived "in a transparent manner" (Article 8(1)). This includes a number of contractual safeguards for the third party, prohibiting contractual agreements that undermine the user rights (Article 8(2)), or are discriminatory (Article 8(3)). Additionally, for third parties that are micro, small, and medium-sized enterprises, Article 13 intended to ensure that the contractual agreement is fair is applicable.

The contractual agreement will usually coverthe technical terms of access, including technical protection measures (cf. Article 11), but also the economic conditions of access, and in particular **a price for access**. Article 9(1) specifically allows the data holder to obtain a 'reasonable' compensation, which can exceed the direct costs of access provision. Only for micro, small, and medium enterprises the compensation must be limited to the direct costs of access (Article 9(2)). It is upon the data holder to demonstrate its costs "in sufficient detail" (Article 9(4)). However, the cost standard that shall be applied is not clear (marginal costs, incremental costs, or total average costs, for instance). From an economic perspective it is evident that a data holder, who is generally opposed to sharing data but forced to do so under the DA, has an incentive to inflate its costs in order to disincentivize the data seeker to actually demand access. Even if the data holder has to prove its costs, it is well known from other regulated access regimes (such as telecoms) that are or were based on a so-called rate-of-return regulation (that is, where the access price is based on the regulated firm's stated costs plus an allowed rate-of-return) that there are accounting techniques and managerial means, among other things, to artificially inflate costs of the regulated segment.[19] For example, a company could redistribute costs from the unregulated to the regulated segment, and thereby even subsidize the unregulated segment. As a consequence, disagreement between the data holder and the access seeker on whether access

[19] For more on rate-of-return regulation and low powered incentive regulation, see, e.g., Jean Jacques Laffont and JeanTirole (2001), 'Competition in Telecommunications', MIT Press.

conditions are 'fair' and 'reasonable' is almost guaranteed. In other industries where an access regime is imposed (for instance, telecoms, or energy), access prices are nowadays typically set by the regulator, based on benchmarking or some other independently derived cost model, and not on costs reported by the access provider. However, the determination of efficient access prices is information intensive, economically very challenging, and requires heavy-handed regulatory oversight.[20] In the context of the DA, which covers a vast amount of products, such regulated access pricing ex-ante is clearly unfeasible. However, dealing with every case in courts ex-post, because access seeker and access provider do not agree on a 'reasonable' compensation, is also clearly unfeasible. There are also legal questions as to what obligations the data holder has to obey to in the meantime, until court cases have been settled, which can well be many years.[21]

Further, it is not evident, **whether and to what extent the data holder can further limit the purpose for which the data can be used by the third party**, over and beyond the purpose limitation that the third party agreed upon with the user.[22] Article 8(2) notes that "A contractual term […] shall not be binding […] if it excludes the application of, derogates from, or varies the effect of the user's rights under Chapter II". One could understand this as a **"user-purpose is king"** clause, whereby the user can authorise the third party to obtain its data for 'any lawful purpose' (Recital 28), and the data holder may not further limit that purpose in its contract with the third party. At the same time, the contractual agreement between the data holder and the third party may fail (due to this or some other grounds). Such possibility of failure is already acknowledged by the DA (see Article 5(7)).

In any case, the need to contract with each data holder, in particular to agree on a price, and the high likeliness of that contractual agreement to end up in either dispute settlement (Article 10) or courts, constitutes a **significant transaction cost, which likely limits access and use of data by third parties authorised by users** .[23]

Direct vs indirect access to user data by third parties

Interestingly, and possibly unintendedly, the DA allows an alternative path by which user data can be shared with third parties. Namely, the user could first obtain the data directly (using Article 4(1)), and then immediately pass it on to the third party. We denote this as an **indirect access**, because the data must flow through the user to the third party. This is to be distinguished from the **direct access scenario** discussed above, where the user authorises a third party (using Article 5(1)), and the data then flows directly from the data holder to the third party, without being sent to the user first. Recital 28 explicitly opens up the possibility for the indirect access scenario, as data can be shared for "any lawful purpose", which "includes providing the data the user has received exercising the right under this Regulation to a third party".

[20] See, e.g. Mark Armstrong, Chris Doyle, and John Vickers (1996), 'The access pricing problem: a synthesis'. The Journal of Industrial Economics 1996, 131, https://www.jstor.org/stable/2950642

[21] For a legal discussion on this see Metzger and Schweitzer, supra note 13.

