



DATA ACT: TOWARDS A BALANCED EU DATA REGULATION

March 2023

— Jan Krämer (Coord)

Giuseppe Colangelo

Heiko Richter

Daniel Schnurr



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 (Institut national de l’information géographique et forestière), Huawei, 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.

© Copyright 2022, Centre on Regulation in Europe (CERRE)

info@cerre.eu – www.cerre.eu



TABLE OF CONTENTS

ABOUT CERRE.....	3
ABOUT THE AUTHORS.....	4
1. EUROPEAN PROPOSAL FOR A DATA ACT: A FIRST ASSESSMENT.....	10
2. IMPROVING THE ECONOMIC EFFECTIVENESS OF THE B2B AND B2C DATA SHARING OBLIGATIONS IN THE PROPOSED DATA ACT	27
3. ACCESS TO PRIVATE SECTOR DATA FOR THE COMMON GOOD: A CRITICAL REVIEW OF CHAPTER V OF THE PROPOSED DATA ACT.....	39
4. SWITCHING AND INTEROPERABILITY BETWEEN DATA PROCESSING SERVICES IN THE PROPOSED DATA ACT	47



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, the specification of market rules, and 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 AUTHORS



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.



Giuseppe Colangelo is a Jean Monnet Professor of European Innovation Policy and an Associate Professor of Law and Economics at the University of Basilicata (Italy). He also serves as an Adjunct Professor of Markets, Regulation and Law, and of Competition and Markets of Innovation at LUISS (Italy). He is a fellow of the Stanford Law School and University of Vienna Transatlantic Technology Law Forum (TTLF), the scientific coordinator of the Research Network for Digital Ecosystem, Economic Policy and Innovation (Deep-In), and an academic affiliate with the International Center for Law & Economics (ICLE).



Heiko Richter is a senior research fellow at the Max Planck Institute for Innovation and Competition in Munich (Germany). He received his master's degree in business administration from the University of Mannheim, completed his legal state examinations and PhD in Berlin, and holds an LL.M. from Columbia University, New York. His research addresses the regulation of data and information, copyright law, and competition law. He advises German and EU policy makers in these areas.



Daniel Schnurr is a CERRE Research Fellow and Professor of Machine Learning and Uncertainty Quantification at the University of Regensburg. He is also head of the research group Data Policies.

He received his Ph.D. in Information Systems from the Karlsruhe Institute of Technology, where he previously studied Information Engineering and Management (B.Sc. & M.Sc.). Daniel Schnurr has published in leading journals in Information Systems and Economics on competition and data sharing in digital markets, regulation of data-driven market power and competition and cooperation in telecommunications markets.

His current research focuses on the role of artificial intelligence in competition, privacy and data sharing in digital markets as well as regulation of AI and the data economy.



EUROPEAN PROPOSAL FOR A DATA ACT

A FIRST ASSESSMENT

Giuseppe Colangelo



TABLE OF CONTENTS

1. INTRODUCTION AND BACKGROUND	8
2. PROBLEMS AND OBJECTIVES	11
3. NEW DATA ACCESS AND SHARING RIGHT: SCOPE AND MAIN FEATURES.....	15
3.1 Competitive Level Playing Field and Protection of Weaker Parties	19
3.2. The Interface With Intellectual Property Rights.....	22
4. BUSINESS-TO-GOVERNMENT DATA SHARING	25
5. DATA PROCESSING SERVICES SWITCHING AND INTERNATIONAL DATA ACCESS.....	27
6. INTEROPERABILITY	30
7. IMPLEMENTATION AND ENFORCEMENT	32



1. INTRODUCTION AND BACKGROUND

On 23 February 2022, the European Commission unveiled its proposal for a Data Act (DA)¹. As declared in the Impact Assessment², the DA complements two other major instruments shaping the European single market for data, such as the Data Governance Act³ and the Digital Markets Act (DMA)⁴, and is **a key pillar of the European Strategy for Data in which the Commission announced the establishment of EU-wide common, interoperable data spaces** in strategic sectors to overcome legal and technical barriers to data sharing⁵. The DA also represents the latest effort of European policy makers to ensure free flows of data through a broad array of initiatives which differ among themselves in terms of scope and approach: some interventions are horizontal, others are sector-specific; some mandate data sharing, others envisage measures to facilitate the voluntary sharing; some introduce general data rights, others allow asymmetric data access rights.

Notably, the General Data Protection Regulation (GDPR) enshrined a general personal data portability right for individuals⁶, the Regulation on the free flow of non-personal data facilitated business-to-business data sharing practices⁷, the Open Data Directive aimed to put government data to good use for private players⁸, and the Data Governance Act attempted to harmonising conditions for the use of certain public sector data and further promoting the voluntary sharing of data by increasing trust in neutral data intermediaries that will help match data demand and supply in the data spaces⁹. Sector-specific legislations on data access have also been adopted or proposed to address identified market failures, such as in the automotive¹⁰, payment service providers¹¹, smart metering information¹²,

¹ European Commission, 'Proposal for a Regulation of the European Parliament and of the Council on harmonised rules on fair access and use of data (Data Act)' COM(2022) 68 final.

² 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, 1.

³ Regulation (EU) 2022/868 on European data governance (Data Governance Act) [2022] OJ L 152/1.

⁴ Regulation (EU) on contestable and fair markets in the digital sector (Digital Markets Act).

⁵ European Commission, 'A European strategy for data' COM(2020) 66 final.

⁶ 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, [2016] OJ L 119/1, Article 20.

⁷ Regulation (EU) 2018/1807 on a framework for the free flow of non-personal data in the European Union, [2018] OJ L 303/59.

⁸ Directive (EU) 2019/1024 on open data and the re-use of public sector information, [2019] OJ L 172/56.

⁹ Data Governance Act, supra note 3.

¹⁰ Regulation (EU) 2018/858 on the approval and market surveillance of motor vehicles and their trailers, and of systems, components and separate technical units intended for such vehicles, amending Regulations (EC) No 715/2007 and (EC) No 595/2009 and repealing Directive 2007/46/EC, [2017] OJ L 151/1.

¹¹ Directive (EU) 2015/2366 on payment services in the internal market, [2015] OJ L 337/35, Article 67.

¹² Directive (EU) 2019/944 on common rules for the internal market for electricity and amending Directive 2012/27/EU, [2019] OJ L 158/125; and Directive 2009/73/EC concerning common rules for the internal market in natural gas and repealing Directive 2003/55/EC, [2009] OJ L 211/94.



electricity network data¹³, intelligent transport systems¹⁴, renewables¹⁵, and energy performance of buildings¹⁶.

Against this background, given that the DA is a horizontal legislative initiative fostering data sharing by unlocking machine-generated data and overcoming vendor lock-in, an issue of **coherence with existing and forthcoming EU data-related legislations** emerges.

The premise of such regulatory intervention is provided by the fact that an ever-increasing amount of data is generated by machines or processes based on emerging technologies, such as the Internet of Things (IoT), and is used as a key component for innovative services and products, in particular for developing artificial intelligence (AI) applications¹⁷. The ability to gather and access different data sources is crucial in order for IoT innovation to thrive. IoT environments are possible as long as all sorts of devices can be interconnected and can exchange data in real-time. Therefore, access to data and data sharing practices are pivotal factors for unlocking competition and incentivising innovation.

From this perspective, **the proposal for a DA represents the last episode of a long thread of European Commission interventions**. Since the 2015 Digital Single Market Communication, the Commission has indeed emphasised the central role played by big data, cloud services, and the IoT for the EU's competitiveness, also pointing out that the lack of open and interoperable systems and services and of data portability between services represents a barrier for the development of new services¹⁸. The issue of (limited) access to machine-generated data has been raised in the 2017 Communication on the European Data Economy¹⁹, where the Commission envisaged some potential interventions which are now advanced by the DA, as well as in more recent Commission' Communications on a common European data space and a European strategy for data²⁰. In particular, the latter indicated the "issues related to usage rights for co-generated data (such as IoT data in industrial settings)" as a priority area for a legislative intervention²¹.

Moreover, the IoT economy has been the subject of a recent sector inquiry which offered a comprehensive insight into the current structure of IoT environments and the competitive dynamics that are shaping their development²². In particular, the Commission underlined the role of digital ecosystems within which a huge number of IoT interactions take place and identified the most widespread operating systems and general voice assistants as the key technological platforms that

¹³ Regulation (EU) 2017/1485 establishing a guideline on electricity transmission system operation, [2017] OJ L 220/1; and Regulation (EU) 2015/703 establishing a network code on interoperability and data exchange rules, [2015] OJ L 113/13.

¹⁴ Directive 2010/40/EU on the framework for the deployment of Intelligent Transport Systems in the field of road transport and for interfaces with other modes of transport Text with EEA relevance, [2010] OJ L 207/1.

¹⁵ Proposal for a Directive amending Directive (EU) 2018/2001, Regulation (EU) 2018/1999 and Directive 98/70/EC as regards the promotion of energy from renewable sources, and repealing Council Directive (EU) 2015/652, COM(2021) 557 final.

¹⁶ Proposal for a Directive on the energy performance of buildings (recast), COM(2021) 802 final.

¹⁷ On the economic value of data, see Jan Krämer, Daniel Schnurr, and Sally Broughton Micova (2020), 'The role of data for digital markets contestability', CERRE Report <https://cerre.eu/wp-content/uploads/2020/08/cerre-the-role-of-data-for-digital-markets-contestability-case-studies-and-data-access-remedies-september2020.pdf>.

¹⁸ European Commission, 'A Digital Single Market Strategy for Europe', COM(2015) 192 final, 14.

¹⁹ European Commission, 'Building a European Data Economy', COM(2017) 9 final, 12-13.

²⁰ European Commission, 'A European strategy for data', supra note 5, 10; and European Commission, 'Towards a common European data space', COM(2018) 232 final, 10.

²¹ European Commission, 'A European strategy for data', supra note 5, 13, and 26.

²² European Commission, 'Final Report - Sector inquiry into consumer Internet of Things' COM(2022) 19 final.



connect different hardware and software components of an IoT business environment, increase their complementarity as well as provide a single access point to diverse categories of users²³. Against this backdrop, interoperability is deemed to play a crucial role in improving consumer choice and preventing lock-in into providers' products.

To contribute to the current policy debate, **this paper will provide a first assessment of the tabled DA and will suggest possible improvements for the ongoing legislative negotiations.** The paper is structured as follows. Section 2 deals with the problems addressed and the objectives pursued by the legislative initiative. Section 3 analyses the scope of the new data access and sharing right for connected devices. Then, Section 4 investigates the provisions aimed at favouring business-to-government data sharing for the public interest. Section 5 deals with the rules which tackle the vendor lock-in problem in data processing services by facilitating switching between cloud and edge services. Section 6 analyses the requirements set forth regarding interoperability. Finally, Section 7 concludes by addressing the governance structure. Each section briefly summarises the DA proposal and then makes a first assessment with suggestions for improvements.

²³ Commission Staff Working Document accompanying the 'Final Report - Sector inquiry into consumer Internet of Things' COM(2022) 10 final.



2. PROBLEMS AND OBJECTIVES

The proposed DA aims to achieve **five objectives**²⁴:

- to **facilitate access to and the use of data by consumers and businesses**, while preserving incentives to invest in ways of generating value through data;
- to **provide for the use by public sector bodies and EU institutions of data held by enterprises** in certain situations where there is an **exceptional data need**;
- to **facilitate switching between cloud and edge services**;
- to **put in place safeguards against unlawful data transfer without notification by cloud service providers**;
- and to **provide for the development of interoperability standards for data to be reused between sectors**, in a bid to remove barriers to data sharing across domain-specific common European data spaces and between other data that are not within the scope of a specific common European data space.

These goals reflect the main problem that the initiative detects, which is the insufficient availability of data for use and reuse. Notably, although the use of connected products increasingly generates data which in turn may be used as input by services that accompanied these products, **consumers and companies (especially start-ups, small and medium-sized enterprises - SMEs²⁵) have limited ability to realise the value of data generated by their use of products and related services**, since they lack effective control over the data²⁶. In many sectors, manufacturers are often able to determine, through their control of the technical design of the product or related services, what data is generated and how it can be accessed, even though they have no legal right to the data²⁷. In situations where the data is generated by machines through the use of products and related services by businesses and consumers, it is indeed unclear whether the acquisition of an object includes the benefit of having a share in the value of the data²⁸. Legal uncertainties regard the question of the applicability of the Database Directive to machine-generated data²⁹ and also pertain to the portability and interoperability of data. Moreover, with regards to data subjects, the GDPR is considered insufficient to alleviate the problem of limited control over the data, because the right to data portability does not apply to non-personal data and it is confined to personal data processed for the performance of a contract or based on consent³⁰. In a similar vein, sectoral legislations ensure that only in certain areas (e.g., electricity, banking, cars) third parties can have access to relevant data.

Furthermore, **low levels of data availability restrain the possibility to create added value in business-to-business (B2B) relations** as data access is sometimes a precondition for market entry, participation

²⁴ Data Act proposal, supra note 1, Explanatory Memorandum, 3.

²⁵ Ibid., Recital 36.

²⁶ Impact Assessment, supra note 2, 9-10.

²⁷ Data Act proposal, supra note 1, Recital 19.

²⁸ Impact Assessment, supra note 2, 15-16.

²⁹ Directive 96/9/EC on the legal protection of databases [1996] OJ L 77/20.

³⁰ Impact Assessment, supra note 2, 10; Data Act proposal, supra note 1, Recital 31.



in a supply chain or innovation³¹. While some codes of conduct exist (e.g., on agricultural data sharing)³², B2B data sharing is essentially based on contracts, therefore it may be affected by imbalances in negotiating power (and related abusive conduct), which arise when the party requesting access to data needs the data for developing or running innovative business models and can only get that data from a specific data holder³³. Such contractual imbalances particularly harm SMEs without a meaningful ability to negotiate the conditions for access to data, who may have no other choice than to accept ‘take-it-or-leave-it’ contractual terms³⁴.

Furthermore, although data is essential for driving evidence-based policymaking, it is mainly created outside of the public sector³⁵. The **lack of efficient rules and practices for public sector bodies using business data** also creates a burden for companies as they do not know what to expect in terms of scope of requests, licensing or charging possibilities³⁶.

Moreover, given that data are useless without data-processing infrastructures, according to the Impact Assessment the lack of a competitive market for cloud and edge services is an additional obstacle for generating value through data, hence the DA considers the ability for customers to switch from one data processing service to another as a key condition for a more competitive market³⁷. **Unfair practices and vendor lock-in produce significant barriers to switching of cloud and edge services, which the Free flow of non-personal data Regulation has been unable to soften effectively so far**³⁸. Notably, its self-regulatory approach is meant to address this problem by encouraging the development of codes of conduct for easier cloud switching. However, the resulting switching cloud providers and data porting (SWIPO) codes have been adopted just by a small number of players³⁹. In addition, the industry’s proposed codes do not comply with the requirements of the Regulation as they are largely limited to an approach of pre-contractual transparency, instead of addressing also technical and economic hurdles. Given the limited efficacy of the self-regulatory frameworks developed in response to the Regulation and the general unavailability of open standards and interfaces, the SWIPO codes are therefore considered insufficient to have a positive impact on the cloud market dynamics⁴⁰.

Finally, **data sharing within and between sectors requires an interoperability framework**. Indeed, the absence of common and compatible standards for both semantic and technical interoperability represents the main barrier to data sharing and reuse, and a very relevant problem for the effective portability of data and for switchability between cloud and edge services⁴¹.

³¹ Impact Assessment, supra note 2, 11.

³² Data Act proposal, supra note 1, Recital 25.

³³ Impact Assessment, supra note 2, 17.

³⁴ Data Act proposal, supra note 1, Recital 51.

³⁵ Impact Assessment, supra note 2, 12 and 19.

³⁶ Ibid., 12.

³⁷ Ibid., 13-14; and Data Act proposal, supra note 1, Recital 69.

³⁸ Impact Assessment, supra note 2, 19-20.

³⁹ These codes are available at <https://swipo.eu>.

⁴⁰ Ibid., 20. See also Data Act proposal, supra note 1, Recital 70 and Explanatory Memorandum, 4.

⁴¹ Data Act proposal, supra note 1, Recital 2; Impact Assessment, supra note 2, 22.



In summary, **alongside the general goal of empowering users to gain and exert control over their data, the DA is also pursuing other objectives, such as safeguarding and promoting competition, innovation, and fairness in the digital economy**⁴².

The concept of fairness is interpreted in broad terms and refers to the allocation of economic value from data among actors⁴³. This concern stems from the observation that data value is concentrated in the hands of relatively few large companies, while the data produced by connected products or related services are an important input for aftermarket, ancillary and other services⁴⁴. Therefore, **to achieve a greater balance in the distribution of such value, the fairness of both contractual terms and market outcomes are addressed**. Indeed, the creation of a cross-sectoral governance framework for data access and use aims to ensure contractual fairness, namely to rebalance the negotiation power for SMEs in data sharing contracts and prevent vendor lock-in in cloud and edge services.⁴⁵ As a result, fairer and more competitive market outcomes shall be promoted in aftermarkets and in data processing services⁴⁶.

Such a broad notion of fairness has also been applied in the DMA and this may not be without legal risks. In the DMA, the unfairness is related to the inability of market participants to adequately capture the benefits resulting from their innovative efforts because of gatekeepers' gateway position and superior bargaining power⁴⁷. Moreover, contestability and fairness are considered intertwined, given that the lack of the former can enable a large player to engage in unfair practices and, similarly, unfair practices by a gatekeeper can reduce the possibility of rivals to contest its position⁴⁸. Concerns about fair dealing in online markets have also motivated the platform-to-business (P2B) Regulation, which noted that, given the increasing dependence of business users on online intermediation services, the providers of those services often have superior bargaining power which enables them to behave unilaterally in a way that can be unfair⁴⁹.

⁴² Data Act proposal, supra note 1, Recital 6.

⁴³ Ibid., Explanatory Memorandum, 2; European Commission, 'Inception Impact Assessment – Data Act', Ares (2021) 3527151, 1, https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13045-Data-Act-amended-rules-on-the-legal-protection-of-databases_en.

⁴⁴ Data Act proposal, supra note 1, Explanatory Memorandum, 1, and Recital 6. See also Victoria Fast, Daniel Schnurr, and Michael Wohlfarth (2022), 'Regulation of Data-driven Market Power in the Digital Economy: Business Value Creation and Competitive Advantages from Big Data', https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3759664; Hemant K. Bhargava, Olivier Rubel, Elizabeth J. Altman, Ramnik Arora, Jörn Boehnke, Kaitlin Daniels, Timothy Derdenger, Bryan Kirschner, Darin LaFramboise, Pantelis Loupos, Geoffrey Parker, and Adithya Pattabhiramaiah (2020), 'Platform data strategy', 31 Marketing Letters 323.

⁴⁵ Inception Impact Assessment, supra note 43, 2.

⁴⁶ Ibid. See also Lucie Antoine and Matthias Leistner (2022), 'IPR and the use of open data and data sharing initiatives by public and private actors', Study for the European Parliament, 78, <https://www.europarl.europa.eu/committees/en/supporting-analyses/sa-highlights>.