[22] Irrespective of what the third party agreed on with the user, it is by Article 6(2)(e) that the third party cannot develop a competing product using the data, or share it with another third party for that purpose; but this restriction also applies to users (Article 4(4)). Moreover, the third party may not share the data with gatekeepers under the DMA (Article 6(2)(d)).

[23] For a similar conlcusion see also Moritz Hennemann and Björn Steinrötter (2022), 'Data Act – Fundament des neuen EU-Datenwirtschaftsrechts?', NJW 2022, 1481.

It is important to distinguish between the direct access scenario and the indirect access scenario, because the economics involved are quite different. In the indirect access scenario, there is no need for the third party to conclude a contract with the data holder, and thus no price for data access would have to be paid, unless such a price is agreed between the third party and the user. By Article 4(1) the user can obtain the data in real-time and continuously and **free of charge**. This means, the data holder cannot even levy a direct cost of access from the user.[24] The user could then pass the data on, circumventing most of the obligations and safeguards in Article 6. Article 5(2)(c) implicitly acknowledges the indirect access scenario in the context of gatekeeper access when it notes that gatekeepers shall not "receive data from a user that the user has obtained pursuant to a request under Article 4(1)".

In practice, the indirect access scenario could be facilitated by a third party. That is, the third party could provide tools, such as a Personal Information Management System (PIMS), through which users could easily exercise their access right under Article 4(1), and through which the data could then be easily shared with the third party (using a cloud service to store the data intermittently, for example). Technically, this could probably even be done in a way that mirrors very closely a direct access scenario, such as through providing the user with tools that immediately transfer the data to a cloud storage that is also accessible by the third party. This would not require additional expertise by the user, and would bear similar costs for the access provider (especially because the user also has the right to continuous, real-time access).

While we highlight the possibility of a direct and indirect access scenarios for third parties, the stark economic differences between the two scenarios must be considered as a 'bug' rather than a 'feature' of the DA. **While it may make sense to allow for both access scenarios, the DA should more explicitly acknowledge both, and devise a coherent (economic) regime**. Especially, whatever safeguards to protect users and obligations for third parties receiving data the DA has in stock should apply equally in both settings.

[24] Of course, the manufacturer/data holder may implicitly levy an access price on the user through the price for the connected product.

3. EFFECTIVENESS OF THE DATA ACT WITH RESPECT TO ACHIEVING ITS GOALS

The expressed goals of the DA were highlighted in the introduction. For B2B/B2C in particular, these are: consumer empowerment to obtain data generated by their use of IoT products with the intent (i) to increase **competition and innovation in aftermarkets**, including repair services, and (ii) to stimulate the **development of new products and innovations**. In the following, we discuss, whether the DA's framework, presented in Section 2, is effective in achieving these goals. Furthermore, albeit not an expressed goal, we discuss whether the DA is suitable to truly enable **unlocking of data**. This could be subsumed under the DA's overarching goal to increase "fairness in the allocation of value from data among actors in the data economy and to foster access to and use of data"[25] and it would mean that data can also be traded on **data markets or data brokers**.

3.1 Competition and Innovation in Aftermarkets

Starting from the premise that product manufacturers and their associated data holders do not make any data available to users, the DA does make more data available to users and third parties. In this sense, it is an improvement over the status quo, and can stimulate competition and innovation in aftermarkets. However, the DA probably falls short of its ambitions and there would be a lot more potential under an improved DA framework.

First, the DA only provides access to raw data generated by users, and only if the user authorises access to this data. However, no access is provided to derived data (error codes, or advanced device status, for instance), which arguably may be necessary for many aftermarket applications. In particular, the DA does not allow for interoperability or 'write' access over and beyond 'read' access to the data. If competition in aftermarket repair services is to be stimulated by the DA, which is the expressed goal, this is not sufficient. Even for predictive maintanancemaintenance purposes, that is, services that warn in time about the requirement to repair in order to prevent failure in the future, access to derived data is likely necessary. The DA also does not include a 'right to repair' for the IoT products that it covers. It rests on the hope that the raw data generated by use is sufficient. Importantly, we do not argue here for such a 'right to repair' or interoperability requirements in the DA, and indeed these may be very difficult to place in a horizontal regulation, but note that the existing framework is not sufficient to achieve this.

Second, competition and innovation incentives in aftermarket services are further reduced due to the need to contract and, in particular, to compensate the data holder. This gives rise to vertically integrated market structure, where the provider of an essential input resource (here the data holder providing data to third parties) is at the same time a competitor in the downstream market (here the aftermarket). This is a well known structure from network industries, which gives rise to a number of competitive issues. Foremost, the data holder, who does not want to share data has economic incentives to engage in a margin squeeze, by raising the input price (such as through stating inflated

[25] Data Act, supra note 1, Explanatory Memorandum, 2.

costs of access provision, as discussed in Section 2.3.6). Further, it can engage in non-price discrimination known as 'sabotage', that is, deliberately degrading the quality of access, or the quality of the data. Albeit Article 5(1) demands that such sabotage is not admissible, experience from other regulated industries (telecoms, for example) suggests that it requires heavy-handed regulatory oversight to remedy this. Fixing the access price to zero ex-ante would at least alleviate the margin squeeze concerns. However, a zero access price may increase incentives to sabotage, and it would also – compared to a positive access price – put an additional cost burden on the access provider, which may lower its innovation incentives. Whether a price of zero is justified in this trade-off will thus also crucially depend on the actual costs of providing access.

Third, the no-competition clause may also stifle innovation and competition in aftermarkets. This is because the no-competition clause raises numerous legal and economic uncertainties, for instance, with respect to the definition of product markets and the degree of innovation that would qualify as a new product. Indeed, if the accessed data is actually put to an economically viable use by a third party, such that the third party is successful in the aftermarket, then it would often be in an excellent position to also enter the primary market at a later point in time. However, the no-competition clause disincentivises this entry-and-growth strategy and option.[26] But in doing so, it also disincentivises (at least some potential entrants) to enter and to invest in the aftermarket in the first place. This seems especially problematic if the goal is to invite SMEs to provide aftermarket services.

The no-competition clause is also problematic for a different reason. Suppose the DA achieves its goal to render aftermarkets competitive where before they were monopolized by the data holder and not competitive. Clearly, this reduces the profits of the manufacturer/data holder. However, the prospect of monopoly rents and consumer lock-in in the aftermarkets has previously led the manufacturer to compete more aggressively in the primary market. This is a well known result from the economic literature on switching costs.[27] Hence, increasing competition in the aftermarkets reduces competition in the primary markets, everything else being equal. In a functioning market, this could be counterbalanced by the entry of new competitors in the primary market, especially from those firms that have gained a foothold in the aftermarket already. However, the no-competition clause prevents this to a large degree. In reverse, if it is argued that there is no hope for competition in the primary market anyway (because the primary product is so specialised, for example) then the no-competition clause is also not necessary to protect that monopoly.[28]

3.2 Enabling Innovation and Investment in new Products and Services

While the DA does not intend to unlock data in order to stimulate competition in the primary market from which the data originate (even if we do not share this goal), it is the expressed goal of the DA to

[26] Or, alternatively, it disincentives a third party to acquire access to the data made available under the DA in the first place, which would run counter to the whole idea of the DA.

[27] See, e.g., Paul Klemperer (1996) 'Competition when consumers have switching costs: An overview with applications to industrial organization, macroeconomics, and international trade'. The review of economic studies 62(4), 515-539, https://doi.org/10.2307/2298075

[28] The reverse causality, i.e. that the absence of the no-competition clause would render even specialised (monopoly) product markets competitive, is, of course, not true.

stimulate innovation and investment in entirely new products and services. However, the DA does not lay out a clear (economically convincing) mechanism through which this could be achieved.

The underlying idea is that the raw data generated by a device is sufficiently useful for developing a new product or a new service which is not essential to the IoT product, as otherwise it would have existed already. In case the new service is a service complementary to the IoT product or an aftermarket service, our reasoning in Section 3.1 applies. In case the product or service is not complementary to the IoT device from which the data originate, then this bears the questions of why consumers would equip the new provider with their data. There exists a chicken-and-egg problem. Users see no value in transferring their data to a provider intending to develop a new product or service unless the product or service exists and the value of providing data becomes tangible. But if the presumption is right that the data is needed to develop a product or service in the first place, then the product/service will not be developed. The DA does not resolve this chicken-and-egg problem, because the DA does not have a mechanism to facilitate bulk data access for innovators, that is, enabling the innovator to acquire a large trove of (anonymised) raw data without needing to obtain authorization from many users. For example, the impact assessment mentions mobility data and better mobility services that are based on such data access. Such a service would require access to many mobility profiles, spanning over a representative set of users, whereas the DA only provides for access to those users that have authorised access. Generally, the transaction costs of obtaining the authorisation of many users, without being able to demonstrate an immediate value, will be high for innovators, especially SMEs that do not already have a strong user base. Bulk data access could be achived through functioning data markets and data brokers, if the DA would enable those. However, we are not very optimistic that is the case (see Section 3.3.).