⁴⁷ Digital Markets Act, supra note 4, Recital 33. See also Gregory S. Crawford, Jacques Crémer, David Dinielli, Amelia Fletcher, Paul Heidhues, Monika Schnitzer, Fiona M. Scott Morton, and Katja Seim, 'Fairness and Contestability in the Digital Markets Act', (2021) Yale Digital Regulation Project, Policy Discussion Paper No. 3, <https://tobin.yale.edu/sites/default/files/Digital%20Regulation%20Project%20Papers/Digital%20Regulation%20Project%20-%20Fairness%20and%20Contestability%20-%20Discussion%20Paper%20No%203.pdf>.

⁴⁸ Ibid., Recital 34.

⁴⁹ Regulation (EU) 2019/1150 on promoting fairness and transparency for business users of online intermediation services, [2019] OJ L 186/57.



ASSESSMENT

Alongside the general goal of empowering users to gain and exert control over their data, the DA is pursuing other objectives, such as safeguarding and promoting competition, innovation, and fairness in the digital economy. By aiming to achieve different goals, the DA introduces provisions which target different players and address different problems. As a consequence, **the DA would require further efforts to ensure both coordination among the obligations and a clear connection between the obligations and the objectives pursued by the legislative initiative.**



3. NEW DATA ACCESS AND SHARING RIGHT: SCOPE AND MAIN FEATURES

The DA moves from the premise that the manufacturer/designer of a product or related service typically has exclusive control over the use of data generated by the use of a product or related service, which contributes to user lock-in and hinders market entry for players offering aftermarket services and novel services. To address this problem, the **DA envisages a cross-sectoral governance framework to ensure that products are designed and manufactured and related services are provided in such a manner that data generated by their use are easily accessible to the user.**

Notably, while users of IoT products and related services are empowered with new access and use rights⁵⁰, and a right to share the generated data with third parties⁵¹, manufacturers and designers are required to design products in a way that makes the data directly accessible by default or, where data cannot be directly accessed from the product, makes available the data generated promptly and free of charge to users⁵².

In this scenario, the difficulty of coordinating different goals emerges from the outset. To empower users, Article 4 grants them the right to use (and to authorise a third party to use) the data “for any lawful purpose”, namely without any limitation deriving from the proclaimed goal to promote competition and enabling innovation by more market players⁵³. Therefore, users’ empowerment apparently prevails over other goals or at least indirectly incorporates them⁵⁴. Nonetheless, this absolute right faces a limitation: to safeguard investment incentives, users and third parties cannot develop products that compete with the product from which data originates⁵⁵. Therefore, the safeguard of incentives to innovate in primary markets prevails over users’ empowerment, the free flow of data, and especially competition. This seems to confirm that, **by commingling different objectives without a clear hierarchy of values, DA obligations risk lacking consistency.**

Insofar as personal data are processed, the requirements set forth in the GDPR must be fulfilled⁵⁶. When non-personal data is involved, the data holder is allowed to use only those authorised by the user on the basis of a contractual agreement⁵⁷. Furthermore, the right to share data with third parties complements to some extent the right to receive and port personal data under Article 20 GDPR by mandating the technical feasibility of third-party access for both personal and non-personal data⁵⁸.

⁵⁰ Data Act proposal, supra note 1, Article 4.

⁵¹ Ibid., Article 5.

⁵² Ibid., Articles 3(1) and 4(1).

⁵³ Ibid., Explanatory Memorandum, 13.

⁵⁴ See Max Planck Institute for Innovation and Competition (2022), ‘Position Statement on the Data Act’, 7-9, <https://www.ip.mpg.de/en/research/research-news/position-statement-on-the-eu-data-act.html>, suggesting to introduce a purpose

limitation by restraining the permitted uses to added value uses and services.

⁵⁵ Data Act proposal, supra note 1, Article 4(4) and 6(2)(e).

⁵⁶ Ibid., Article 4(5) and Recital 24.

⁵⁷ Ibid., Article 4(6). See Antoine and Leistner, supra note 46, 92, finding hard to understand the necessity to assign such contractual control to the user even if neither the fundamental rights of protecting personal data nor an exclusive IPR or other property right apply.

⁵⁸ Ibid., Article 5 and Recital 31.



Indeed, while under GDPR users can transfer personal data to third parties free of charge, the DA requires a contract with the third party.

In a similar way, the DA appears more lenient than the DMA. According to Article 6(9) DMA, indeed, gatekeepers shall ensure that end users or third parties authorised by end users can freely port the data provided by the end user (or generated through the activity of the end user in the context of the relevant core platform service) continuously and in real-time.

Furthermore, although the DA aligns with the GDPR supporting the principles of data minimisation and data protection by design and by default⁵⁹, the provisions introducing the new data access and sharing right however prescribe neither that the products should be designed in a way that data subjects are allowed to use them anonymously (or in the least privacy intrusive way) nor that data holders should anonymise data as much as possible⁶⁰. In contrast, in the business-to-government (B2G) data sharing Chapter (see *infra* Section 4), the proposal states that the data holder should take reasonable efforts to anonymise the data or, where such anonymisation proves impossible, should apply technological means such as pseudonymisation and aggregation, prior to making the data available⁶¹.

Whereas the access to users must be granted free of charge, the data holder may instead ask for compensation from a third party when it is obliged under the DA (or under EU law or national legislation implementing EU law) to make data available to it⁶². In such case, the compensation shall be reasonable and the parties involved (i.e., data holder and data recipient) must agree on fair, reasonable, and non-discriminatory (FRAND) terms⁶³. This represents a significant departure from the the Second Payment Services Directive (PSD2) and the GDPR where the access to data account and the portability respectively are free of charge. Therefore, at least with regard to the GDPR, it should be clarified which instrument takes precedence⁶⁴. Moreover, given that the FRAND obligation would cover also the cases under which the data holder is obliged to make data available pursuant to other EU law (or national legislation implementing EU law), **the DA may generate conflicts with other EU sector-specific regulations**. Finally, given that, in the context of standard-essential patents (SEPs), parties have regularly failed to reach a licensing agreement on FRAND terms⁶⁵, **the significant uncertainty about the very meaning of the FRAND paradigm can spawn a new wave of litigation**.

By setting horizontal principles for all sectors, **DA rules potentially have a wide scope of application covering all IoT devices, business-to-consumers (B2C) and B2B relationships, and personal and non-**

⁵⁹ Ibid., Recital 8.

⁶⁰ European Data Protection Board and European Data Protection Supervisor (2022), 'Joint Opinion 2/2022 on the Proposal of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act)', https://edpb.europa.eu/our-work-tools/our-documents/edpb-edps-joint-opinion/edpb-edps-joint-opinion-2022-proposal-european_en.

⁶¹ Data Act proposal, *supra* note 1, Recital 64 and Article 20(2).

⁶² Ibid., Articles 8(1) and 12(1).

⁶³ Ibid., Articles 8(1) and 9(1).

⁶⁴ Inge Graef and Marting Husovec (2022), 'Seven Things to Improve in the Data Act' https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4051793.

⁶⁵ See, e.g., Giuseppe Colangelo and Valerio Torti (2022), 'Anti-suit injunctions and geopolitics in transnational SEPs litigation', *European Journal of Legal Studies*; Oscar Borgogno and Giuseppe Colangelo (2021), 'SEPs licensing across the supply chain: an antitrust perspective', 11 *Queen Mary Journal of Intellectual Property* 484.



personal data. Nonetheless, in regard to products, the scope of the DA includes physical products that obtain, generate or collect data concerning their performance, use or environment and that are able to communicate that data via a publicly available electronic communications service (e.g., vehicles, home equipment and consumer goods, medical and health devices or agricultural and industrial machinery)⁶⁶, while products that are primarily designed to display or play content, or to record and transmit content (e.g., personal computers, servers, tablets and smartphones, cameras, webcams, sound recording systems, and text scanners) are excluded, as well as electronic communications services (e.g., fixed-line telephone networks, television cable networks, satellite-based networks and near-field communication networks)⁶⁷.

Furthermore, to avoid undermining manufacturers' investment incentives, DA's new rights cover only generated data (i.e., data that "represent the digitalisation of user actions and events"), hence do not apply to derived or inferred data⁶⁸.

Finally, for the same reason, as already mentioned, although the user is entitled to use the data for any lawful purpose⁶⁹ and the third party receiving data can process such data for the purposes and under the conditions agreed with the user⁷⁰, their rights are limited to uses which do not compete with the product from which data originates⁷¹.

Within this framework, **further clarity about some relevant definitions would be welcomed.** Indeed, **the proposal seems to describe a simplified relationship between a user and a data holder, while the IoT scenario may involve multiple players in the value chain.**

A problem of oversimplification also regards the definition of products. Moreover, it is not clear why products such as webcams are excluded from the scope of DA, despite being prototypical IoT devices.

In addition, **both the rationale and the implementation of the non-compete clause raise doubts.** About the latter, the notion of competing products is far from conclusive since in some cases it may be difficult to draw the line and define the competitive relationships between products⁷². In addition, it is not clear if and how the non-compete clause will be also applied to products already in commerce. Moreover, the current version of the clause appears extremely broad because it implies that users and third parties are prevented from ever entering the primary market, while a proper balance between competitive goals and safeguards of incentives to invest would at least require the introduction of a sunset provision.

⁶⁶ In line with the findings of the Commission's sector inquiry (supra note 22), a special emphasis is given to the role of virtual assistants: see Article 7(2) and Recital 22.

⁶⁷ Data Act proposal, supra note 1, Article 2(2) and Recitals 14-15.

⁶⁸ Ibid., Recitals 14 and 17. Such emphasis on the incentive problems of manufactures is criticized by Wolfgang Kerber (2022), 'Governance of IoT Data: Why the EU Data Act will not fulfill its objectives', 16-19, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4080436.

⁶⁹ Data Act proposal, supra note 1, Recital 28.

⁷⁰ Ibid., Article 6(1).

⁷¹ Ibid., Article 4(4) and 6(2)(e).

⁷² See, e.g., Jacques Crémer, Yves-Alexandre de Montjoye, and Heike Schweitzer (2019), 'Competition policy for the digital era', <https://ec.europa.eu/competition/publications/reports/kd0419345enn.pdf>, on the problems with market definition in digital markets.



With regard to its rationale, one might wonder why users and data recipients are not allowed to use such data to compete in the primary market. Given that the aim of the DA is “to foster the development of new, innovative products or related services, stimulate innovation on aftermarkets, but also stimulate the development of entirely novel services making use of the data”⁷³, there is an apparent lack of justification in limiting the promotion of competition and innovation to aftermarkets. In addition, because of the argument for the protection of investment incentives, the scope of the new right envisaged by the DA is already limited with regard to the kind of data that could be used (i.e., only generated data, rather than also derived or inferred data).

It is worth noting that, alongside the described **limits regarding the type of data, the type of products, and the type of use by data recipients**, the DA introduces **additional limits to the scope of the new access and sharing right with regard to the type of data holders (by exempting SMEs from product design obligations) and the type of data recipients (by excluding gatekeepers from the list of potential beneficiaries)**, as we will illustrate in the next paragraph.

While many provisions of the DA have a strong competition policy flavour⁷⁴, these limiting factors appear not fully coherent with such a goal.

ASSESSMENT

While the aim of the new access and sharing right is essentially to unlock machine-generated data, the DA’s attempt to pursue different objectives (i.e., user empowerment, competition, innovation, fairness) affects the provisions about the scope and the main features of the new right. **Because of the lack of a hierarchy of values, such provisions appear sometimes not fully coherent among themselves.** In particular, while the new right is so extensive to include any lawful purpose, at the same time it faces the limitation of products that compete with the product from which data originates. Both the broad scope of user right and its limit related to primary markets would require a clear justification.

Relevant **definitions would benefit from further clarification** as well. Indeed, the proposal seems to rely on an oversimplified definition of both products and the relationship between users and data holders, which may be deemed unfit to deal with the complexity of the IoT scenario.

Finally, given that the data holder may ask for compensation from a third party when it is obliged to make data available to it, the reference to FRAND conditions may not only be controversial about its meaning but may also generate **conflicts with other EU sector-specific regulations.**

⁷³ Ibid., Recital 28. See also Explanatory Memorandum, 13, stating that the proposal “allows for a competitive offer of aftermarket services, as well as broader data-based innovation and the development of products or services unrelated to those initially purchased or subscribed to by the user.”

⁷⁴ Peter Georg Picht (2022), ‘Caught in the Acts: Framing Mandatory Data Access Transactions under the Data Act, further EU Digital Regulation Acts, and Competition Law’, Max Planck Institute for Innovation and Competition Research Paper No. 22-05, <https://ssrn.com/abstract=4076842>.



3.1 Competitive Level Playing Field and Protection of Weaker Parties

The proposal of a new data access and sharing right is meant to promote a competitive offer of aftermarket services as well as the development of products or services unrelated to those initially purchased or subscribed to by the user. In this scenario, **the DA introduces an asymmetric regulation, which operates at two layers by helping SMEs to get access to relevant data⁷⁵ and rebalancing their bargaining power vis-à-vis large players⁷⁶.**

Under this logic, with regard to the former goal, **micro and small enterprises are exempted** from abiding by the data sharing obligation⁷⁷: given the current state of technology, it is considered overly burdensome to impose over them design obligations⁷⁸. Micro and small enterprises are also exempted from the obligation to provide public sector bodies and EU institutions data in situations of exceptional need⁷⁹. Further, to protect SMEs from excessive economic burdens which would make it commercially too difficult for them to develop and run innovative business models, the compensation for making data available to be paid by them shall not exceed the direct cost of making the data available to the data recipient⁸⁰. Such exceptions indirectly seem to reveal the high implementation and transactions costs that this regulation will likely entail and the related risk of undermining the promotion of innovation.

On the contrary, replicating the asymmetric treatment imposed by the PSD2 over banks, firms designated as **gatekeepers in core platform services under the DMA are not eligible to receive data**, either directly or indirectly⁸¹, given their “unrivalled ability” to acquire data⁸². Nonetheless, such exclusion does not prevent them from obtaining data through other lawful means (e.g., pursuant to the GDPR)⁸³.

The assessment of benefits and drawbacks of any asymmetric regulation requires further investigation. The PSD2’s access to data account rule, for instance, has been criticised for the lack of reciprocity in data sharing obligation between BigTechs and banks⁸⁴. In the case of the DA, on the one side, it may be argued that, even if focused on services rather than products, the DMA already addresses competitive concerns related to the role of gatekeepers imposing over them obligations which, among the other things, limit some data uses. In addition, the DMA allows the Commission to add new services and new obligations as a result of a market investigation. Moreover, the DA includes a non-compete clause which would prevent the risk of leveraging a market position in core platform services on secondary markets. Therefore, if current and future competitive risks are already under

⁷⁵ Data Act proposal, supra note 1, Recitals 3 and 36.

⁷⁶ Ibid., Recital 51.

⁷⁷ Ibid., Article 7(1).

⁷⁸ Ibid., Recital 37, which specifies that is not the case where a micro or small enterprise is sub-contracted to manufacture or design a product.

⁷⁹ Ibid., Article 14(2).

⁸⁰ Ibid., Article 9(2) and Recital 44.

⁸¹ Ibid., Articles 5(2) and 6(2)(d).

⁸² Ibid., Recital 36.

⁸³ Ibid.

⁸⁴ Miguel de la Mano and Jorge Padilla (2018), ‘Big Tech Banking’, 14 Journal of Competition Law and Economics 494.



control, a restriction to the access and use of data may just hinder the development of innovative products or services, as well as a bidirectional access to data account rule in PSD2 could have been used to enhance digital payment services. On the other side, if the concern is about gatekeepers' data accumulation, it is surprising that there are no limitations for manufacturers and data holders to sell them access to the data at stake⁸⁵.

With regard to the second goal (i.e., rebalancing their bargaining power vis-à-vis large players), **the DA pursues contractual fairness by introducing limits to the freedom of contract to protect SMEs** against the exploitation of contractual imbalances when negotiating access to and use of data. Indeed, according to the Commission, given their meaningful inability to negotiate the conditions for access to data, SMEs may have no other choice than to accept 'take-it-or-leave-it' contractual terms⁸⁶. Therefore, unfair terms unilaterally imposed on SMEs shall not be binding on them. A contractual term is considered unfair if it is of such a nature that its use grossly deviates from good commercial practice, contrary to good faith and fair dealing⁸⁷.

To provide a yardstick to interpret such unfairness test for B2B relationships⁸⁸, Article 13 includes a list of terms that are always considered unfair and a list of terms that are presumed to be unfair. If a contractual term is not included in these lists, the general unfairness provision applies. Model contractual terms recommended by the Commission may assist commercial parties in concluding contracts based on fair terms.

Given the relevance of the principle of freedom of contract, it is appropriate to sound a note of caution against excessive limitations that may lead to straight jacket effects in B2B relationships. As acknowledged in Recital 54, the vast majority of contractual terms that are commercially more favourable to one party than to the other are a normal expression of the principle of contractual freedom and shall continue to apply. However, by revolving around vague and broad concepts such as gross deviation from good commercial practices or contrary to good faith and fair dealing, the unfairness test may generate uncertainty which could be heightened by potential different interpretations at a national level. Moreover, **contractual fairness in B2B negotiations is already tackled by provisions on the abuse of economic dependence which have been adopted over the years in several Member States** (i.e., Austria, Belgium, Bulgaria, Czech Republic, Cyprus, France, Germany, Greece, Italy, Portugal, and Spain) to scrutinise the unfairness of terms and conditions due to the imbalance of bargaining power between business parties. Some Member States have recently introduced (i.e., Belgium) or updated (i.e., Germany and Italy) such provisions to address the emergence of large digital platforms.

The new German and Italian rules are particularly relevant for our analysis. Indeed, according to the German rule, such dependency may also arise from the fact that an enterprise is dependent for its own activities on access to data controlled by another enterprise⁸⁹. In a similar vein, the Italian Annual

⁸⁵ Kerber, *supra* note 68, 18.

⁸⁶ *Ibid.*, Recital 51.

⁸⁷ *Ibid.*, Article 13(2).

⁸⁸ *Ibid.*, Recital 55.

⁸⁹ GWB Digitalization Act (2021), Section 20.



Competition Law Bill included a specific provision aimed at introducing a (rebuttable) presumption of economic dependence when an undertaking uses intermediation services provided by a digital platform that plays a key role in reaching end users or suppliers, also thanks to network effects or availability of data⁹⁰.

The rationale of protecting weaker parties against the risk of abuse of their economic dependence has also supported sector-specific legislations, such as the European Directive on agricultural and food supply chain⁹¹ and national interventions (i.e., Austria, Belgium, France, Italy, and Portugal) banning the adoption of parity clauses to end the imbalance between hotels and online travel agencies (OTAs).

Some terms considered unfair by the DA are clearly inspired by the abuse of economic dependence. In particular, pursuant to Article 13(4)(e), a contractual term is presumed unfair if its object or effect is to enable the party that unilaterally imposed the term to terminate the contract with unreasonably short notice, taking into consideration the reasonable possibilities of the other contracting party to switch to an alternative and comparable service and the financial detriment caused by such termination. Given that economic dependence is mainly the result of significant switching costs that may lock a party into a business relationship, not allowing it to find equivalent alternative solutions, a classic situation where economic dependence is deemed to emerge regards the threat of terminating the business relationship, which may induce the weak party to accept unfair amendments to the agreement.