Of course, there may also be other use cases where the data generated by other IoT devices is not necessary for developing a new product or service but yet increases its value if the unlocked data feeds into it. Here, the DA can potentially increase the incentives to innovate in such products, but only if there is a significant overlap in the user base between the existing IoT product from which the data originateoriginates and the new product or service, as users still have to authorize that data flow. This seems to be rather limiting.

The no-competition clause is also problematic in the context of innovation of new products, because competition is a key driver of innovation. Better and more innovative services and products may be developed precisely because the current manufacturer is challenged or can be challenged in its position. Again, it cannot be overstated that only access to raw data is to be provided. Other economic and legal mechanisms to protect innovative efforts, such as copyright and patents, are of course still available to manufacturers.

3.3 Enabling Free Flow of Data through Data Brokers and Data Markets

As laid out in Section 2.3, users could be compensated for making data available to third parties. This seems to open up the possibility for **data brokers** who buy data from users and sell it again on **data markets.** In theory, if authorised by the user to do so, the data broker could use the data for profiling

of natural persons (Article 6(2)(b)) and/or pass it on to third parties (Article 6(2)(c)). The user could even instruct the data holder not to make the data available to any other third party (Article 8(4)).

However, further provisions of the DA make a **data brokerage scenario highly unlikely**. First, the third party **cannot contract with the user on exclusivity** (Article 6(2)(f)). From the data broker's point of view, data is most valuable if it has exclusive access to it. Every time the data is shared with a new third party, the value depreciates and hence lowers the price that the broker would be willing to pay to the user. Eventually, data brokers are not willing to compensate users any more for data access, and in return users will see little value in granting access.

Second, and even more problematic for a data brokerage scenario, is the fact that third parties need to agree with the data holder on a contract on the terms for using the data (Article 8(2), see next paragraph), which may also include a price for access according to Article 9.[29] Although such a price must be 'reasonable', the price charged by the data holder has to be paid in addition to the price paid to users for acquiring the data.

Third, acting as a data broker would require a wide purpose authorisation by the user. This seems possible in principle (Article 6(2)(c)), but it would need to be obtained from a large number of users in order to compile a large enough and representative enough data set. If our interpretation is right, the data holder cannot further limit the purpose authorised by the user; but the third party must ensure that the data is not used to develop a competing product by any other third party that may acquire the data (Article 6(2)(e)). For a data broker, compliance with this provision will be very difficult or costly, especially if data sets are further aggregated with other data sources. Additionally, Article 5(8) empowers the data holder to raise concerns with respect to trade secrets, which may put an additional compliance burden on the data brokers that makes such a business model unattractive.

The preceding discussion has assumed the direct access scenario (cf. Section 2.3.6), where the user authorises a third party to receive the data directly. Some of our concerns, especially those related to the need to contract and to negotiate a price, would not apply in the indirect access scenario. However, in this case, some safeguards for the user in Article 6, especially with respect to profiling (Article 6(2)(b), would not apply, and would need to be negotiated by the user directly with the data broker. This may also raise transaction costs.

Taken together, the DA theoretically does not exclude the possibility of data brokers and data markets to emerge; however, it does not offer economically favourable conditions for this to occur, due to the manifold transaction costs (stemming from the restrictions laid out in Section 2.3) that are introduced by the DA. However, there are good reasons to believe that the DA must enable specialized data brokers to emerge, who can then serve as intermediaries for data aggregation, data processing and access, and particularly bulk data access by third parties, empowering users insofar as they are compensated for the data that they provided.

[29] While micro, small and medium enterprises would only need to pay the direct costs of access, the negotiated compensation for other third parties is likely to well exceed direct access costs.