In addition, given the suggested parallel between data dependence and economic dependence, the exclusion of SMEs from the scope of application of Article 13 is not justified. Indeed, the abuse of economic dependence scrutinises the unfairness of terms and conditions due to the imbalance of bargaining power between business parties, regardless of the size of the players involved. Moreover, in the case of data-sharing contracts, such imbalance would be generated by a data dependence, which may emerge also when SMEs exert control over some data.

ASSESSMENT

The already mentioned concerns about **the risk of inconsistency generated by the attempt to commingle different policy goals** also emerge with regards to the provisions introducing an asymmetric regulation according to the size of players involved.

In general, given the experience of the PSD2 and the upcoming entry into force of the DMA, the assessment of benefits and drawbacks of any **asymmetric regulation requires further investigation**. Furthermore, the exemptions granted to SMEs may generate relevant implementation costs as the size of a company may quickly change, especially in fast-moving markets. Moreover, if the exemption of SMEs from several obligations reflects a proportionality principle, the exclusion of gatekeepers from the potential beneficiaries of the new right addresses

⁹⁰ Italian Government (2021), 'Annual Competition Law Bill', Article 29, https://www.ansa.it/documents/1636051142145_concorrenza.pdf.

⁹¹ Directive (EU) 2019/633 of the European Parliament and of the Council of 17 April 2019 on unfair trading practices in business-to-business relationships in the agricultural and food supply chain, [2019] OJ L 111/59.



the competitive goal to avoid further data accumulation. However, the lack of limitations for manufacturers and data holders to sell gatekeepers access to the data at stake appears at odds with such an objective.

Even more caution is needed with regards to the provision introducing limits to large companies' freedom of contract to protect SMEs against the exploitation of contractual imbalances when negotiating access to and use of data. Indeed, in terms of trade-off, if excessive limitations may lead to straight jacket effects in B2B relationships, the imbalance of bargaining power between weaker parties and large players is already handled by national provisions on the abuse of economic dependence. Furthermore, the unfairness of terms and conditions due to the imbalance of bargaining power between business parties is not related to the size of the players involved, hence the exclusion of SMEs from the scope of application of such provision appears not justified.

3.2. The Interface With Intellectual Property Rights

The exercise of the new data access and sharing right affects two main intellectual property rights (IPRs), namely trade secrets and the *sui generis* database protection.

About the latter, the **DA clarifies that databases containing data from IoT devices do not qualify for the *sui generis* right under the Database Directive**, which enables the database maker to prevent any extraction and re-utilisation of the database's contents where there has been a substantial investment in obtaining, verification or presentation of the contents, irrespective of eligibility of the database for protection by copyright⁹². The aim is to eliminate the risk that holders of data in databases obtained or generated using physical components of a connected product and a related service claim the *sui generis* right and in so doing secure their control over data hindering the effective exercise of the right of users to access and share data with third parties under the DA⁹³.

The role of *sui generis* protection in the data economy context has been questioned on several recent occasions. Indeed, the Database Directive has been conceived in a completely different economic and technical reality and includes provisions that now represent legal obstacles that might hinder data access and re-use, thus jeopardising the competitiveness of the European data industry⁹⁴. Accordingly, the Intellectual Property Action Plan suggested to revisit the Database Directive to facilitate the sharing of and trading in machine-generated data and data generated in the context of rolling out the IoT⁹⁵. Therefore, the Database Directive is among the legal instruments that was expected to be revised in light of the DA⁹⁶.

⁹² See Data Act proposal, *supra* note 1, Article 35.

⁹³ *Ibid.*, Recital 84.

⁹⁴ European Commission, 'Making the most of the EU's innovative potential. An intellectual property action plan to support the EU's recovery and resilience' COM(2020) 760 final, 14. See also Commission Staff Working Document, 'Evaluation of Directive 96/9/EC on the legal protection of databases', SWD(2018) 146 final.

⁹⁵ Intellectual Property Action Plan, *supra* note 94.

⁹⁶ European Commission (2022), 'Study to support an impact assessment for the review of the Database Directive', <https://copenhageneconomics.com/wp-content/uploads/2022/02/study-to-support-an-impact-assessment-for-the-review-of-the-database-directive.pdf>.



The envisaged solution raises some doubts⁹⁷. Notably, **rather than clarifying what is not protected under the Database Directive, the goal of excluding machine-generated data from the scope of *sui generis* right likely requires amending that Directive**. Indeed, the DA assumes that, in any scenario, databases containing data obtained from or generated by the use of a product or a related service cannot be protected under the Database Directive, hence it would be sufficient to “clarify” that the *sui generis* right does not apply to such databases as the requirements for protection would not be fulfilled⁹⁸. However, as pointed out by several IP scholars⁹⁹, as long as the database maker can prove the data collection as obtaining of data and the investment is substantial and separated from the irrelevant investments, the *sui generis* claim may meet the legal test elaborated by the Court of Justice case law¹⁰⁰.

Promoting data access and sharing also requires the “clarification” of certain provisions of the Trade Secrets Directive¹⁰¹. Some data can, indeed, be protected by trade secrets, hence a duty to disclose them would affect the protection because it would destroy secrecy. While it is considered important to respect trade secrets in handling data to preserve incentives to invest¹⁰², at the same time the vagueness of trade secrets requirements may incentivise data holders to claim protection just to refuse to obey their data access and sharing obligations.

To strike a balance between the interests at stake, the DA relies on the confidentiality requirement stating that trade secrets shall only be disclosed to the user provided that all specific necessary measures are taken to preserve the confidentiality of trade secrets, in particular with respect to third parties¹⁰³. Furthermore, in case of data sharing with third parties, trade secrets shall only be disclosed to the extent that they are strictly necessary to fulfil the purpose agreed between the user and the third party and all specific necessary measures agreed between the data holder and the third party are taken by the third party to preserve the confidentiality of the trade secret¹⁰⁴. However, Article 4(3) and Article 5(8) are at odds with the provision included in Article 8(6), which instead, regardless of any confidentiality requirement, establishes that an obligation to make data available to a data recipient shall not oblige the disclosure of trade secrets within the meaning of the Trade Secrets Directive, hence opening the door to potential opportunistic behaviour by data holders.

⁹⁷ See European Copyright Society (2022), ‘Opinion on selected aspects of the proposed Data Act’, <https://europeancopyrightsocietydotorg.files.wordpress.com/2022/05/opinion-of-the-ecs-on-selected-aspects-of-the-data-act-1.pdf>.

⁹⁸ Data Act proposal, supra note 1, Recital 84.

⁹⁹ European Copyright Society, supra note 97, 3.

¹⁰⁰ See CJEU, Case C-444/02, *Fixtures Marketing Ltd v. Organismos Prognostikon Agnon Podosfairou*; Case C-338/02, *Fixtures Marketing Ltd v AB Svenska Spel*; Case C-46/02, *Fixtures Marketing Ltd v Oy Veikkaus AB*; and Case C-203/02, *The British Horseracing Board Ltd v. William Hill Organisation Ltd*.

¹⁰¹ Directive (EU) 2016/943 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure [2016] OJ L 157/1. See Inception Impact Assessment, supra note 43, 1 and 3; and Intellectual Property Action Plan, supra note 94, 13-14.

¹⁰² Data Act proposal, supra note 1, Recital 28.

¹⁰³ *Ibid.*, Article 4(3).

¹⁰⁴ *Ibid.*, Article 5(8).



ASSESSMENT

The DA correctly acknowledges the need to address the interface between IPRs protection and the envisaged new data access and sharing right. However, the proposed solutions do not appear to properly achieve such results.

Notably, while the aim of avoiding the risk that the database sui generis right may be strategically used to undermine the effectiveness of the DA is commended, **the exclusion of machine-generated data from the scope of sui generis right would likely require amending the Database Directive**. With regards to trade secrets, the approach of relying on the confidentiality requirement to strike a balance between the interests at stake is convincing. Nonetheless, the **coherence among some internal provisions** should be better ensured.



4. BUSINESS-TO-GOVERNMENT DATA SHARING

As the Open Data Directive has introduced an obligation for public bodies to publish data to stimulate innovation for products and services by encouraging the wide availability and re-use of public sector information for private or commercial purposes, the DA requires private actors to contribute to this logic of openness by making available their data to public bodies for the implementation of public tasks in specific circumstances. Notably, the objective of Chapter V of the DA is to **favour B2G data sharing** by allowing public sector bodies or European institutions, agencies or bodies to use data held by an enterprise to respond to public emergencies or in other exceptional cases¹⁰⁵. The rationale is that in such exceptional cases the public interest outweighs the interests of the data holders, hence the latter should be placed under an obligation to make the data available to public sector bodies upon their request¹⁰⁶.

As previously mentioned (see *supra* Section 3), this obligation does not apply to micro and small enterprises.

The DA frames **three circumstances under which an exceptional need arises so that public bodies may request data access**¹⁰⁷: (a) response to a public emergency; (b) prevention of or recovery from a public emergency; (c) fulfilment of a specific task in the public interest explicitly provided by law. The distinction is also relevant for the compensation. Indeed, while data made available under hypothesis (a) will be provided free of charge¹⁰⁸, in the hypothesis (b) and (c) data holders will be entitled to a reasonable compensation which should not exceed the technical and organisational costs incurred in complying with the request and the reasonable margin required for making the data available to the public sector body¹⁰⁹.

However, although at first glance the hypotheses (a) and (b) appear defined, **their scope may still be controversial** (Recital 57 mentions as examples public health emergencies, emergencies resulting from environmental degradation and major natural disasters, as well as human-induced major disasters, such as major cybersecurity incidents; however, the list is not exhaustive), **as well as it is unclear for how long the obligation will apply**. The third group of cases appears even more broad and vague, making it difficult to predict what other circumstances may activate the obligation at stake. In addition, hypothesis (c) allows access even if public sector bodies may obtain the data by other means under the mere condition that obtaining such data would substantially reduce the administrative burden for data holders or other enterprises.

¹⁰⁵ Ibid., Article 14.

¹⁰⁶ Ibid., Recital 57.

¹⁰⁷ Ibid., Article 15.

¹⁰⁸ Ibid., Recital 67, arguing that public emergencies are rare events, therefore the business activities of the data holders are not likely to be negatively affected as a consequence of the public sector bodies having recourse to this provision.

¹⁰⁹ Ibid., Article 20.



ASSESSMENT

The rationale of the provision aimed at promoting B2G data sharing in response to public emergencies cannot be questioned. However, the circumstances under which an exceptional need arises so that public bodies may request data access would require a more clear and narrow definition.

These hypotheses require clarification and should be narrowly specified given that such data sharing may involve personal data and commercially sensitive data, hence its sharing may have significant implications in terms of intellectual property and privacy, as confirmed by the deep concerns raised by the European Data Protection Board and the European Data Protection Supervisor¹¹⁰.

¹¹⁰ European Data Protection Board and European Data Protection Supervisor, *supra* note 60.



5. DATA PROCESSING SERVICES SWITCHING AND INTERNATIONAL DATA ACCESS

The vendor lock-in problem has been at the top of the European policy agenda in the last few years. The Free Flow of Non-Personal Data Regulation explicitly refers to a lack of competition between cloud service providers in the EU and various vendor lock-in issues¹¹¹. According to the study carried out for the European Commission, such concerns are shared by approximately 25% of companies surveyed and data portability between different cloud providers is not considered a problem for large companies¹¹². Nonetheless, the DA finds that the self-regulatory approach promoted by such Regulation has been largely ineffective so far¹¹³.

As a consequence, the DA opts for introducing legally **binding and detailed obligations to facilitate switching between data processing services**, which include all conditions and actions that are necessary for a customer to terminate a contractual agreement of a data processing service, to conclude one or multiple new contracts with different providers of data processing services, to port all its digital assets to the concerned other providers and to continue to use them in the new environment **while benefitting from functional equivalence**¹¹⁴. Functional equivalence is defined as the maintenance of a minimum level of functionality of a service after switching, to such an extent that the destination service will deliver the same output at the same performance and with the same level of security, operational resilience and quality of service as the originating service at the time of termination of the contract, and which should be deemed technically feasible whenever both the originating and the destination data processing services cover the same service type¹¹⁵.

The DA provisions seem to complement the DMA as an additional regulatory intervention that will affect cloud providers. Indeed, according to the Impact Assessment, the DA rules would be “lighter, albeit wider in scope”, than the direct portability obligation of the DMA to cloud providers designated as gatekeepers¹¹⁶. However, it is worth noting that, unlike the DA, the DMA does not limit the freedom of contract of gatekeepers¹¹⁷.

The notion of **data processing service is defined broadly** as covering services that allow on-demand and broad remote access to a scalable and elastic pool of shareable and distributed computing resources, therefore including all the models of cloud services, i.e. infrastructure as a service (IaaS) and software as a service (SaaS) and platform as a service (PaaS)¹¹⁸. Moreover, no exception is granted to SMEs. However, to facilitate effective cloud interoperability at the SaaS and PaaS levels, providers of such data processing services are required to make open interfaces publicly available and ensure

¹¹¹ Free Flow of Non-Personal Data Regulation, *supra* note 7, Recital 6.

¹¹² IDC and Arthur’s Legal (2018), ‘Switching of Cloud Services Providers’, Executive Summary and para. 2.5, <https://op.europa.eu/en/publication-detail/-/publication/799e50ff-6480-11e8-ab9c-01aa75ed71a1/language-en/format-PDF/source-search>.

¹¹³ Data Act proposal, *supra* note 1, Recital 70.

¹¹⁴ *Ibid.*, Article 23 and Recital 72.

¹¹⁵ *Ibid.*, Article 2(14) and Recital 72.

¹¹⁶ Impact Assessment, *supra* note 2, 35.

¹¹⁷ Max Planck Institute for Innovation and Competition, *supra* note 54, 64.

¹¹⁸ *Ibid.*, Recital 71.



compatibility with open interoperability specifications or European standards for interoperability¹¹⁹. To this aim, the Commission can mandate the use of European standards for interoperability or open interoperability specifications for specific service types¹²⁰.

It is not immediately obvious why IaaS are excluded from the technical duties about open interfaces and interoperability specifications¹²¹. However, the exclusion is consistent with the Impact Assessment findings that in PaaS and SaaS cloud markets interoperability problems are gravest and hyperscalers have a smaller share of the market¹²².

Furthermore, **the implementation of the principle of ensuring the functional equivalence within the same service type as defined in the proposal, next to difficulties establishing what the type of the same services constitutes, will likely generate controversies regarding potential technical obstacles and security issues.** In addition, **it is not clear how the functional equivalence will deal with innovation**, namely to what extent a cloud provider offering an innovative feature could be responsible to ensure the functional equivalence to the user that decides to switch to another cloud provider. As a result, this could lead to a race to the bottom as all providers would be required to deliver similar services. Finally, **a definition of 'open interface' is missing.**

Providers of data processing services are also required to **take all reasonable technical, legal and organisational measures to prevent international transfer or governmental access to non-personal data held in the EU where such transfer or access would create a conflict with EU law or the national law of the relevant Member State**¹²³. Moreover, a foreign judgment or administrative decision requiring a provider of a data processing service to transfer or give access to non-personal data held in the EU will be recognised and enforced based on an international agreement¹²⁴. Finally, in the absence of such an international agreement and where the compliance with the foreign decision would risk putting the service provider in conflict with EU law (or the national law of the relevant Member State), the transfer or the access to data will be allowed only under some cumulative requirements¹²⁵.

Such provision mirrors the approach undertaken in the Data Governance Act aiming to transpose it in the DA since the former does not directly apply to cloud and edge services, even if the two legislative initiatives pursue different goals and the former has a much more limited scope¹²⁶.

Moreover, the first situation addressed by Article 27 poses relevant concerns since, as a practical consequence, **it could result in data localisation in the EU.** Indeed, by requiring data processing services providers to act as enforcers to take all reasonable technical, legal and organisational

¹¹⁹ Ibid., Article 26(2) and (3).

¹²⁰ Ibid., Article 29(5) and Recital 79.

¹²¹ See also Max Planck Institute for Innovation and Competition, supra note 54, 66.

¹²² Impact Assessment, supra note 2, 5. See also Data Act proposal, supra note 1, Recital 76, arguing that market-driven processes have not demonstrated the capacity to establish technical specifications or standards that facilitate effective cloud interoperability at the PaaS and SaaS levels.

¹²³ Data Act proposal, supra note 1, Article 27(1).

¹²⁴ Ibid., Article 27(2).

¹²⁵ Ibid., Article 27(3).

¹²⁶ Impact Assessment, supra note 2, 35.



measures to prevent international transfer or government access where such transfer or access would create a conflict with EU law (or the national law of the relevant Member State), Article 27(1) may *de facto* induce such providers to completely refrain from transferring data to countries outside the EU and granting access to data from such countries¹²⁷. Moreover, data localisation would increase compliance costs (including those related to legal uncertainty) for EU players, thus potentially diverting resources from investments in research and innovation.

ASSESSMENT

The envisaged obligations to facilitate switching between data processing services are justified by the lack of effectiveness of the self-regulatory approach promoted by the Free Flow of Non-Personal Data Regulation. However, given that such Regulation has been enacted only four years ago, **the speed at which new provisions are introduced may appear at odds with the timeframe needed to assess the impact of the previous initiative.**

In addition, the implementation of the principle of ensuring that customers maintain **functional equivalence** of the service after they have switched to another service provider may produce litigations regarding technical obstacles, security issues, and innovative features.

Further **doubts are raised by the provision addressing unlawful third-party access to non-personal data held in the EU by data processing services offered on the EU market.** Notably, by requiring data processing services providers to take all reasonable technical, legal and organisational measures to prevent international transfer or governmental access where such transfer/access would create a conflict with Union law or the national law of the relevant Member State, the DA risks to favour data localisation in the EU and therefore should be deleted.

¹²⁷ Max Planck Institute for Innovation and Competition, *supra* note 54, 72-73.



6. INTEROPERABILITY

Besides the interoperability for data processing services, the DA proposal signals a fully-fledged recognition of the key role played by interoperability and standardisation¹²⁸. However, **rather than introducing general interoperability obligations, the DA imposes interoperability requirements only on operators of data spaces.**

Notably, in order to facilitate interoperability, operators of data spaces shall ensure that¹²⁹:

- a) dataset content, use restrictions, licenses, data collection methodology, data quality and uncertainty are sufficiently described;
- b) data structures and formats, vocabularies, classification schemes, taxonomies and code lists are described in a publicly available and consistent manner;
- c) APIs and other technical means to access the data, as well as their terms of use, are sufficiently described;
- d) the means to enable the interoperability of smart contracts are provided.

To facilitate conformity with such requirements, a presumption is provided for interoperability solutions that meet **harmonised standards** and the Commission is allowed to request European standardisation organisations to draft harmonised standards¹³⁰. Finally, the Commission should adopt common specifications where harmonised standards do not exist or where they are insufficient to enhance interoperability for common EU data spaces, APIs, cloud switching, and smart contracts¹³¹.

Because of the relevance of the obligations at stake, **a clear definition of operators of data spaces is needed**, while the proposal does not provide it at all. As mentioned, interoperability under Chapter VIII apparently does not refer to the new data access and sharing right for IoT products and related services envisaged in Chapter II. However, **the exclusion of the new IoT data right may undermine the effectiveness of the initiative**¹³². After all, as argued by the same Commission in its recent IoT sector inquiry, interoperability is essential for the full deployment of functionalities that a consumer IoT ecosystem can offer to users¹³³. Further, the majority of participants in the sector inquiry expressed the need to prioritise standardisation to guarantee higher levels of interoperability¹³⁴.