4. RECOMMENDATIONS

The preceding analysis has led us to the conclusion that the DA is too complicated for a horizontal regulation with such a vast application context, and it falls short of its ambitions. Although the DA provides new data access rights, which can have limited effect on innovation and competition in aftermarkets, it also contains too many restrictions that create new transaction costs and limitations in data use. The DA runs the risk of either being ineffective or creating unintended consequences, many of which have been pointed out here. Lumping B2B and B2C access scenarios into one bucket is also risky in this regard, because the economic bargaining positions, innovation incentives, and data use scenarios may be very different in both contexts.

Our main overarching recommendation is to **simplify the DA by reducing the number of restrictions** (for example, of product categories or, purpose limitations) **and obligations** (in particular with respect to contracting) to a minimum. As a horizontal regulation, the **DA should be more humble with respect to its goals**. Unlocking consumer data for the sake of competition and innovation, while preserving innovation incentives of the data provider is challenging enough. The DA should be more agnostic with respect to the specific types of innovation and services that are intended. In particular, the preceding analysis highlights that it is problematic to shield the primary market from the competitive and innovative process that may emerge from unlocking the data. Moreover, enabling 'repair services' likely requires a different framework and this goal is ill placed in a horizontal regulation centred on the idea of data portability. The focus of the DA should really be to set out **basic rules** for access to and use of co-generated data, and leave more specific provisions to sector-specific regulation.

Building from the existing framework of the DA, we make the following recommendations to achieve a leaner yet more effective framework:

Recommendation 1: Balance innovation incentives between data providers and data seekers through limiting scope of data access to raw data generated by product use

The main trade-off that the DA needs to balance is that between preserving innovation and investment incentives of data providers, on the one hand, and increasing innovation and investment incentives of data recipients, on the other hand. Balancing this trade-off, especially in a horizontal regulation, is generally very difficult. Next to economic considerations also considerations of fairness may be of relevance. In our view, this balancing act can be done by maintaining the **limitation on the scope of data access to raw data that was generated by the use of the product, whether actively provided by the user or not.** This is also consistent when viewed from a fairness perspective, as the data was co-generated between the manufacturer and the user, and the user has already paid for using the product. Moreover, the same inalienable right and access scope already applies to personal data. Extending it to non-personal data would therefore not only be legally coherent, but would also avoid many issues arising from needing to delineate the blurring line between personal and non-personal data. This also means that the consent-like mechanisms that the DA borrows from the GDPR should be maintained. While there are valid reasons to question this consent-based data processing regime

in general,[30] it is important to have the same architecture for both personal and non-personal data, and there currently does not seem to be a reasonable prospect to change GDPR in such a fundamental way.

Some uncertainty remains on where to draw the boundary between processed and raw data. Raw data should only be provided at the lowest level at which the manufacturer/data holder has access to it itself. For example, if the provider of a virtual assistant has access the actual sound files of the voice commands and the autmatically transcribed text of the voice commands, then only the sound files would need to be provided. If the raw sound files are not accesible, for instance, because the text is automatically transcribed on the device, then access to the text files should be provided. However, access to both sound files and text files should not be warranted by the DA, as one was the processed outcome (derived data) of the other, and considerable innovation investments went into the automatic transcription. Generally, derived data, that is, data which was aggregated or processed based on user input or sensors (raw data) in some intelligent way, should not be in scope to preserve innovation incentives. Responses by the virtual assistant based on the user input, for example, should therefore not be shared.

However, raw data can and should also include status information of the device, such as whether the device is activated or not, or error codes arising during operation (and their meanining), insofar as they can be readily derived from user input or sensors. Of course, in practice, cases can arise where it is difficult to delineate the appropriate threshold at which status information may be considered 'derived data'. If in question, this threshold can only be determined on a case-by-case basis, but the presumption should be that status data is 'raw data' and falls into the scope of the regulation. It is emphasizded again that the data holder must only share data at the lowest level available to itself, and it must not share data on how the status data was derived (say from raw sensor data).

Recommendation 2: Remove the no-competition clause (Articles 4(4) and 6(2)(e)), which otherwise undermines innovation incentives by both data holders and data access seekers.