Moreover, given the interoperability provisions imposed by the DMA on app stores and number-independent interpersonal communication services, the DA proposal should have also tackled the issue of the type of interoperability that is considered desirable and workable for IoT environments. Indeed, with regard to the decision to mandate horizontal interoperability for number-independent

¹²⁸ Data Act proposal, *supra* note 1, Recital 79.

¹²⁹ *Ibid.*, Article 28(1).

¹³⁰ *Ibid.*, Article 28(3-4).

¹³¹ *Ibid.*, Article 28(5) and Recital 79.

¹³² Kerber, *supra* note 68, 13.

¹³³ European Commission, *supra* note 22, para. 17.

¹³⁴ Commission Staff Working Document, *supra* note 23, 71.



interpersonal communication services offered by gatekeepers under the DMA, concerns have been raised about the unintended consequences of such measure in digital markets not only because of technical issues, but also because of the risk of enshrining existing incumbency and hindering innovation and service differentiation¹³⁵.

ASSESSMENT

The DA is in line with other recent and ongoing European legislative initiatives which assign interoperability a key role in promoting effective and smooth data sharing. However, to assess the effectiveness of the intervention, it is worth noting that the **DA provisions on interoperability do not apply to the new IoT data access and sharing right**, but only regard operators of data spaces and providers of data processing services.

¹³⁵ See Marc Borreau, Jan Krämer, and Miriam Buiten (2022), 'Interoperability in Digital Markets', CERRE Report, <https://cerre.eu/publications/interoperability-in-digital-markets>; European Commission (2022), 'Non-paper from the Commission services on interoperability for messenger services and online social networks in the DMA', <https://www.iccl.ie/wp-content/uploads/2022/03/wk03135.en22.pdf>; Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen (2021), 'Interoperability between messaging services – an overview of potential and challenges', https://www.bundesnetzagentur.de/SharedDocs/Pressemitteilungen/EN/2021/20211209_Messenger.html.



7. IMPLEMENTATION AND ENFORCEMENT

Pursuant to Article 31, Member States shall designate one or more competent authorities as responsible for the application and enforcement of the DA¹³⁶. Furthermore, the authorities responsible for the supervision of compliance with data protection and competent authorities designated under sectoral legislation should have the responsibility for the application of the DA in their areas of competence¹³⁷. Therefore, in contrast with the policy choice adopted in the DMA and partially in the Digital Services Act¹³⁸, but in line with the Data Governance Act¹³⁹ and the Artificial Intelligence Act¹⁴⁰, the proposal opts for a fully decentralised enforcement structure at the national level. Notably, rather than envisaging a one-stop-shop according to a centralised model or a decentralised model based on the country of origin, **the DA adopts a decentralised model based on the countries of destination**¹⁴¹.

However, **the interplay with data protection and antitrust issues as well as the coordination with other recent regulatory initiatives (in particular, the Data Governance Act) represent a delicate task to be handled for the governance architecture of the DA.**

The envisaged solution raises two concerns. The first is related to the possibility that the Member States designate different competent authorities. Although, in the case that the Member State is required to designate a coordinating competent authority¹⁴², the risk of confusion is apparent. The second concern regards the possibility that Member States put different authorities in charge of the DA and the Data Governance Act. The lack of coordination may undermine the harmonised implementation of the rules.

¹³⁶ Data Act proposal, supra note 1, Article 31(1).

¹³⁷ Ibid., Article 31(2).

¹³⁸ See Council of the European Union (2022), 'Digital Services Act: Council and European Parliament provisional agreement for making the internet a safer space for European citizens', Press release <https://www.consilium.europa.eu/it/press/press-releases/2022/04/23/digital-services-act-council-and-european-parliament-reach-deal-on-a-safer-online-space/>, conferring on the Commission the exclusive power to supervise very large online platforms and search engines. The text of the provisional agreement is available at https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/IMCO/DV/2022/06-15/DSA_2020_0361COD_EN.pdf.

¹³⁹ Data Governance Act, supra note 3, Articles 13 and 23.

¹⁴⁰ European Commission, 'Proposal for a Regulation laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)', COM(2021) 206 final, Article 30.

¹⁴¹ For an analysis of pros and cons of different institutional design models for the enforcement of EU platform laws, see Giorgio Monti and Alexandre de Streel (2022), 'Improving EU Institutional Design to Better Supervise Digital Platforms', CERRE Report <https://cerre.eu/publications/improving-eu-institutional-design/>.

¹⁴² Data Act proposal, supra note 1, Article 31(4).



ASSESSMENT

Given the interplay between the DA and data protection and antitrust issues as well as its coordination with other recent regulatory initiatives, **the adoption of a decentralised model based on the countries of destination** (according to which Member States may designate even more than one authority as responsible for the application and enforcement of the DA) **raises relevant concerns in terms of coordination** between authorities and harmonised implementation of the new rules.



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

Jan Krämer



TABLE OF CONTENTS

1. INTRODUCTION	36
2. THE ARCHITECTURE OF THE DATA SHARING OBLIGATIONS UNDER THE PROPOSED DATA ACT	38
2.1 Right to Real-Time Data Portability for Generated Data.....	38
2.2 Contractual Agreement Between User and Data Holder	39
2.3 Restrictions to the User's Data Portability Right (Free Flow of Data)	41
2.3.1 Restrictions on the type of connected products.....	42
2.3.2 Restrictions on the scope of data that can be accessed	43
2.3.3 Restrictions on the type of firms which have to make data available	44
2.3.4 Restrictions on the use of accessed data.....	44
2.3.5 Restrictions on the recipients of accessed data	45
2.3.6 Restrictions for authorised third parties seeking to access data	45
3. EFFECTIVENESS OF THE DATA ACT WITH RESPECT TO ACHIEVING ITS GOALS	49
3.1 Competition and Innovation in Aftermarkets	49
3.2 Enabling Innovation and Investment in new Products and Services	50
3.3 Enabling Free Flow of Data through Data Brokers and Data Markets	51
4. RECOMMENDATIONS	53
Recommendation 1: Balance innovation incentives between data providers and data seekers through limiting scope of data access to raw data generated by product use	53
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.	54
Recommendation 3: Introduce a rebuttable presumption that access to raw data does not impede trade secrets. Remove Article 8(6) which suggests otherwise.	55
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.	55
Recommendation 5: Remove most product exclusions. Exclude only those products that provide general connectivity and computing resources, which are fully configurable by the user.	56
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.....	56
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.	57



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 leave 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"**.¹⁴³ 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"**.¹⁴⁴ 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."¹⁴⁵ 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 DA¹⁴⁶ emphasizes that a main goal of the DA is **to promote competition and innovation in aftermarkets** of connected products.¹⁴⁷ 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**.¹⁴⁸ 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

¹⁴³ 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

¹⁴⁴ Data Act proposal, supra note 1, Explanatory Memorandum, 3

¹⁴⁵ Data Act proposal, supra note 1, Explanatory Memorandum, 13

¹⁴⁶ 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

¹⁴⁷ Impact Assessment, supra note 4, 1

¹⁴⁸ Impact Assessment, supra note 4, 10



problems arise due to lack of 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.¹⁴⁹ 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.¹⁵⁰ 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.**¹⁵¹

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.

¹⁴⁹ Data Act, supra note 1, Explanatory Memorandum, 5

¹⁵⁰ 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

¹⁵¹ 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).¹⁵² 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.¹⁵³ 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**.

¹⁵² 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.”

¹⁵³ 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.¹⁵⁴

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 holder¹⁵⁵ 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

¹⁵⁴ 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

¹⁵⁵ 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 positioning. 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 economically aligned) entities.



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 Raspberry 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.¹⁵⁶ 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

¹⁵⁶ 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 Secret Directive, nor with IP law (Recital 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,¹⁵⁷ 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).¹⁵⁸ Such an exception based on size is generally laudable, as otherwise small firms are disproportionately 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 view¹⁵⁹, 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 aftermarket, 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 protection of the data

¹⁵⁷ 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>

¹⁵⁸ In Section 4 we recommend to exclude also medium-sized enterprises from having to provide access.

¹⁵⁹ 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 incentives 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-generated data). Yet, the main goal of the DA is precisely to stimulate data-driven innovation by third parties.

2.3.5 Restrictions on the recipients 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, Martens¹⁶⁰ points to the case of in-car operating systems (OS), such as Apple’s CarPlay 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.

¹⁶⁰ 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 cover the 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.¹⁶¹ 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

¹⁶¹ For more on rate-of-return regulation and low powered incentive regulation, see, e.g., Jean Jacques Laffont and Jean Tirole (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.¹⁶² 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.¹⁶³

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.¹⁶⁴ 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**.¹⁶⁵

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”.

¹⁶² 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>

¹⁶³ For a legal discussion on this see Metzger and Schweitzer, supra note 13.

¹⁶⁴ 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)).

¹⁶⁵ For a similar conclusion 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.¹⁶⁶ 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.

¹⁶⁶ 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"¹⁶⁷ 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 maintenance 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

¹⁶⁷ 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.¹⁶⁸ 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.¹⁶⁹ 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.¹⁷⁰

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

¹⁶⁸ 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.

¹⁶⁹ 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>

¹⁷⁰ 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 achieved 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 originate 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 9.¹⁷¹ 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.

¹⁷¹ 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,¹⁷² 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 automatically transcribed text of the voice commands, then only the sound files would need to be provided. If the raw sound files are not accessible, 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 meaning), 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 emphasized 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

¹⁷² For example, it has been proposed to move away from a consent-based architecture 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 data 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 rebuttable 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 scholars¹⁷³ 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.

¹⁷³ See Drexel 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 particularly 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.



ACCESS TO PRIVATE SECTOR DATA FOR THE COMMON GOOD

Heiko Richter



TABLE OF CONTENTS

1. BACKGROUND AND KEY POINTS.....	60
2. CRITICAL REVIEW OF CHAPTER	62
2.1 Scope, Preemption, and Subsidiarity	62
2.1.1 The ‘exceptional need to use data’ (Article 15)	62
2.1.2 Subsidiarity and pre-emption (Article 16).....	64
2.1.3 Possible avenues for legislation	66
2.1.4 The relationship with voluntary data sharing agreements	67
2.2 Request for Data to be Made Available and Compliance (Article 17 and 18)	68
2.3 Purpose Limitation and Re-use (Article 17 and 19)	69
2.4 Use for Research and Statistical Purpose (Article 21)	70
2.5 Compensation (Article 20)	71
2.6 Interface with Private Rights and Interests	72
2.6.1 Personal data	72
2.6.2 Intellectual property	73
2.6.3 Contractual restrictions with third parties.....	73
3. POLICY RECOMMENDATIONS	74



1. BACKGROUND AND KEY POINTS

In its Proposal for a Regulation on harmonised rules on fair access to and use of data (**Data Act**),¹⁷⁴ the Commission, in Chapter V, proposed mandatory rules on making data available to public sector bodies (PSBs) and Union institutions, agencies or bodies based on exceptional need. Chapter V aims to provide data held by private enterprises to PSBs in situations where there is an exceptional data need (such as emergencies).¹⁷⁵

Looking at the **evolution** of the provisions, it has been a long way from first considerations to the much-discussed legislative proposal of the Commission. The idea of systematically allowing public sector bodies to access privately held data for enabling or improving the fulfillment of the public task originally stems from public-private cooperations in developing countries where the state was lacking the capability to collect and provide the needed data. In 2016, the French ‘Loi Lemaire’¹⁷⁶ introduced some specific provisions on ‘B2G data sharing’, which inspired the European Commission to follow suit.¹⁷⁷ The drafting of Chapter V of the Data Act was also considerably influenced by a high-level expert group report¹⁷⁸ that was published in January 2020.

The **underlying idea** of ‘B2G data sharing’ is that private companies have large stocks of data which can be used for the common good. The technical developments and the liberalisation of sectors in the last three decades have led to a noticeable shift of data power – the state is no longer the largest collector and processor of data, private companies are.¹⁷⁹ Therefore, public sector bodies could benefit from this privately held data if they can access and use it for specific public purposes.

However, empowering the state to access privately held data comes with **risks and reservations**, which highly politicises this issue. First, the Snowden revelations have called into question the trust in the state’s integrity regarding the use of privately held data.¹⁸⁰ While certainly much good can be done with the data, there is a permanent risk of abuse of state power, which leads to a general caveat: empowering the state to access privately held data is subject to the condition that the interests of data holders and data subjects are sufficiently safeguarded, and that abuse is effectively prevented. Second, from an economic perspective, Chapter V raises fundamental questions on the incentives to

This paper provides a significantly extended, refined and updated view, which the author has previously expressed in the Position Statement of the Max Planck Institute for Innovation and Competition of 25 May 2022 on the Commission’s Proposal of 23 February 2022 for a Regulation on harmonised rules on fair access to and use of data (Data Act).

¹⁷⁴ Proposal of the Commission of 23 February 2022 for a Regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act), COM(2022) 68 final. See also the accompanying Commission Staff Working Document – Impact Assessment Report, SWD(2022) 34 final.

¹⁷⁵ See COM(2022) 68 final, p. 3.

¹⁷⁶ See provisions on data of general interest (‘données d’intérêt général’) under arts 17-24 LOI n° 2016-1321 pour une République numérique of 7 October 2016.

¹⁷⁷ See also Alberto Alemanno, ‘Big Data for Good: Unlocking Privately-Held Data to the Benefit of the Many’ (2018) 9 European Journal of Risk Regulation 183, 187; for more specific academic discussions on the subject matter Teresa Scassa, ‘Sharing Data in the Platform Economy: A Public Interest Argument For Access to Platform Data’ (2017) 50 UBC Law Review 1017; Niva Elkin-Koren and Michal Gal, ‘The Chilling Effect of Governance-by-Data on Data Markets’ (2019) 86 University of Chicago Law Review 403.

¹⁷⁸ European Commission (ed), *Towards a European strategy on business-to-government data sharing for public interest: Final report prepared by the High-Level Expert Group on Business-to-Government Data Sharing* (EU 2020) 28.

¹⁷⁹ See Jennifer Shkabatur, ‘The Global Commons of Data’ (2019) 22 Stan. Tech. L. Rev. 354, 357.

¹⁸⁰ For the background see Heiko Richter, The law and policy of government access to private sector data (‘B2G data sharing’), in German Ministry of Justice and Consumer Protection and Max Planck Institute for Innovation and Competition (eds), *Data Access, Consumer Interests and Public Welfare* (Nomos: Baden-Baden 2021) 529, 531–534.



collect, process, store, and analyse data sets, and to what extent privately collected data can still be monetised and marketed if businesses are exposed to mandatory access by the state. Therefore, the provisions must also account for the incentives of businesses to create and collect data when delineating the limits and modalities of state access to private data.

Against this background, this paper **generally supports** the idea of stipulating duties for private businesses to share their data with the state for public purposes, **however, it should be treated with great caution**. In particular, the Commission's proposal needs additional thought, public discussion and improvement, which this report aims to foster. The report analyses the proposal and closes with policy recommendations suggesting that Chapter V of the proposed Data Act should more clearly delineate the scope of B2G data sharing, which in turn determines pre-emption of national legislation in this area, by strictly limiting it to situations of *ad hoc* data access. The report also addresses the effectiveness of the proposed procedure, which appears questionable, especially regarding public emergencies. Compensation should be limited to cost recovery which has to be specified in detail with regard to its components (see 2.5). Moreover, the proposal falls short of integrating the existing legal regimes for public sector information (Data Governance Act¹⁸¹ and OD PSI Directive¹⁸²) and coherently accounting for private rights and interests.

The addressed issues (scope, subsidiarity, compensation, re-use, request and dispute settlement procedure, and the interface with private rights) are considerably interconnected. Therefore, this report takes a holistic view, considering each of them as **different levers to appropriately balance the involved interests**, while providing a legal framework that can effectively reach the regulatory goal.

¹⁸¹Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724, [2022] OJ L 152/1 (Data Governance Act – DGA).

¹⁸²Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information, [2019] OJ L 172/56 (OD PSI Directive).



2. CRITICAL REVIEW OF CHAPTER V

2.1 Scope, Preemption, and Subsidiarity

2.1.1 The 'exceptional need to use data' (Article 15)

The Data Act introduces a **horizontal legal framework**, given that the reference point for providing access is not related to specific data or sectoral purposes, but to the *circumstances* under which PSBs should be entitled to request data from private data holders. Within this horizontal legal framework, there is ample room for further improvement and specification.

The legal basis in the context of **public emergency according to Article 15(a) and (b)**¹⁸³ appears straightforward.¹⁸⁴ However, there is no clear justification for Article 14(2) to exclude small and micro enterprises from the scope of the Regulation. Public interest must prevail in case of an exceptional need for data in cases of public emergency according to Article 15(a). Therefore, **the exclusion of micro and small enterprises according to Article 14(2) should be eliminated with regard to cases covered by Article 15(a)**. In case the existence of such entities is endangered by the request (Recital 56), a more differentiated compensation mechanism can be introduced to mitigate negative effects on such enterprise (see below 2.5).

In contrast, **Article 15(c) is ambiguous and needs further consideration**. This article provides a general legal basis for data access requests beyond public emergencies and follows a different reasoning than the one presented above. Article 15(c) is equally based on the idea of the 'exceptional need to use data',¹⁸⁵ rendering the interpretation of this notion decisive for the application of Chapter V.¹⁸⁶ However, Article 15(c) is not related to emergencies, but requires that the lack of available data prevents the PSB from fulfilling its tasks.¹⁸⁷ It remains unclear how strictly this criterion is to be understood, not least because Recital 58 speaks of '[preventing] it from *effectively* fulfilling a specific task'.¹⁸⁸ Thus, it is unclear whether it should be necessary that the data access enables the PSB to fulfil the public task, or it should be sufficient that the data access would simply improve the effectiveness of fulfilling the public task (which arguably is also true for minor increases). Indeed, the word 'prevents' in Article 15(c) should be interpreted strictly. Otherwise, the provisions of Chapter V could hinder future data access legislation that would systematically improve the effectiveness of fulfilling the public task, especially when considering potential pre-emption of national legislation. This view is supported by the Impact Assessment Report, which regards the fact that the need for data cannot be easily foreseen in advance and that the use of the data is a necessary condition for a PSB to fulfil its statutory task as characteristic of the exceptional data need.¹⁸⁹ Therefore, the additional requirements of Article 15(c)(1) and (2) must be interpreted in this light. To eliminate doubts, **the EU legislature should delete the word 'effectively' from Recital 58, while 'prevent' should be understood as**

¹⁸³ All Articles and Recital refer – if not indicated otherwise – to the Data Act Proposal.

¹⁸⁴ See also Art 2(10) as well as the definition mentioned in SWD(2022) 34 final, p 158.

¹⁸⁵ See also SWD(2022) 34 final, p 158.

¹⁸⁶ Ibid.

¹⁸⁷ See also SWD(2022) 34 final, p 34.

¹⁸⁸ Emphasis added.

¹⁸⁹ See SWD(2022) 34 final, p 13.



significantly increasing the effectiveness of fulfilling the specific task, considering the ad hoc nature of the data request.

Article 15(c)(1) also requires that the PSB be **unable to obtain such data by alternative means**.¹⁹⁰ From an economic perspective this principle is important because it can incentivise businesses to make data available beforehand and systematically. According to this subsidiarity principle, mandatory access is a means of last resort in non-emergency cases. Examples for such non-emergency cases are manifold, such as access to insurance or vehicle data to enhance planning of the local mobility infrastructure, access to data of accommodation booking platforms to advance urban housing planning, or access to consumption data of energy suppliers to advance policy concepts to foster the green transition. As a matter of principle, PSBs have to make an attempt to acquire the data by other means first. In practice, however, it remains unclear what efforts PSBs have to make. The general threshold appears high, but not too high, as the Impact Assessment Report states that ‘difficulties must be justified by objective reasons that make it impossible or very difficult to buy data on the market’.¹⁹¹ In this light, all alternative means of getting the data as listed in Article 15(c)(1) have to be considered.

‘Purchasing the data on the market at market rates’ implies that the data is actually offered to the public. At the same time, **the PSB should be required to have taken reasonable efforts to enquire into the market, and this should be clarified in Recital 58**. It should not, however, be required to individually negotiate with potential data providers if they have not offered the needed data before. If the data is available for purchase, then the question remains how to determine the ‘market rate’. Often a given dataset will constitute the only access point to the required information, which would mean the required data is single-source and therefore prone to monopoly pricing. To determine whether the price matches market rates, **Recital 58 should declare that average cost pricing (which can account for the fixed costs on top of the marginal costs) can be taken as the relevant benchmark**, as this comes closest to the competitive ‘as if’ price. ‘Relying on existing obligations to make data available’ implies that even if obligations to make the data available existed, access based on such obligations would come too late or prove inefficient. In that case, Article 15 provides a means to request *ad hoc* access.

In any case, Article 15(c)(1) requires that **‘the adoption of new legislative measures cannot ensure the timely availability of the data’**. This criterion is vague as it does not say anything about the perspectives of such legislation or whether legislative measures already have to be initiated. The criterion appears to be motivated by the Commission’s belief that much of B2G data sharing is not likely to be addressed to a sufficient degree by legislative means in the future.¹⁹² This logic, however, can lead to a deadlock: If Member States do not enact legislation, and if exactly this inactivity is a prerequisite for the legitimacy of requests under Article 15(c)(1), while at the same time Member States are pre-empted from implementing future legislation (see below 2.1.2), this insufficient status of the legal framework will be perpetuated. The legislature should prevent this deadlock and also

¹⁹⁰ See SWD(2022) 34 final, p 34.

¹⁹¹ See SWD(2022) 34 final, p 158.

¹⁹² See SWD(2022) 34 final, p 13.



consider the pre-emptive effect of Chapter V on national legislation when discussing solutions (see below 2.1.3).

Article 15(c)(2) sets out an alternative requirement to Article 15(c)(1), which is highly questionable. Essentially, Article 15(c)(2) would allow the PSB to request data access under Chapter V even if it could actually obtain the data by other means. The precondition is that obtaining the data according to Chapter V **‘would substantially reduce the administrative burden for data holders or other enterprises’**. This criterion, however, is conceptually flawed. The Impact Assessment Report explains that there is an exceptional need for data where ‘the different way of collecting the data would lead to substantial reduction of administrative burden for companies, replacing existing reporting obligations’.¹⁹³ However, this requirement contradicts Article 15(c), 1st sentence, according to which a lack of data prevents the PSB from fulfilling its public task. Article 15(c)(2) seems rather meant to increase the effectiveness of the means for fulfilling the public task and therefore comes close to reporting obligations (for instance, to statistical offices), which Chapter V should actually not affect according to Article 16(1). Moreover, the suggested request procedure (Articles 17, 18) is not suitable for it. Requests based on Article 15(c)(2) could at best be issued only once, if one takes the ‘exceptional need’ criterion seriously, while it cannot provide a legal basis for regular and permanent data access. This would run against the nature of *ad hoc* data access. **In sum, we recommend that the legislature delete Article 15(c)(2).**

2.1.2 Subsidiarity and pre-emption (Article 16)

A crucial question concerns the proposal’s understanding of **subsidiarity and the pre-emptive effect on national legislation**, specifically, to what extent Member States can impose legislation that would derogate from the provisions in Chapter V. At first glance, Article 15 extends the rights of PSBs vis-à-vis private data holders, so that the Proposal could be considered as being in their interest. However, depending on its pre-empting effect with regard to national legislation, the Proposal might also take away considerable legislative flexibility from the Member States in the future. This could run against the interests of the Member States in adopting sectoral regulation or even relaxing the requirements of Chapter V to safeguard the interests of businesses, for instance.

The **draft is ambiguous**: to be applicable, Article 15(c)(1) requires that ‘new legislative measures cannot ensure the timely availability of the data’. This means that the lack of national legislation is a requirement to trigger Article 15(c)(1). It indicates that national legislation (often sectoral) is actually wanted in this regard and held as legitimate. However, what contradicts this logic is the pre-emption clause found in Article 40, according to which Chapter V would derogate any national legislation in place that would allow for data access on exceptional basis (meaning that falls within the scope of Chapter V). In other words: if a Member State enacts national legislation that empowers data access on an exceptional basis, Article 40 would derogate such legislation and hold Chapter V generally applicable; but, at the same time, the condition of Article 15(c)(1) is not met, due to the existence of

¹⁹³ See SWD(2022) 34 final, p 34.



national legislation. To break up this contradictory relationship, delineating the scope of Chapter V is crucial but not self-evident – it requires a contextual and more systemic view.

To determine the scope of pre-emption, it is decisive to establish whether Chapter V **only regulates *ad hoc* data access** and not constellations of regular B2G data access.¹⁹⁴ The title of Article 15 supports this view: ‘exceptional need’ expresses that it is not about regular situations.¹⁹⁵ Chapter V also aims to reduce the duplication of similar requests to data holders, which is typical in *ad hoc* data access situations.¹⁹⁶ Moreover, the request mechanism under Articles 17 and 18 is designed as a one-off request mechanism and is not suitable for multiple requests that amount to a permanent and regular data transfer.

Regular means of obtaining data should therefore fall outside the scope of Chapter V. Such regular means are ‘existing reporting or compliance obligations in sectoral legislation that establish ongoing or recurring data exchange mechanism between public institutions and the private sector.’¹⁹⁷ Such regular access regimes are motivated by needs of non-exceptional nature, that is where the range of data holders is known and where data use can take place on a regular basis (Recital 59). Ultimately, this explains why the Regulation should be ‘without prejudice to Union and national legislation obliging companies to share data in other situations and for other purposes (such as reporting or monitoring regulatory compliance)’.¹⁹⁸ Article 16(1) reflects this and therefore confirms the *ad hoc* quality of the proposed Chapter V, which should not affect ‘reporting, complying with information requests, or demonstrating or verifying compliance with legal obligations’.¹⁹⁹ The exceptions of Article 16(2)²⁰⁰ also support this interpretation as they exempt requests for some *ad hoc* purposes. The Commission argues that, in these cases, obligations for private entities to provide data access to PSBs already exist or will exist.²⁰¹ So in the listed areas, there cannot be pre-emption by Chapter V, allowing Member States to remain free to regulate *ad hoc* data access (see also Article 1(4)). *E contrario*, Chapter V can serve as a legal basis for *all* other purposes when it comes to *ad hoc* access and it pre-empts Member States from imposing respective legislation.

As a consequence, Chapter V, as it stands, does not provide a legal basis for *regular* B2G data access, but only for data access on an *ad hoc* basis. Arguably, it can be challenging to draw the line between *ad hoc* and regular data access, such as when looking at the problem of repeated requests under Article 17 concerning the same data. If Chapter V enabled such requests, this would take away pressure from Member States to systematically enact desirable sectoral legislation for regular B2G data transfers. Accordingly, the envisaged pre-emption of national law would then reach too far and perpetuate the current, unsatisfactory legal situation. As pre-emption should not prevent sectoral rules for continuous access (such as in the mobility or housing sector), it must be limited to *ad hoc*

¹⁹⁴ This is explicitly stated in SWD(2022) 34 final, p 34.

¹⁹⁵ See also SWD(2022) 34 final, p 34.

¹⁹⁶ See SWD(2022) 34 final, p 19.

¹⁹⁷ See SWD(2022) 34 final, p 158.

¹⁹⁸ See SWD(2022) 34 final, p 34.

¹⁹⁹ See SWD(2022) 34 final, p 34.

²⁰⁰ See also Recital 60.

²⁰¹ See SWD(2022) 34 final, p 159.



access, which needs to be interpreted narrowly. One exception to *ad hoc* access in sectoral legislation concerns specific conditions on compensation, which the Member States are free to define, provided that they do not exceed the limits set by the Proposal (for instance, the free-of-charge provision).²⁰² However, as this is envisaging a limitation on pre-emption, the law should address this more explicitly.

2.1.3 Possible avenues for legislation

Against the background of the vague/inconsistent scope, the principle of subsidiarity and the effect or pre-emption, the EU legislature should consider the following options:

Option 1: Procedural solution

The restrained solution would be that Article 15 does not stipulate a legal basis (empowerment clause) itself for access to data, but that it requires another legal basis (stemming from Union or Member State laws) which mandate data access. The function of Chapter V would then be reduced to a EU-wide harmonisation (minimum standard) of the procedure. One could also think about a split: Article 15 could provide a legal empowerment for data access in emergency situations, while in all other cases, it would require another legal basis and harmonise the request procedure.

Option 2: Narrow/centralised empowerment solution

A narrow/centralised solution that would actually directly empower PSB to request access to data is that Article 15(c)(1) would only concern *ad hoc* access and stipulate a full derogation of national rules as already be done in Article 40. This appears only advisable, if ‘ad hoc access’ is clearly and narrowly defined. In that case, the legislature should delete the requirement of a lack of national legislative measures in Article 15(c)(1). In addition, Article 16(1) should add: ‘This Chapter only regulates *ad hoc* data access and ...’; while ‘ad hoc access’ should be properly defined in Article 2. To increase legal certainty, a presumption regarding the maximum duration and/or number/frequency of repeated similar requests should be included.

Option 3: Decentralised empowerment solution

A decentralised solution of empowerment would emphasise the principle of subsidiarity and incentivise Member States for more complementary legislation with regard to B2G data sharing. According to this solution, Chapter V would explicitly allow the Member States (meaning leave the competence to them) to regulate *ad hoc* access. But this would be made dependent on whether they implement legislation on continuous data access (meaning data access rules beyond *ad hoc* situations). Such a rule could actually incentivise/nudge Member States to enact more desired B2G data legislation on regular/continuous access. However, a more explicit definition of and distinction between *ad hoc* access and regular access must be included in the law as a prerequisite.

Option 4: Extended/hybrid solution

Finally, a hybrid solution could be implemented. According to this approach, Article 15(c)(1) would not be limited to cases of *ad hoc* access, but it would extend to systematic/continuous access. However, this would be limited to particular areas/purposes. To achieve legal certainty, this could be done by

²⁰² Ibid.



including additional empowerment of the Commission to enact delegated acts to designate areas (health, environmental protection, mobility planning, and so on) and harmonise procedures and conditions for access. These acts would have to relate to or modify the request rules of Article 17, 18 (which we would have to modify for this purpose as well), so that it would still be horizontal legislation. This proposal resembles the regulatory technique of the provision of High Value Datasets under Article 14 of the OD PSI Directive.

When comparing the options, option 3 and 4 would have a considerably larger impact on data sharing, as they would broaden the scope as compared to the Commission's proposal. However, they would also require the legislature to significantly strengthen the safeguards to protect the legitimate interests of businesses while at the same time, these solutions would need considerable conceptual re-thinking and refinement. On the other side of the spectrum, the merely procedural option 1 would significantly water down the Commission's proposal and might have a chilling effect on national legislators to enact B2G legislation (which would also not allow for cross-border access), so that it would ultimately raise the question what the benefit of Chapter V would be at all. Therefore, **option 2 appears like the most reasonable and viable avenue for the legislature at the given time – keeping the scope rather narrow, while at the same time providing more than just procedural harmonisation, something that could make a tangible impact. At the same time, a more restrictive definition that imposes clear boundaries to the scope of application has functional advantages. It allows safeguards to be strong and effective, and to more coherently justify the rules on compensation and the treatment of small and micro enterprises (see below 2.5). Option 2 also enables the legislature to extend legislation towards options 3 or 4 at a later stage, once substantial experiences with B2G ad hoc access based on Chapter V have been made and evaluated. Not least in this regard, starting with a rather narrow scope while keeping the perspective of broadening it in future appears reasonable.**

2.1.4 The relationship with voluntary data sharing agreements

Regardless of the option to be followed, it is important to stress that the proposed Regulation **neither applies to nor prohibits voluntary agreements** that consider the exchange of data between private and public entities (Recital 59), even within the scope of the Regulation. The operational part of the Data Act should state this more explicitly. In fact, a large deal of B2G data sharing is and has always been based on voluntary agreements. When introducing an *obligation* to grant access to data, one needs to carefully consider how this affects the businesses' eagerness to share data in future on a voluntary/contractual basis – not least to avoid that B2G data sharing decreases because of disincentivising agreements and including circumvention clauses.

Therefore, the legislature should **include a new provision in the form of an Article 16(3), according to which the Regulation leaves voluntary data-sharing agreements between PSBs and private data holders unaffected as long as such agreements do not explicitly rule out the application of the rules under Chapter V. At the same time, Article 16(3) should declare such clauses void *ex lege*. The title of Article 16 should also be amended accordingly ('Relationship with data sharing agreements and other obligations ...').**



2.2 Request for Data to be Made Available and Compliance (Article 17 and 18)

The Proposal takes transparency and proportionality as guiding principles for the proposed data request mechanism in Articles 17 and 18 (see also Recital 61), which is to be welcomed. To ensure **transparency**, Article 17(2)(f) obliges PSBs to make all requests publicly available online without undue delay. However, Article 31(3)(g), which designates competent authorities and tasks, is narrower as it only concerns the online public availability of requests in case of public emergencies. In order to maximise transparency, **Article 31(3)(g) should cover all requests and therefore be changed to ‘in case of exceptional need to use data’.**

Nevertheless, the Proposal does not solve a factual challenge that PSBs face: According to Article 17(1)(a), it is necessary that PSBs specify the required data in their request. Often, however, PSBs do not know exactly what data private entities hold. If the request is not framed precisely, the data holder may legitimately decline the request due to an ‘unavailability’ of the requested data pursuant to Article 18(2)(a). Therefore, a **systemic information asymmetry** can hamper the effectiveness of the proposed data access right. The legislature could consider two options to address this concern. One would be to provide the PSBs with a more differentiated access right according to a three-step logic: (1) right to access information about the available datasets; (2) access to (sample) datasets for assessing their usefulness with regard to fulfilling the desired purpose; and (3) access to datasets for using them in accordance with the purpose.²⁰³ However, since this may lead to additional efforts of the data holder and might cause problematic delays, it is sensible **to at least require best efforts on the part of the data holders to provide information about available datasets and ultimately provide data that are best suited to fulfil the public interest purpose.** In any case, data holders should not be able to decline a request too easily on the grounds of data unavailability.

Article 18(3) implements the ‘**once-only principle**’,²⁰⁴ which aims to avoid burdening companies with multiple requests.²⁰⁵ This principle obliges PSBs to keep track of and publish data requests (Article 17(2)(f)) and to destroy the data when no longer needed (Article 19(1)(f)), and it may also incentivise a better cross-border coordination between PSBs. The ‘once-only principle’ is however limited to situations of public emergency (Article 18(3) and (4)) – and, particularly in this context, the design of the proposed procedure can be counterproductive.: As it stands, the proposed rules allow the data holder to legitimately decline the request (and therefore effectively prevent the PSB from obtaining the desired data) not only (a) if the PSB that made the first request forgot to notify the data holder of the destruction of the data, but also (b) if this PSB is no longer in possession of the data, or (c) if it cannot provide the data in a timely manner to the PSB in exceptional need. In case of emergency, the public interest in effectively responding to the emergency should prevail – at least in cases (b) and (c). Hence, the **legislature could consider applying the ‘once-only principle’ only to exceptional cases of**

²⁰³ See Heiko Richter, The law and policy of government access to private sector data (‘B2G data sharing’), in German Ministry of Justice and Consumer Protection and Max Planck Institute for Innovation and Competition (eds), *Data Access, Consumer Interests and Public Welfare* (Nomos: Baden-Baden 2021) 529, 547.

²⁰⁴ See SWD(2022) 34 final, p 160.

²⁰⁵ Ibid.



need for data under Article 15(1)(b) and (c) but not Article 15(1)(a). Arguably, however, the practical relevance may become limited as the requests then covered are probably less likely to serve exactly the same purpose in multiple cases. A preferable alternative solution would consist in **providing for a ‘backdoor’ provision in Article 18(4), according to which the data holder still has an obligation to make the data available if the requesting PSB – after making reasonable efforts²⁰⁶ – cannot obtain the data from PSBs that made previous requests.**

As for the **procedure on challenging requests**, Article 18(6) refers to Article 31. However, Articles 31-34 do not further specify the procedure (deadlines or interim decisions, for instance). This appears particularly insufficient in case of public emergency: While Article 18(2) recognises the urgency by shortening the period for declining or seeking modification of the request, it remains entirely unclear and therefore left to the Member States to decide what happens if the data holder declines the request and the PSB wants to challenge it. **Therefore, it is important that the enforcement provisions of Chapter IX install a more specific procedure on challenging requests and redress. Moreover, Article 17(2)(e) should require the PSB to include a reference to the means of redress where the applicant wishes to challenge the request (see, for example, Article 4(4) OD PSI Directive).**

2.3 Purpose Limitation and Re-use (Article 17 and 19)

As a key provision, Article 17(3) prohibits the PSB from making obtained data available for re-use under the OD PSI Directive. This prohibition seeks to safeguard the interests of the data holders – if they are obliged to share their data with PSBs, this data should not be re-used by third parties for other purposes (except for the rather narrow cases mentioned in Article 21). However, as regards the use and re-use of the obtained data in question, the **proposal falls far short** in safeguarding the interests of the data holders while at the same time it failing to unleash the potential for data-related societal benefits.

Article 17(3) **does not effectively protect the legitimate interests of the data holders** for two reasons. Firstly, the provision does not rule out the application of Articles 3-8 DGA, which regulate the re-use of public sector data that is protected by private rights (trade secrecy, personal data, intellectual property). Secondly, the provision would not prevent the *accessibility* of data under legislation of the Union or the Member States. This is because the OD PSI Directive does not provide access to data, but only regulates re-use of data. For access to data, national rules (such as access to information regimes) or sectoral EU or national legislation (access to environmental or geographic information, for instance) are key. But the Proposal does not affect, let alone exclude, access of third parties to data which a PSB has obtained under Chapter V under such access regimes. This is surprising, because it appears that this is exactly what the Proposal ultimately aims to avoid in order to duly safeguard the interests of the data holders. This regulatory intention is reflected in Art. 17(4), which allows only for privileged access for third parties in case of outsourcing under the condition that the third party meets the obligations and safeguards outlined in Art. 19.

²⁰⁶ This would also have to consider the urgency of the request.