It is difficult to see how a data access limited to such raw data co-generated by the use would materially undermine investment incentives of manufacturers. Neither the Impact Assessment nor the Recitals make a convincing case in this regard. Thus, given that the balancing of innovation incentives is already done by limiting the scope of data (Recommendation 1), we suggest **to remove other restrictions to use or share the data as far as possible**. In particular, preventing entry in the primary market in return for access to raw data that was co-generated through use would in our view overcompensate the data holder. Moreover, it would add to the economic and legal uncertainty for data access seekers that further contributes to transaction costs which impede the unlocking of data intended by the DA. Thus, as has been pointed out in our analysis, the no-competition-clause likely hinders innovation by third parties in a significant way and undermines the emergence of data markets

[30] For example, it has been proposed to move away from a consent-based architectuture to one where only the scope of applications in regulated, but not the collection and use of data, see Jan Krämer and Michael Wohlfarth (2018) 'Market power, regulatory convergence, and the role of data in digital markets'. Telecommunications Policy, 42(2), 154-171, https://doi.org/10.1016/j.telpol.2017.10.004

and data brokers. Thus, we suggest to remove the no-competition clause (Articles 4(4) and 6(2)(e)) altogether.

Recommendation 3: Introduce a rebuttable presumption that access to raw data does not impede trade secrets. Remove Article 8(6) which suggests otherwise.

It is also difficult to understand what trade secrets may be affected when only raw that was co-generated by the use of the device is to be shared. Other innovation-protecting rights, such as patents or copyright, that protect the technical design of the product or the processing of data remain of course in place. Also the Trade Secrets Directive remains in effect and the DA does not (and should not) undermine it. However, as argued in Section 2.3.2, in light of the fact that trade secrets can potentially be construed very broadly, Article 8(6) could justify a possible circumvention strategy by data holders whereby they deny any data access based on trade secrets. Instead, we argue that there should be a rebuttale presumption in the DA that access limited to raw data (as detailed in Recommendation 1) does not impede on trade secrets. This recommendation is also in line with the underlying idea of the DA that the raw data made available was co-generated and thus should be at the disposal of both the manufacturer/data holder as well as the user.

While Articles 4(3) and 5(8) provide a useful balancing of data access in case trade secrets are indeed involved, we echo the recommendation of some legal scholars[31] that Article 8(6) should be removed, and a recital should be added on the rebuttable presumption. This would provide guidance and increase legal certainty for all parties involved. If, in a specific scenario, a manufacturer/data holder can make a convincing case that raw data would indeed materially affect trade secrets and undermine its innovation incentives, then the DA would still allow for exceptions.

Recommendation 4: Introduce rebuttable presumption for a zero access price for third parties, instead of stipulating that access seekers need to negotiate a positive access price.

As a further significant simplification, we suggest to remove the requirement for the authorised third-party to negotiate a price with the data provider for accessing the data. Instead, there should be a rebuttable presumption that data access for third parties does not constitute significant additional costs for the data holder. In other words, the marginal costs of providing access to another data recipient should generally be very low, given that only those devices fall under the scope of the regulation that are connected (IoT) devices, and thus transfer the relevant data presumably to a cloud service anyway. In cases where a data holder can prove that the actual *marginal* costs significantly depart from zero, a cost-based access price may be acceptable. However, since data access is limited to (co-generated) raw data, the price should not include an additional margin on the costs.

At the same time we suggest to raise the threshold for firms exempted from providing access (see Recommendation 7) in order to ensure that only those firms that are likely to already have an appropriately sized infrastructure in place have to provide access.

[31] See Drexl et al, supra note 15.

However, we suggest to **maintain provisions on liability and technical protection measures**, foremost with the goal to ensure that the data access provided by the data holder is not abused for undermining the integrity and security of the data holder; and in order to prevent sharing and use of the data beyond what the user authorised.

The **data holder should nevertheless not have the right to further limit the purpose authorised by the user**. This includes potentially a wide purpose, such as allowing the third party to act as a data brokers and to resell (aggregated) data on their behalf. This could facilitate the emergence of data markets.

Fixing the presumed access price at zero eliminates a host of concerns and issues, as highlighted above; this includes issues arising from data being resold, including typical competition issues in vertical industries (such as hold-up and margin squeeze) that typically require heavy-handed regulation. However, it may increase concerns for sabotage, that is, incentives of the data holder to artificially degrade the quality of access. Thus, non-discrimination provisions (Article 5(1) and Article 8(3), for instance) become ever more relevant and need to be enforced strictly under this proposal. If marginal costs of providing access with the same quality do indeed significantly depart from zero, the access provider will have no difficulty demonstrating those costs in a convincing way, and the costs of doing so will be much lower than non-compliance with the DA by engaging in sabotage.