At the same time, the proposal **does not duly take into account the potential for data-related societal benefits through re-use**. Chapter V data access enlarges the pool of public sector data, so that rules on access to and re-use of public sector information can potentially apply. This means that the OD PSI Directive could be applicable, which regulates re-use by generally accessible public sector information (PSI), following the premise that wide and non-discriminatory re-use of data is favourable, because it can create additional economic and societal value. Against this background, there is no convincing justification for this *per se* prohibition. Recital 62 still aims to explain this by stating that the data ‘may be commercially sensitive’. However, such sensitive data only amounts to a portion of all data shared under the Regulation and would be excluded from the scope of application of the OD PSI Directive anyway.²⁰⁷

Therefore, the **legislature should re-consider the Proposal’s handling of accessibility and re-use of the data**. Due to the potential positive externalities of data re-use, the PSB should be able to make the obtained data available under the OD PSI Directive as long as legitimate interests of businesses as data holders are not negatively affected.²⁰⁸ Therefore, the proposed Regulation should reconcile the involved interests by ultimately leaving the decision of access and re-use to the businesses. This translates into the following **proposal of a consent-based solution, according to which there is no conflict if the data holder agrees with access and re-use. Therefore, the law should at least provide for the possibility of consent of the data holder and provide three options: (1) accessibility of the data and re-use under the OD PSI Directive and the DGA; (2) restricted accessibility of the data and re-use only under the DGA; (3) no accessibility and re-usability**. It remains to be seen whether companies have sufficient incentives (positive public image, data altruism, and so on) to choose the re-use-friendly options. But at least the law should enable (and even nudge) them to do so.

When providing the data according to Article 18, **the data holder should be obliged to choose one of these options. As an opt-out solution, the data holder has the possibility to object to the re-use without the need for justification. In case personal data is affected, an opt-in mechanism is necessary**. This consent-based solution is already reflected in Recital 65, which states that the data holder who made the data available can expressly agree for the data to be used for other than the requested purposes – but surprisingly, the Regulation does not echo this possibility in the provided request mechanism. **Thus, the consent-based solution would require to: first, delete Article 17(3); second, add a paragraph in Article 18, which provides the data holder with the three options to decide on accessibility and re-use of the data as stated above; and third, provide a possibility to waive the PSB’s obligation to destroy the data according to Article 19(1)(c).**

2.4 Use for Research and Statistical Purpose (Article 21)

Article 21 allows use of the obtained data for scientific research or analytics and compilation of official statistics. However, the research must be compatible with the purpose for which the data was originally requested, and there may be grey zones (for instance, as regards the questions of whether

²⁰⁷ See Art 1(2)(c) OD PSI Directive.

²⁰⁸ See Heiko Richter, The law and policy of government access to private sector data (‘B2G data sharing’), in German Ministry of Justice and Consumer Protection and Max Planck Institute for Innovation and Competition (eds), Data Access, Consumer Interests and Public Welfare (Nomos: Baden-Baden 2021) 529, 554.



the research has to relate to addressing the concrete emergency or whether the data can be used for general research on emergency prevention).²⁰⁹ Article 21 appears **overly narrow** when it comes to the legitimate research purposes, not least because scientific research is an open-ended process. Regarding Article 21, **the legislature should consider whether there are reasonable means to broaden the purpose or install a more flexible regime while safeguarding the interests of the data holder**. In fact, the legislature has already installed a mechanism in Articles 3-8 DGA that carefully balances such involved interests. The text should consider potential benefits of systematically referring to the DGA or at least borrowing from its concepts, crucially because Article 21 remains silent on conditions, non-exclusivity, technical and legal safeguards (except for Article 21(3)) and so on – all aspects which the DGA explicitly addresses.

However, it must be acknowledged that from a realistic policy standpoint framing an adequate legal framework for data access to the benefit of research organisations appears as a **complex challenge where legislative conceptualisation is only in the early stages**. In order to do so, multiple interests must be considered, definitions have to be clarified (research organisation, research purpose, how to deal with public private partnerships, the safeguards for the interests of data holders), while also accounting for the specificities of the distinct research systems of the Member States. **Given the current stage, duly conceptualising privileged access for research organisations appears to overburden the policy discussion on Chapter V. Therefore, the legislature should take separate initiative at a later stage with regard to data access that reaches beyond the rare cases covered by Art. 15(a)** – not the least to already consider whether access under Chapter V proves to take place effectively.

2.5 Compensation (Article 20)

It is to be supported that Article 20(1) obliges data holders to make data available free of charge in case of **public emergency** (see also Recital 67). As this report has argued that **micro and small enterprises should be included in the scope of the Regulation in case of public emergencies covered by Article 15(a)** (see above), **the legislature should consider providing compensation to them if the data access request would endanger their existence (implicitly presuming that a single request might considerably affect the operations of micro and small entities). To avoid endangering their existence, Article 20 should also oblige public sector bodies to a lump-sum payment, or an upfront payment of the compensation, based on a rough estimate of the costs. The difference is to be made up after the provision of the data has terminated.**

In other cases of exceptional need for data, Article 20(2) provides for compensation of the costs incurred to comply with the request, including the costs for pseudonymisation. This includes the marginal costs of a request (which can be compared to Article 6(1) OD PSI Directive). In addition, Article 20(2) **allows for a 'reasonable margin'** to be charged. This, however, is problematic. First, it remains unclear how to calculate the reasonable margin as required in Article 20(2). The provision already implies that this should be calculated based on a cost-based and not on a benefit-based

²⁰⁹ See also Recital 68.



approach.²¹⁰ For the sake of legal certainty, the cost-based approach as a reference point for calculating the reasonable margin should then be made more explicit in Recital 67 – it can be compared to Article 6(4) OD PSI Directive, which allows to include cost of the data “collection, production, reproduction, dissemination and data storage, together with a reasonable return on investment”. Second, as the scope of the access right is limited to *ad hoc* situations, it is unlikely that access requests would negatively affect the data holders’ ability to collect/create the data,²¹¹ which could justify a full-cost-recovery approach such as a ‘reasonable margin’. Moreover, margins are unlikely to create incentives for the businesses “to have such data ready”, due to the unforeseeability of requests given the *ad hoc* logic of the exceptional data need according to Chapter V. Third and last, compensation under Article 20(2) relates to cases where the PSB cannot obtain the data on the market at market rates (Article 15(c)(1)). If the data holder has decided not to provide the data on the market, there is no economic justification for why mandatory sharing should reward the data holder by providing a reasonable margin. Conversely, such mandated margin could disincentivise data holders from providing their data through market mechanisms, which the Commission’s data policies actually seek to foster. Therefore, **while compensation of marginal cost occurring because of the request appears justified, the possibility to charge a reasonable margin under Article 20(2) should be deleted.**

2.6 Interface with Private Rights and Interests

2.6.1 Personal data

Deciding to what extent Chapter V also covers personal data requires the legislature to make a **trade-off**. This trade-off depends on how one assesses the specific risks that data access under Chapter V would pose for individuals’ informational self-determination. The answer to this question also depends on the actual effectiveness of investigations and enforcement regarding violations of data protection laws. However, this question goes beyond what this analysis can provide.

If the legislature follows the Commission’s proposal, in which Chapter V also covers personal data, the provisions should be made more precise regarding the relationship to personal data protection. Article 1(3) states that the Regulation leaves the application of data protection law unaffected. But what this means depends on the specific case and context. In particular, Article 18(5) requires data holders to take reasonable efforts to pseudonymise the data if such data are needed. An extension of this obligation to **anonymisation** is also implied in Recital 64.²¹² Therefore **anonymisation should be explicitly mentioned in Article 18(5) as well. At the same time, Chapter V should explicitly ban efforts of PSBs and other data recipients to “re-identify” anonymised data, or to link datasets with the purpose of re-identification.**

²¹⁰ See Heiko Richter, The law and policy of government access to private sector data (‘B2G data sharing’), in German Ministry of Justice and Consumer Protection and Max Planck Institute for Innovation and Competition (eds), Data Access, Consumer Interests and Public Welfare (Nomos: Baden-Baden 2021) 529, 549;

²¹¹ See Heiko Richter, The law and policy of government access to private sector data (‘B2G data sharing’), in German Ministry of Justice and Consumer Protection and Max Planck Institute for Innovation and Competition (eds), Data Access, Consumer Interests and Public Welfare (Nomos: Baden-Baden 2021) 529, 549.

²¹² Where anonymisation proves insufficient, Recital 64 requires pseudonymisation.



Conversely, the provision on compensation only mentions compensation for anonymisation, while there are no reasons to exclude the compensation for **pseudonymisation**. Hence, **Article 20(2) should equally provide compensation for pseudonymisation**. As anonymisation and pseudonymisation constitute data processing under Article 4(2) GDPR, they must be lawful according to Article 6(1) and (2) GDPR. For this purpose, **the legislature should clarify (in Recital 64, for example) that Article 18(5) itself provides a legal basis for anonymisation and pseudonymisation according to Article 6(1)(c) and (3)(a) GDPR**.

2.6.2 Intellectual property

Chapter V leaves intellectual property unaffected²¹³ with one exception: when it comes to **sui generis database protection**, Recital 63 states that ‘data holders should exercise their rights in a way that does not prevent the PSB and Union institutions, agencies, or bodies from obtaining the data, or from sharing it, in accordance with this Regulation’. This provision is necessary to enable B2G data sharing,²¹⁴ and it resembles Article 1(6) OD PSI Directive as well as Article 5(7) DGA. However, due to its substantive effect to limit the businesses’ exercise of intellectual property rights, a Recital is not sufficient; **the subsidiarity of sui generis database protection in the context of B2G data sharing must be made explicit in the operational part of the Regulation (included as a new Article 35(2), for instance)**. In fact, should the concerned data be the content of a protected database, Chapter V makes it compulsory for data holders to license the *sui generis* database right to the requesting PSB. At the same time, Recital 63 implies that businesses will not be prevented from invoking *sui generis* protection for any sharing that is not in accordance with the Regulation and therefore will have some control over illegitimate (re-)use.

2.6.3 Contractual restrictions with third parties

Chapter V has another blind spot: what about cases in which the data holder is prevented from making the data accessible to the PSB due to **mere contractual restrictions with third parties** (and not due to trade secrecy or intellectual property)? Recital 66 implies that such contracts trump and may therefore prevent data access under Chapter V *per se*. Again, such a strict consequence must be reflected in the operational part of the Regulation (such as by including a new Article 19(3)). In substance however, the approach appears questionable: it is hardly justifiable to let contractual restrictions prevent access *per se*, not least because Chapter V would allow the PSB to request access to the data from the original data holder as well. Moreover, such precedence of contract could incentivise data holders and third parties who supply data to data holders to insert clauses in their contracts with the aim of derogating access obligations pursuant to Chapter V. To enhance B2G data sharing, **the Regulation should render mere derogation clauses void and include a balancing test for cases in which contractual restrictions would prevent data access**.

²¹³ See SWD(2022) 34 final, p 160.

²¹⁴ See Heiko Richter, The law and policy of government access to private sector data (‘B2G data sharing’), in German Ministry of Justice and Consumer Protection and Max Planck Institute for Innovation and Competition (eds), Data Access, Consumer Interests and Public Welfare (Nomos: Baden-Baden 2021) 529, 547, 570.



3. POLICY RECOMMENDATIONS

The following recommendations aim to improve Chapter V of the proposed Data Act. They are based on a holistic view, which considers the highly interconnected regulatory components of Chapter V (scope, subsidiarity, compensation, re-use, request and dispute settlement procedure, the interface with private rights) as **different levers to appropriately balance the involved interests**, while providing a legal framework that can effectively reach the regulatory goal.

1. *Scope, preemption, and subsidiarity (Article 15 and 16)*

- 1.1. To increase the effectiveness of state action in public emergencies, the exclusion of micro and small enterprises according to Article 14(2) should be deleted in cases of public emergency according to Article 15(a). The compensation rules should account for legitimate interests of micro and small enterprises that are subject to data requests (see recommendation 5.1).
- 1.2. To clarify and further limit the scope of Article 15(c), the word 'effectively' should be deleted from Recital 58. The word 'prevent' in Article 15(c) should be understood as significantly increasing the effectiveness of fulfilling the specific task, considering the ad hoc nature of the data request.
- 1.3. To avoid that PSBs rely on requests of Chapter V overhastily, and to prevent competition on and the emergence of data markets, the PSB should be required to have taken reasonable efforts to enquire into the market before making requests. This should be spelled out more clearly in Recital 58.
- 1.4. For determining whether the data is available on the market at market rates and to prevent monopoly pricing in such markets, Recital 58 should declare that average cost pricing (which can account for the fixed costs on top of the marginal costs) can be taken as the relevant benchmark.
- 1.5. To limit the scope and to provide legal certainty, it should be clarified that Article 15(c)(1) only concerns *ad hoc* access and stipulates a full derogation of national rules as already be done in Article 40. For this purpose, 'ad hoc access' has to be clearly and narrowly defined. The legislature should delete the requirement of a lack of national legislative measures in Article 15(c)(1). In addition, Article 16(1) should add: 'This Chapter only regulates *ad hoc* data access and ...'; while 'ad hoc access' should be properly defined in Article 2. To increase legal certainty, a presumption should be included regarding the maximum duration and/or number/frequency of repeated similar requests.
- 1.6. Article 15(c)(2) should be deleted because it contradicts the rationale of an 'exceptional' data need.
- 1.7. To strengthen private autonomy (that is, voluntary data-sharing), a new provision should be included as Article 16(3), according to which the Regulation leaves agreements between PSBs and private data holders unaffected as long as such agreements do not explicitly rule out the application of the rules under Chapter V. At the same time, Article 16(3) should declare such clauses void *ex lege*. The title of Article 16 should be amended accordingly ('Relationship with data sharing agreements and other obligations ...').



2. *Requests for data to be made available and compliance (Article 17 and 18)*

- 2.1. In order to increase public transparency on requests based on Chapter V, Article 31(3)(g) should cover all requests and therefore be changed to 'in case of exceptional need to use data'.
- 2.2. To increase the effectiveness of the request mechanism, Art. 18(2) should require at least best efforts on the part of the data holders to provide information about available datasets and ultimately provide data that are best suited to fulfil the public interest purpose.
- 2.3. For the same reason, the legislature could consider applying the 'once-only principle' only to exceptional cases of need for data under Article 15(1)(b) and (c) but not Article 15(1)(a). Alternatively, the legislature could include a provision in Article 18(4), according to which the data holder still has an obligation to make the data available if the requesting PSB – after making reasonable efforts – cannot obtain the data from PSBs that made previous requests.
- 2.4. To strengthen enforcement, Chapter IX should install a more specific procedure on challenging requests and redress. Moreover, Article 17(2)(e) should require the PSB to include a reference to the means of redress where the applicant wishes to challenge the request (such as in Article 4(4) OD PSI Directive).

3. *Purpose limitation and re-use (Article 17 and 19)*

- 3.1. To increase re-usability of data provided under Chapter V, while at the same time safeguarding the interests and respecting the private autonomy of businesses, Chapter V should leave the decision of access and re-use of the shared data to the private data holder. The legislature should implement a consent-based solution, according to which the data holder may agree with access and re-use. Therefore, the Article 17 should at least provide for the possibility of consent of the data holder and provide three options: (1) accessibility of the data and re-use under the OD PSI Directive and the DGA; (2) restricted accessibility of the data and re-use only under the DGA; (3) no accessibility and re-usability. The data holder should be obliged to choose one of these options. As an opt-out solution, the data holder has the possibility to object to the re-use without the need for justification. In case personal data is affected, an opt-in mechanism is necessary.
- 3.2. Therefore, (1) Article 17(3) should be deleted; (2) a paragraph in Article 18 should be added, which provides the data holder with the said three options to decide on accessibility and re-use of the data as stated above; and (3) Article 19 should provide a possibility for the data holders to waive the PSB's obligation to destroy the data according to Article 19(1)(c).

4. *Use for research and statistical purposes (Article 21)*

- 4.1. To increase the potential of using the provided data for research, the legislature should consider whether there are reasonable means to broaden the purpose or install a more flexible regime, while better safeguarding the interests of the data holder.
- 4.2. However, given the current stage, duly conceptualising privileged access for research organisations appears to overburden the policy discussion on Chapter V. Therefore, the legislature should take separate initiative at a later stage with regard to data access that reaches beyond the (rare) cases covered by Art. 15(a).



5. *Compensation (Article 20)*

- 5.1. If micro and small enterprises are included in the scope of the Regulation with regards to public emergencies under Article 15(a), the legislature should consider providing compensation to them if the data access request would endanger their existence. To prevent this, Article 20 should also oblige PSBs for upfront payment of the compensation, based on a cursory estimate of the costs. The difference is to be made up latest after the provision of the data has terminated.
- 5.2. In cases other than public emergencies, it not justified to compensate for more than marginal costs that occur because of the request. Given the ad hoc nature of Chapter V, the request mechanism is not designed to subsidise general investments / fixed costs of the data holders. Also, the compensation regime should not curtail incentives to provide data on the market (see 1.4). Therefore, the possibility to charge a ‘reasonable margin’ under Article 20(2) should be deleted.

6. *Interface with private rights and interests*

- 6.1. To increase coherency and provide legal certainty, Article 18(5) should explicitly mention anonymisation, while Article 20(2) should equally provide compensation for pseudonymisation. Furthermore, the legislature should clarify (in Recital 64, for instance) that Article 18(5) itself provides a legal basis for anonymisation and pseudonymisation according to Article 6(1)(c) and (3)(a) GDPR. Moreover, to safeguard the interests of the businesses and rights of data subjects, Chapter V should explicitly ban efforts of PSBs and other data recipients to “re-identify” anonymised data, or to link datasets with the purpose of re-identification.
- 6.2. To comply with the principle of the reservation of the law, the subsidiarity of *sui generis* database protection in the context of B2G data sharing must be made explicit in the operational part of the Regulation (for example, included as a new Article 35(2)).
- 6.3. In order to prevent data holders from circumventing obligations under Chapter V, the chapter should render mere derogation clauses (that is cases in which the data holder is prevented from making the data accessible to the PSB due to mere contractual restrictions) void and include a balancing test for cases in which contractual restrictions would prevent data access.



SWITCHING AND INTEROPERABILITY BETWEEN DATA PROCESSING SERVICES IN THE PROPOSED DATA ACT

Daniel Schnurr



TABLE OF CONTENTS

1. INTRODUCTION	79
2. ECONOMIC AND TECHNOLOGICAL CHARACTERISTICS OF DATA PROCESSING SERVICES MARKETS.....	81
2.1 Economic Characteristics	81
2.2 Technological characteristics	83
3. DATA PORTABILITY AND INTEROPERABILITY AS TWO DISTINCT CONCEPTS.....	85
3.1 Data Portability	85
3.2 Interoperability	86
3.3 Lack of clarity due to mixing of terminology	86
4. ASSESSMENT OF THE SWITCHING AND INTEROPERABILITY PROVISIONS IN THE DATA ACT..	88
4.1 Provisions on Facilitating Switching Between Data Processing Services	88
4.1.1 Maximum notice period to terminate contract and maximum transition period	88
4.1.2 Gradual withdrawal of switching charges.....	89
4.1.3 Transparency requirements and minimum scope of portable data	89
4.1.4 The functional equivalence criterion	90
4.1.5 Services of the same service type.....	92
4.2 Provisions on Open Interfaces and Interoperability of Data Processing Services.....	92
4.2.1 Publicly available open interfaces.....	92
4.2.2 Compatibility with open interoperability specifications or European standards for interoperability	94
5. POLICY RECOMMENDATIONS	96



1. INTRODUCTION

The proposed Data Act (COM(2022) 68 final), henceforth DA, is a key part of the Commission's European strategy for data that complements the recent legislative efforts to facilitate more free flow of data (including, e.g., the Data Governance Act, the Open Data Directive, the Digital Markets Act and several sector-specific regulations on data sharing²¹⁵). The Data Act contains four main parts. The first part (Chapters II-IV) addresses business to consumers (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 data processing services and data spaces. The fourth part (Chapter VII) relates to international access and data transfers.

This issue paper deals exclusively with the third part of the DA, which devises new rules on customer switching and interoperability for data processing services and data spaces. Moreover, the issue paper takes an economic and technological viewpoint and does not discuss the possible legal issues that may arise with respect to this new regulatory framework in further detail. As in the third part of the DA, **the focus of the issue paper will be on data processing services**, which are defined in Art. 2 (12) of the DA as any “digital service other than an online content service [...], provided to a customer, which enables on-demand administration and broad remote access to a scalable and elastic pool of shareable computing resources of a centralised, distributed or highly distributed nature”. Thus, data processing services in the DA are equated with cloud and edge services in all their variety which span from Infrastructure-as-a-service (IaaS) offerings over Platform-as-a-service (PaaS) offerings to Software-as-a-service (SaaS) offerings. In consequence, the scope of these rules is different from the scope of the first part of the DA on B2B and B2C access that refers to manufacturers, service providers, data holders, and data recipients in the context of connected products and related services (i.e. the “internet of things”).²¹⁶

The rules on data processing services in the DA are intended to “**unlock the EU cloud market**”²¹⁷ by facilitating customers' ability to switch between data-processing services and build directly on the earlier **Regulation on the free flow of non-personal data**.²¹⁸ In order to promote a competitive data economy, this regulation called for a cooperative approach among stakeholders to develop self-regulatory codes of conduct that should establish **principles of transparency and interoperability** (considering also open standards) for data processing services.²¹⁹ The Regulation further specified four criteria that should be covered by the envisioned codes of conduct, including **best practices for**

²¹⁵ See, for example, the European Commission's recent proposal on a European Health Data Space (COM(2022) 197 final) as well as the initiatives on mobility, open finance and energy. See on the latter: Ennis and Colangelo (2022). Energy Data Sharing and the Case of EV Smart Charging. CERRE Report. <https://cerre.eu/publications/energy-data-sharing-and-the-case-of-ev-smart-charging/>

²¹⁶ See Krämer (2022). Improving the Economic Effectiveness of the B2B and B2C Data Sharing Obligations in the Proposed Data Act. CERRE Report. <https://cerre.eu/publications/improving-the-economic-effectiveness-of-the-b2b-and-b2c-data-sharing-obligations-in-the-proposed-data-act/>

²¹⁷ European Commission. Data Act. <https://digital-strategy.ec.europa.eu/en/policies/data-act>

²¹⁸ Regulation (EU) 2018/1807 on a framework for the free flow of non-personal data in the European Union, [2018] OJ L 303/59.

²¹⁹ Ibid., Art. 6.



facilitating the switching of service providers and the porting of data as well as minimum information requirements for data processing contracts.

Four years after the adoption of the Regulation on the free flow of non-personal data the European Commission has deemed the self-regulatory efforts of the industry and the developed code of conducts²²⁰ insufficient to satisfy the criteria established in the regulation.²²¹ In consequence, the DA imposes mandatory rules on switching and interoperability between data processing services in order to achieve its **overarching objective of “unlocking” customers’ data and mitigating the supposed vendor lock-in of customers in data services processing markets**. To this end the DA pursues two main goals:

Firstly, the **DA aims to facilitate the switching between data processing services** by removing commercial, technical, contractual, and organisational obstacles that may hinder customers to switch between providers of data processing services.²²²

Secondly, the **DA envisions establishing a seamless multi-vendor cloud environment**, which is viewed to be “a key requirement for open innovation in the European data economy”.²²³ To this end, the DA devises new interoperability regulation and standardisation regimes for data processing services.

The DA is a horizontal law and devised as a symmetric regulation. Thus, in principle, its rules apply equally to any provider of data processing services irrespective of firm size, market position or industry background. In general, this is consistent with the two primary goals of the DA to facilitate customer switching and to promote a seamless multi-vendor cloud environment. Also with respect to the overarching goal of mitigating vendor lock-in a symmetric regulation approach can be justified, as vendor lock-in can generally arise in the context of any data processing service if customers face significant barriers to switching.²²⁴ However, **the symmetric regime also implies that the overall economic costs and the regulatory burden will generally be higher than for a more targeted asymmetric regulatory approach**, as all service providers must comply with the new rules. Moreover, the resulting compliance costs as well as limitations on the freedom to conduct a business **may affect smaller providers disproportionately more than larger providers**.²²⁵ This is important to consider as **the DA is often also viewed as an instrument to address potential competition issues in the market for data processing services**.²²⁶

²²⁰ SWIPO – The Association on Switching and Porting (2022). Switching and Porting, <https://swipo.eu>

²²¹ Data Act, Explanatory Memorandum, p. 4.; Data Act, Recital 70

²²² Data Act, Explanatory Memorandum, p. 3;

²²³ Data Act, Explanatory Memorandum, p. 3; Recital 76

²²⁴ Especially data-induced switching costs can arise for any data processing service provider if the data created during the use of the services cannot easily be transferred to a new service. See Wohlfarth (2019). Data portability on the internet. *Business & Information Systems Engineering*, 61(5), 551-574.

²²⁵ Cf.: There is now increasing empirical evidence that the European General Data Protection Regulation has hurt smaller firms relative to larger firms and has led to increased market concentration in markets such as advertising and analytics. See Peukert, Bechtold, Batikas & Kretschmer (2022). Regulatory spillovers and data governance: Evidence from the GDPR. *Marketing Science* 41(4), 746-768. Johnson, Shriver & Goldberg (2022). Privacy & market concentration: Intended & unintended consequences of the GDPR. Available at <https://ssrn.com/abstract=3477686>

²²⁶ Cf. Data Act, Recital 69; SWD(2022) 34 final. Commission Staff Working Document Impact Assessment Report, p. 50; ACM (2022), ACM (2022). Amendments to Data Act necessary for promoting competition among cloud providers. <https://www.acm.nl/en/publications/acm-amendments-data-act-necessary-promoting-competition-among-cloud-providers>



2. ECONOMIC AND TECHNOLOGICAL CHARACTERISTICS OF DATA PROCESSING SERVICES MARKETS

To assess the implications of the DA proposal, it is important to consider the specific economic and technological characteristics of the markets for data processing services.

2.1 Economic Characteristics

Foremost, data processing services markets²²⁷ are characterised by **significant economies of scale**. Thus, a larger firm can operate at lower average costs when providing the same service as smaller firms. Firstly, this is due to the need for large investments into physical infrastructures that entail significant fixed costs. This applies especially to data centres, which house servers and network equipment that are crucial to providing data processing services of all types. Secondly, operating costs in these markets also decrease considerably with a larger scale.²²⁸ In particular, data centres of larger size can operate at significantly lower average energy costs, which account for a large share of the total costs of a data centre.²²⁹ Thirdly, quality-of-service features such as security and reliability are characterised by economies of scale. These features are usually developed or purchased by fixed investments, which can then be spread over the entire output, thus yielding decreasing average costs per unit of output. Fourthly, the provision and utilisation of shared resources, a core characteristic of data processing services,²³⁰ implies scale advantages. A larger firm can utilise its shared infrastructure more efficiently, as the demand for this infrastructure balances across customers. The larger the number of customers, the less idle capacity needs to be reserved in relative terms of the entire shared infrastructure, thus leading to lower average costs per unit of output.

At the same time, data processing services entail **significant economies of scope**.²³¹ This is illustrated by the fact that today's largest cloud providers have developed their data processing services offerings by utilising and expanding the IT infrastructure originally established for the operations of their core business units.²³² Utilising an existing IT infrastructure can save large fixed costs and lump-sum investments, allowing instead for incremental upgrading of the necessary IT assets. Moreover, skilled human resources and technical expertise represent important inputs for developing data processing services. These skills and expertise are subject to significant learning effects. Hence, experienced providers with a broad developer base will have significant advantages over single-purpose providers when developing a new data processing service. In turn, many customers today ask for a wide variety

²²⁷ Note that we use the term "data processing services markets" to refer to the various data processing services industries and services segments and do not intend to delineate any relevant market for competition law purposes. Therefore, when we refer to "data processing markets" in this report, we do not refer to a market as in the meaning of a relevant market in competition law.

²²⁸ See Netherlands Authority for Consumers and Markets (2022). Market study into cloud services.

<https://www.acm.nl/system/files/documents/public-market-study-cloud-services.pdf>

²²⁹ Ibid; Banet, Pollitt, Covatariu & Duma (2021). Data Centres and the Grid – Greening ICT in Europe. CERRE Report.

<https://cerre.eu/publications/data-centres-and-the-energy-grid/>

²³⁰ Data Act, Recital 71

²³¹ See Krämer, Schnurr & Broughton Micova (2020). The role of data for digital markets contestability: Case studies and data access remedies. CERRE Report, p. 67f., <https://cerre.eu/publications/data-digital-markets-contestability-case-studies-and-data-access-remedies/>

²³² See, for example, Miller (2016). How AWS came to be. <https://techcrunch.com/2016/07/02/andy-jassys-brief-history-of-the-genesis-of-aws/>



of data processing services, such that offering a broad range of different, complementary data processing services can provide a competitive advantage.

Related to economies of scope, **bundling strategies are widespread for data processing services**, especially at the IaaS and PaaS layers.²³³ While wholesale marketplaces also exist where independent service providers can offer data processing services that run on platforms of different service providers, the largest providers of IaaS and PaaS services now all offer **integrated ecosystems** spanning across specialised data processing services of different types and purposes. Due to synergies on the supply side and customers' frequent demand for a one-stop shop of different types of services, it is often economically advantageous for providers to offer bundles of data processing services that can be assembled and configured freely by each customer on their own. Such product bundling is frequently complemented by providers' pricing schemes that, for example, regularly offer lower fees for data transfers among internal services than for external transfers to services of other providers.²³⁴ Moreover, quantity discounts and discounts for longer-term subscriptions may encourage customers to purchase services from a single provider.²³⁵

Finally, data processing services may be subject to direct and indirect **network effects**.²³⁶ In particular, several providers of data processing services offer marketplaces, where customers can combine services of the provider with additional third-party components and services.²³⁷ The larger a provider's customer base, the higher the incentives for third parties to adopt such a marketplace and develop additional services, and vice versa. Additional network effects can especially emerge at the SaaS layer, although they will usually stem from the specific characteristics of a particular service type rather than from the service's characteristic as a data processing service. For example, the value of a cloud-based office suite for a customer increases in the size of the overall customer base, as this makes it more likely that messages and documents can be exchanged and shared with others outside of their own organisation if no universal standard exists for such messages or documents.

Altogether, these economic characteristics favour larger providers of data processing services and promote concentration of markets for data processing services. Especially at the IaaS and PaaS layers, economies of scale and scope can be expected to be particularly pronounced.²³⁸ These economic characteristics are conducive to a *competition for the market* dynamic, where providers offer integrated services ecosystems and compete based on different technical standards. This has two main implications: First, additional regulatory safeguards may be necessary to maintain the

²³³ In general, product and service bundling is typical for various digital markets, as illustrated by the ecosystems of digital platforms (see, e.g., Recital 3 of the Digital Markets Act) and the earlier debate on service bundling in the context of "digital convergence" in the telecommunications industry (see, e.g., Pereira and Vareda (2013). How will telecommunications bundles impact competition and regulatory analysis?. *Telecommunications Policy*, 37(6-7), 530-539).

²³⁴ ACM market study, supra note 12; Lower fees for internal data flows can stem from lower costs for the service provider to transfer data on its own infrastructure, whereas external flows can result in higher costs that are then passed on to customers.

²³⁵ See, e.g., https://aws.amazon.com/pricing/?nc2=h_ql_pr and <https://learn.microsoft.com/en-us/azure/cost-management-billing/savings-plan/discount-application>; Longer-term subscriptions also offer providers greater certainty and predictability regarding demand and thus facilitate the planning of capacity investments.

²³⁶ See also the ACM market study, supra note 12 for a more detailed discussion of network effects in the context data processing services.

²³⁷ ACM market study, supra note 12.

²³⁸ Service differentiation and specialisation may counteract concentration tendencies from scale and scope advantages as well as network effects as discussed in the next subsection. However, for more general-purpose, less specialised service offerings economic theory predicts more concentrated markets due to the described characteristics.



contestability of these markets in the long run and to protect customers of data processing services. Second, competitors in these markets will often try to establish their own standards in order to differentiate their services from other providers. In these cases, interoperability regulation can restore a common standard thus promoting *competition in the market*. However, such mandatory interoperability regulation would come at the cost of limiting technological flexibility and potential innovation (as discussed further below) and can be at odds with the inherent economic forces and incentives in these markets, which would entail significant implementation costs, especially for regulatory monitoring and enforcement.

2.2 Technological characteristics

From a technological perspective, it is important to acknowledge that **the current data processing services environment is highly dynamic and data processing services are constantly evolving**. This applies to individual data processing services that are updated frequently with added new functionalities, but also to the overall set and variety of available data processing services, which grow steadily and include more and more new specialised services.

With respect to the software architecture of data processing services, there has been an increasing trend toward the **decoupling of software functionalities** and **modularisation of software into micro-services**. In the extreme, this has led to the paradigm of Functions-as-a-Service (FaaS), as most prominently exemplified by the concept of serverless computing.²³⁹ Here, all computing resources are allocated on-demand and provided once a specific function in the software is called on runtime. In consequence, there is no need for reserving computing capacity, and developers, as well as users, do not need to be concerned with resource planning or configuration and management of the underlying software and hardware infrastructure. From a technical perspective, this requires that individual software functions are outsourced and provided as single-purpose micro-services that can be called externally through an interface. Upon request, these micro-services will then return an output according to a pre-defined specification such that the output can be processed by the software that has called the service.

Two main insights can be gained from these observations on the current state of technology of data processing services: On the one hand, the increasing modularisation of functionalities introduces the possibility that various data processing services can be mixed and matched into larger software ensembles and value networks. In principle, this would also allow for **ensembles of services that span across the ecosystem boundaries of a single data processing service provider** and thus could support the vision of a “seamless multi-vendor cloud environment”. From an economic perspective, more granular software modules may also allow for more specialisation and promote service differentiation, which could counteract concentration tendencies from scale and scope advantages as well as network effects. On the other hand, however, increasing modularisation increases the need for **cross-cutting coordination, integration, and management of individual services** such that interoperability, performance, and high quality of service ensembles can be maintained. Such coordination and

²³⁹ Roberts (2018). Serverless Architectures. <https://martinfowler.com/articles/serverless.html>



integration can often be achieved at lower transaction costs within the boundaries of a single organisation, whereas coordination and integration between organisations and across heterogeneous stacks of data processing services introduce additional complexity and costs.²⁴⁰ Technically this can be solved by the **standardisation of interfaces** and respective input/output relations. However, such standards firstly hinge on an agreement between the involved organisations on the **precise requirements for each standardised type of service** and secondly they **codify the status quo of the current input/output requirements into the standard**. Standardisation thus renders changes and further developments on the cross-cutting level subject to more complex coordination, as actors need to agree on synchronous updates of the respective standard. From a technical and institutional view, this can be facilitated by regular updating mechanisms and corresponding procedural arrangements. In general, such inter-organisational coordination is easier to achieve if involved stakeholders participate voluntarily and share an aligned interest in establishing the standard.

²⁴⁰ The manifold dependencies between micro-services and the need for intimate knowledge about the services' relations and properties also make it unlikely that such coordination and integration could be achieved by an emerging market of specialized third parties.



3. DATA PORTABILITY AND INTEROPERABILITY AS TWO DISTINCT CONCEPTS

The DA includes rules referring to both data portability and interoperability in the context of data processing services. Yet, the DA does not clearly distinguish between the two concepts, nor is it sufficiently clear as to which rules are intended to achieve each of them. This could lead to confusion in the interpretation of the rules. Therefore, here we elaborate on data portability and interoperability as two distinct concepts in detail (see also the illustration in Figure 1) and consider how the two concepts are related to the different goals of the DA.

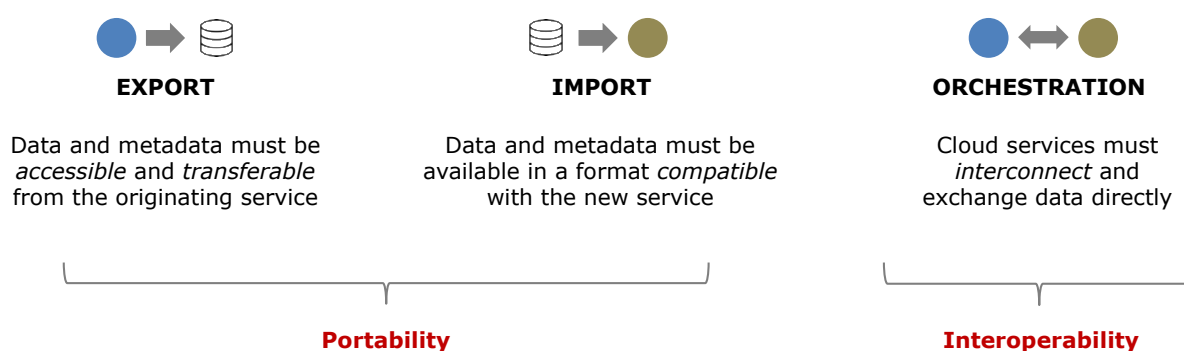


Figure 1: Data portability and interoperability as two distinct concepts.

3.1 Data Portability

Data portability in the context of data processing services requires that **data** that was created during the use of a service by a customer can be **exported from the original service provider and imported to the destination service provider**. In addition, data portability for data processing services should also include **metadata** (such as configuration parameters) that have been entered by customers to set up and configure their services, which would otherwise need to be re-entered manually at the new service provider.²⁴¹ In this context, it is important to distinguish between one-off data portability at a specified point in time and continuous data portability. In general, **one-off data portability is sufficient for the purpose of switching between data processing services**.²⁴² Thus, there is also no general need for application programming interfaces (APIs) to support the data export and import for the purpose of switching, as simple downloading and uploading of the data is generally sufficient to support the switching process.²⁴³ What matters more is that the exportable data is available in a **structured, commonly used, and machine-readable format** such that the data can be transformed into a compatible format and imported and interpreted by the destination service.

²⁴¹ The portability of metadata is more intricate than that of data at the service level, as, e.g., some configurations or parameters may not be directly usable or interpretable by the new service. However, if metadata is provided in a structured, commonly used and machine-readable format, this should enable the destination service provider to access information that can facilitate configuration of services at the destination provider, especially in cases where the customer sets up the same services as at the original service provider.

²⁴² It may sometimes be the case that a switching customer needs to port its data more than once from the original service to the destination service, e.g., if the destination service needs to be tested with data from the original service before serving as the production system. However, this still does not require continuous data portability, as one-off data portability supports the repeated porting of updated data batches.

²⁴³ APIs could nevertheless facilitate direct data transfers and thus could contribute to easier switching between providers.