Fixing the presumed access price at zero also eliminates the economic imbalance between the direct access scenario (where authorised third parties access data directly) and the indirect access scenario (where data is transferred to a third party via the user).

Recommendation 5: Remove most product exclusions. Exclude only those products that provide general connectivity and computing resources, which are fully configurable by the user.

The proposed DA suggests to exclude a number of products (such as webcams) without providing a clear justification for doing so. As discussed in Section 2.3.1, the current distinction between those products that shall fall under the Regulation and those that are exempt seems arbitrary and not future-proof. We thus suggest to limit the number of products that are excluded from the regulation. The focus should be maintained on connected products, that is, products that are able to transmit data generated by its use over a public communications channel. However, **we suggest to exclude only those products that provide general connectivity and computing resources (ISPs, servers, or PCs, for instance), which are fully configurable by the user** (that is, which allow the user to install and configure any compatible software, including the operating system). This is because, on such products, the user would not have any restrictions to accessing any relevant user-generated data.

Recommendation 6: Allow users to transfer data to any third party that they deem useful, including gatekeepers under the DMA, to maximize innovation potential from data.

We suggest that gatekeepers under the DMA should not generally be denied access to the data (remove Article 5(2)(c) and 6(2)(d)). Gatekeepers may especially be in a position to provide valuable services to consumers based on such data, and often they provide connected products themselves. This would also mean that gatekeepers could get access to the data of other gatekeepers offering connected products, which may indeed increase competition to the benefit of users. However, by

definition gatekeepers do have a superior means to reach a large number of consumers, and better financial means than most other firms. Thus, they are in a particurly favourable position to entice consumers through their existing services or through financial means to transfer data made available under the DA.Thus, it is reasonable to maintain Article 5(2)(a) and 5(2)(b) to ensure that gatekeepers cannot not simply buy out data from users, or nudge them otherwise to transfer data.

If policymakers see the need for additional restrictions on data access or use by gatekeepers, then this should be considered as part of the sector-specific regulation under the DMA, and not as part of the horizontal regulation under the DA. Indeed, the DMA already includes limitations on data re-combination and use by gatekeepers, and the list of core platform services already includes virtual assistance. Should the need arise, the list of core platform services can be extended appropriately.

Recommendation 7: Exclude not only micro- and small-sized enterprises, but also medium-sized enterprises from having to provide data access to connected products under the DA.

As with any regulation, the DA introduces some compliance costs. While being horizontal in nature, the regulation needs to be proportionate and not place an overly high compliance burden on small firms. Acknowledging this trade off, the DA already exempts data holders that are micro and small enterprises from having to provide access to the data generated by their IoT products (Article 7(1)). Especially in light of our suggestion to presume that access to data is provided free of charge (Recommendation 4), which means that data holder also need to bear the (arguably small) direct costs of providing access, we deem it necessary to raise the threshold at which manufacturers/data holders need to comply with the DA. In particular, we suggest that medium-sized enterprises should be exempt from the obligations under Chapter II of the DA. The threshold is still relatively low, as the Commission Recommendation 2004/361/EC, defines medium-sized enterprises as those that "employ fewer than 250 persons and which have an annual turnover not exceeding EUR 50 million, and/or an annual balance sheet total not exceeding EUR 43 million." At the same time, SME's that are users of IoT products should, of course, have the same user rights. The provision of unfair contractual terms under Article 13 (already applying to SMEs) should be maintained.

Overall, we believe that these changes would provide for a simpler and yet more effective proposal for the DA. Many of the restrictions and accompanying economic transaction costs would be resolved, which would also facilitate the emergence of data brokers and data markets. Such specialized data intermediaries are required to unlock the ability of data to flow more freely, and for providing access to data in bulk. At the same time, following these recommendation would push the DA not only towards a more economically coherent framework, but also provide for a legally coherent approach for access to personal data and non-personal data. The more detailed goals of the DA, such as enabling 'repair services' are not addressed by the recommendation, and we also believe they should not be addressed by the DA explicitly. For this, regulators would need to impose sector-specific regulation that is tailored to the specific use cases.

cerre Centre on Regulation in Europe

Avenue Louise 475 (box 10)
1050 Brussels, Belgium
+32 2 230 83 60
info@cerre.eu
www.cerre.eu
@CERRE_ThinkTank
Centre on Regulation in Europe (CERRE)
CERRE Think Tank