3.2 Interoperability

In general, the concept of interoperability refers to **the ability of systems to exchange data and information**. In this vein, interoperability is a **prerequisite for the interconnection** of different systems.²⁴⁴ In the context of data processing services, interoperability therefore makes it possible to combine different data processing services into **larger and more complex service ensembles**. Today, this is usually feasible within the environment of a specific provider of data processing services but is more limited to interconnecting services across the boundaries of different service providers. However, this may also depend on the service type, as several data processing services, especially at the IaaS and PaaS layers, contain open interfaces that allow for such interconnection on the service level (see, e.g., web servers or operating systems). In general, **interconnection between decoupled data processing services requires APIs that allow for the continuous and structured flow of data across services**. Interoperability of data processing services is viewed by the European Commission as a necessary requirement to reach the goal of a multi-vendor cloud environment.²⁴⁵

3.3 Lack of clarity due to mixing of terminology

In its most general form, the concept of interoperability allows for the interconnection of data processing services of different providers that are not of the same service type. A key feature of such **vertical interoperability** is that it allows to mix and match different services into service ensembles.²⁴⁶ For example, a service ensemble may include the database service of one provider, the web server of another provider, and the payment service of yet another provider. In addition, vertical interoperability can be viewed as a prerequisite for **service portability**, i.e., the ability of a customer to move an entire data processing service from one provider to the other. Service portability goes beyond data portability, as the customer could port an entire data processing service and run this service on the provider's platform and infrastructure. However, this necessitates vertical interoperability between services and the underlying platform and infrastructure.

More specifically, **horizontal interoperability** refers to the interoperability of data processing services of the same service type. Such horizontal interoperability is imposed by several rules of the DA (see, e.g. Art. 29 (1)) and defined by Art. 2(19). However, it is not obvious what would be the general purpose of interconnecting two services of the same service type at runtime. While it could enable multi-homing of customers that want to use the same service type at two distinct providers and interconnect these two services, such a use case seems rather exceptional. Thus, in the context of these rules, the **definition of interoperability in the DA in Art. 2 (19)** refers to "the ability of two or more data spaces or communication networks, systems, products, applications or components to exchange and use data in order to perform their functions" could be viewed rather **as a requirement**

²⁴⁴ See Bourreau, Krämer & Buiten (2022). Interoperability in Digital Markets. CERRE Report. <https://cerre.eu/publications/interoperability-in-digital-markets/> for more details on interoperability in digital markets and a further distinction between the concepts of horizontal and vertical interoperability.

²⁴⁵ Data Act, Explanatory Memorandum, p. 16.; Data Act, Recital 76

²⁴⁶ CERRE report on Interoperability in Digital Markets, supra note 29.



on the portable data and its compatibility with the destination services. The literature has sometimes referred to such requirements as **data interoperability**.²⁴⁷

However, mixing the terminology risks confusing inherently different concepts of portability and interoperability. Therefore, we reiterate earlier calls from stakeholders²⁴⁸ that the **DA should be clear about the two distinct concepts of data portability and interoperability** and clarify how these two concepts are related to the intended policy goals as well as the individual provisions in the DA.

²⁴⁷ See, e.g., Drexler, Banda, Gonzalez Otero, Hoffmann, Kim, Kulhari, Moscon, Richter & Wiedemann (2022). Position Statement of the Max Planck Institute for Innovation and Competition of 25 May 2022 on the Commission's Proposal of 23 February 2022 for a Regulation on harmonised rules on fair access to and use of data (Data Act). <https://ssrn.com/abstract=4136484>; Hoffmann and Gonzalez Otero (2020). Demystifying the Role of Data Interoperability in the Access and Sharing Debate. *JIPITEC* 11, 252.

²⁴⁸ Netherlands Authority for Consumers and Markets (2022). Proposal to enhance the draft Data Act. Based on a national market study into Cloud services. <https://www.acm.nl/system/files/documents/proposal-to-enhance-the-draft-data-act.pdf>



4. ASSESSMENT OF THE SWITCHING AND INTEROPERABILITY PROVISIONS IN THE DATA ACT

4.1 Provisions on Facilitating Switching Between Data Processing Services

4.1.1 Maximum notice period to terminate contract and maximum transition period

Article 23 is aimed at removing obstacles to effective switching between providers of data processing services. To this end, Art. 23 (a) specifies that **providers must allow customers to terminate their contractual agreement of a service within a maximum notice period of 30 days**. In consequence, customers may be able to change services flexibly and on a short-term notice. At the same time, however, such an obligation would severely limit the parties' freedom to conduct a business and interfere with the freedom of contract, even though the involved parties will regularly be businesses and not consumers. Moreover, in many other markets (including consumer markets), minimum contract durations are present and accepted as commercial instruments. **It is difficult to see what would justify such an exception to the norm for markets of data processing services.**

In addition, the obligation is not specifically targeted to the switching process itself and therefore runs the risk of unintended and adverse side effects. Long-term contracts can also be beneficial for customers of data processing services, especially if they receive rebates or price certainty in return. For providers of data processing services, longer and pre-specified contract durations allow for more certainty regarding demand and thus facilitate the planning of capacity investments. Most importantly, longer-term contracts may represent a valuable commercial instrument for smaller providers and market entrants to entice customers and retain those customers for a pre-specified period of time, which can foster the growth of these businesses.

In contrast, a **maximum transition period for the switching process itself** (after a service contract was terminated), as specified in Article 24 (1) (a), is more targeted to the switching process and can also reduce the uncertainty for customers who consider switching providers. A maximum transition period presents customers with a safeguard against undue delays during the switching process which could otherwise pose a business risk for customers. Delays and risks involved in switching processes have also been prominent issues in telecommunications markets. In response, sector-specific regulation has introduced additional safeguards and respective obligations on providers to protect customers against delays and uncertainties when switching providers.²⁴⁹ Also based on this regulatory experience, we consider a maximum transition period **a suitable safeguard to facilitate switching** between data processing services.

²⁴⁹ See, for example, the Directive (EU) 2018/1972 on establishing the European Electronic Communications Code, [2018] OJ L321/36, which imposes obligations on number portability and requires that "porting of numbers and their subsequent activation shall be carried out within the shortest possible time on the date explicitly agreed with the end-user. In any case, end-users who have concluded an agreement to port a number to a new provider shall have that number activated within one working day from the date agreed with the end-user."



In contrast to telecommunications markets, however, **switching data processing services between providers can be much more complex** depending on the type of service, the size of the customer and whether entire services ensembles are involved, among other factors. In addition, successful switching of data processing services does not depend exclusively on the original service provider but requires input and actions from the destination service provider as well as the customer. Therefore, the original service provider should only be subject to the maximum transition period if the customer and the destination service provider have completed their respective actions that are necessary for switching. In cases where these parties fail to do so, the original service provider should be exempted from the maximum transition period.

In cases where technical obstacles or exceptional circumstances make it unfeasible to comply with the maximum transition period, the burden of proof should be on the original service provider as specified by Art. 24 (2). This presumes that the customer provides the original service provider with all necessary information about the service to be switched. On the other hand, the customer and the destination service provider should bear the burden of proof that they have taken all of their necessary actions to complete the switching process within the maximum transition period.

4.1.2 Gradual withdrawal of switching charges

Art. 25 imposes the **gradual withdrawal of switching charges over three years after the publication of the DA**. The obligation targets potential financial barriers to switching that have been discussed by several analysts and regulators.²⁵⁰ In general, the elimination of switching charges ensures that the customer's switching decision is based on an unbiased comparison of the benefits and costs of different competing data processing services. Therefore, customers should face **no extra charges tied to the switching process**. However, this does not imply that customers will not have to bear costs for regular performances of the original service provider as agreed upon in their service contract, e.g., with respect to costs for outbound data traffic.

It should be acknowledged, however, that to the extent that providers of data processing services incur additional costs for the switching of a departing customer, the symmetric regulation regime **may place a relatively higher burden on smaller providers** of data processing services.²⁵¹ This is because larger providers may be able to recoup or absorb foregone revenues from the withdrawal of switching charges more easily by adjusting general prices, spreading costs across a larger number of customers, or generally having access to greater financial capabilities.

4.1.3 Transparency requirements and minimum scope of portable data

Article 24 imposes conditions on the **contractual terms between the provider and the customer of a data processing service**. Article 24 (1) (b) stipulates **transparency requirements** according to which

²⁵⁰ ACM market study, supra note 12; European Commission (2018). *Switching of cloud services providers*, prepared by International Data Corporation (IDC) and Arthur's Legal. http://publications.europa.eu/resource/cellar/799e50ff-6480-11e8-ab9c-01aa75ed71a1.0001.01/DOC_1; SWD(2022) 34 final. Commission Staff Working Document Impact Assessment Report.

²⁵¹ In telecommunications markets, charges for preselection and number portability services were initially addressed under competition policy and an asymmetric sector-specific regulatory framework. See, e.g., European Commission (1998). Commission terminates procedure against Deutsche Telekom's fees for preselection and number portability and transfers the case to national authorities. https://ec.europa.eu/commission/presscorner/detail/en/ip_22_1113



the contract must include “an exhaustive specification of all data and application categories exportable during the switching process”. The text further defines a **minimum scope of portable data** according to which, the exportable data must comprise the data imported by the customer at the inception of the service agreement as well as all data and metadata created by the customer and by the use of the service (Art. 24 (1) (b)).

This mandatory minimum scope ensures that a customer can **export all of their data that has accumulated over the use of the service** and thus guarantees that the customer should not lose any data as a consequence of switching providers. In addition, the conditions **require that metadata (such as configuration parameters) that was created during the use of the service must be exportable**. This should facilitate switching by mitigating the need for customers to manually reconfigure all of their services at a new provider. Ideally, the exported data can be used to automatically configure services at the new provider and to replicate the quality-of-service functionalities within and across services (such as security and access control) in the environment of the new service provider. Although such automatic configuration may often be not straightforward from a technical perspective, as the metadata depends on the underlying infrastructure and services of the respective service provider, **making the data exportable in a structured, commonly used and machine-readable format** can provide a basis for destination service providers to facilitate data import and the switching process. In cases where the mandatory minimum scope of metadata could reveal **IP-protected information or trade secrets** to the detriment of the original service provider, the service provider should be able to exclude such selected information on an exceptional basis while bearing the burden of proof for demonstrating this.

These conditions on the minimum scope of portable data can be expected to **reduce opportunity costs and transaction costs for customers that want to switch providers** in a meaningful way. In particular, the portability of configurations of data processing services is important to reduce manual effort, which could otherwise be particularly high for customers that want to move larger and more complex ensembles of data processing services to a new provider. At the same time, the necessary **data export functionalities** and accompanying **transparency information** can be provided relatively easily from a technical perspective and can thus be considered proportionate even if they apply to all service providers symmetrically.

4.1.4 The functional equivalence criterion

The obligations on contractual terms and a minimum scope of data portability are complemented by **requirements on technical aspects of switching**.

Art. 23 (1) (d) requires providers of data processing services to ensure **functional equivalence** of a service when a customer switches to another data processing service, which covers the same service type, in accordance with Art. 26. Whereas the legal text of Art. 23 (1) (d) could be interpreted as functional equivalence being a general requirement for all data processing services, Art. 26 is more specific and states that only IaaS services are subject to functional equivalence. However, Article 29 then again discusses functional equivalence in the context of interoperability of data processing



services, which also includes PaaS and SaaS services.²⁵² Therefore, the **applicable scope of the functional equivalence criterion in the DA should be clarified**, especially with respect to Articles 23, 26, and 29.

Article 26 makes a **distinction between data processing services from the IaaS layer and data processing services from the PaaS and SaaS layers**. Article 26 (1) specifically requires providers of IaaS services to “ensure that the customer, after switching to a service covering the same service type offered by a different provider of data processing services, enjoys functional equivalence in the use of the new service.” In contrast, according to Art. 26, providers of PaaS and SaaS services are not subject to such functional equivalence but are subject to obligations on open interfaces and interoperability as specified in Art. 26 (2) to (4), which will be discussed further below.

Functional equivalence itself is defined in Art. 2 (14) as “the maintenance of a minimum level of functionality in the environment of a new data processing service after the switching process, to such an extent that, in response to an input action by the user on core elements of the service, the destination service **will deliver the same output at the same performance** and with the **same level of security, operational resilience and quality of service** as the originating service at the time of termination of the contract” (emphasis added).

Thus, while Art. 24 (1) (b) defines the minimum scope of exportable data and metadata, functional equivalence addresses the **use of the ported data at the new service provider**. To eliminate any losses and opportunity costs from switching for customers, the functional equivalence test in the DA proposal aims to ensure that **the portable data and metadata are of sufficient quality and completeness such that, ideally, an identical service as the original service can be replicated at the destination provider**.²⁵³ Although we agree with this intention behind the functional equivalence test and believe that it is important to include safeguards for the quality and completeness of portable data, we fear that the functional equivalence criterion as currently devised in the DA proposal is **difficult to operationalise** in practice.

In particular, the functional equivalence test seems to hold the original service provider responsible for the output, performance, and quality of the new service (see Art. 2 (14)). However, it is impossible for the original service provider to *ensure* functional equivalence (as stated by Art. 26 (2)), when such equivalence will depend crucially on the actions and the conduct of the provider of the destination service. Instead, the functional equivalence criterion should be clear that **the original service can only be held responsible for its own best effort in providing the exportable data in sufficient quality and completeness such that a destination service provider with the same capabilities as the original provider could replicate the original service**. This principle suggests that the functional equivalence test should be based on a hypothetical “sufficiently capable” service provider (which could also be the

²⁵² Also, Recital 72 of the DA states, seemingly in contrast to Art. 26, that “Functional equivalence means the maintenance of a minimum level of functionality of a service after switching, and should be deemed technically feasible whenever both the originating and the destination data processing services cover (in part or in whole) the same service type.”

²⁵³ See also Recital 72 of the Data Act.



original service provider itself) instead of the actual provider of the destination service.²⁵⁴ We elaborate on this in our proposal for a revised functional equivalence test in Section 5.

4.1.5 Services of the same service type

The DA states that most of the rules on switching between data processing services (see Art. 23) as well as the functional equivalence test for IaaS services should only apply in the context of a customer **switching to a service of the same service type**. The concept of a service type is defined by Art. (2) (13) of the DA as “a set of data processing services that share the same primary objective and basic data processing service model”. Although, on a broad level, it is to some extent intuitive what services belong to different service types (e.g., “data storage service” vs. “computing service” at the IaaS layer or “office suite” vs “enterprise resource planning software” at the SaaS layer), **such a distinction becomes much more intricate on a granular level**. For example, is a SaaS-based office suite that includes a video conferencing tool of the same service type as a stand-alone messaging and video conferencing service? Does a data analytics service belong to a different service type if it uses a different statistical approach than another analytics service? Here, the service type definition of the DA, which refers to the “primary objective” and the “basic data processing service model” of a service is not very helpful to resolve these questions and addressing the **need for establishing a wider classification of service types for all data processing services**. Given the large variety of data processing services that can also be highly differentiated between service providers, this introduces **significant uncertainty about whether and when a data processing service will fall within the scope of the respective obligations of the DA**.

4.2 Provisions on Open Interfaces and Interoperability of Data Processing Services

4.2.1 Publicly available open interfaces

Art. 26 (2) requires providers of PaaS and SaaS services to “make open interfaces publicly available and free of charge”, presumably to facilitate switching between providers. However, if the primary goal of the DA is to facilitate the export and import of data and metadata for switching providers, **the benefits of publicly available open interfaces as described in Art. 26 (2) are not immediately evident** (see also Section 3). Instead, the requirements in Art. 26 (4) that the service provider “shall, at the request of the customer, export all data generated or co-generated, including the relevant data formats and data structures, in a structured, commonly used and machine-readable format” appear more targeted **to facilitate the one-off data import and export for the purpose of switching providers of data processing services**.

In the context of these technical aspects of switching, the Netherlands Authority for Consumers and Markets (ACM) has recently proposed to amend Art. 26 (2) to additionally state that open interfaces should be made available by providers of data processing services *for the purposes of portability and*

²⁵⁴ For the operationalisation of the functional equivalence principle, it is informative to draw on experience in the implementation of the “Equivalence of Input” and “Equivalence of Output” concepts in telecommunications markets regulation, which were designed to ensure non-discriminatory “equivalence of access” for all competitors in downstream telecommunications services markets. See Commission Recommendation on consistent non-discrimination obligations and costing methodologies to promote competition and enhance the broadband investment environment (2013/466/EU), [2013] OJ L 251/13.



interoperability.²⁵⁵ If general interoperability of data processing services were indeed the primary goal of the DA, the need for publicly available open interfaces would be more plausibly justified from a technical perspective, as especially vertical interoperability would require the continuous and automated flow of data across service boundaries. Although Art. 26 (2) in the DA proposal does not explicitly refer to interoperability as a direct purpose, Art. 26 (3) and Art. 29 suggest that interoperability shall be achieved between data processing services at the PaaS and SaaS that cover the same service type.

However, as discussed in Section 3, the benefits of *horizontal interoperability obligations*, which would imply the interconnection of services of the same service type, are rather questionable. A switching customer is seldomly interested in interconnecting the old and the new service of the same service type, but is instead interested in switching from one to the other service provider. As highlighted before, we thus believe that with respect to horizontal relationships between services the focus of the DA should be on promoting data portability and making it feasible for the provider of the destination service to import and interpret the exported data in order to replicate the original service at low transaction costs. If such data portability proves ineffective in specific contexts, *vertical interoperability obligations* can present a possible but more involved approach to facilitate provider switching, e.g., by enabling service portability. However, this then requires an assessment of the technical feasibility as well as the costs associated with such interoperability obligations in the specific context of consideration.

In general, we are **sceptical that an unconditional interoperability regulation regime for data processing services would be desirable** given the economic and technical characteristics of data processing services markets outlined in Section 2. This scepticism is reinforced by the broad scope of Art. 26 (2) and (3) which would cover all data processing services at the PaaS and SaaS layer, which spans across numerous heterogeneous markets, industries, and service types. To avoid overregulation and adverse side effects (such as relatively higher burdens on smaller firms and less entrepreneurial freedom for new market entrants), mandatory interoperability regulation should in our view only be imposed if data portability proves ineffective in a specific market or if justified by the identification of market failures. In such cases, interoperability regulation should be tailored to the specific market of data processing services and their respective characteristics. Also, given the economic characteristics of data processing services markets, the simple lack of common market-driven standards would not suffice per se to justify broad interoperability regulation from an economic perspective.

This is not to say that interoperability should not and cannot play an important and valuable role in markets for data processing services. In particular, **voluntary standardisation initiatives** themselves can be feasible, especially if several competitors join such an initiative to compete with incumbent ecosystems of data processing services. By offering customers the option to easily combine services of different providers, by allowing them to move services across platforms and infrastructures of different providers and by removing technical risks of vendor lock-in, **interoperable systems of data**

²⁵⁵ Netherlands Authority for Consumers and Markets (2022). Proposal to enhance the draft Data Act. Based on a national market study into Cloud services. <https://www.acm.nl/system/files/documents/proposal-to-enhance-the-draft-data-act.pdf>



processing services can promise customers additional business value over closed ecosystems of data processing services in such situations. Hence, there also exist market-driven incentives that can support the emergence of open standards for interoperable data processing services even when markets are characterised by a “competition for the market” dynamic. In addition, **voluntary standardisation among stakeholders is likely to involve much lower coordination and transaction costs** than in the case of mandatory standardisation. Hence, open interoperability standards may also emerge as a competitive response and alternative to proprietary offerings and closed ecosystems of data processing services.

4.2.2 Compatibility with open interoperability specifications or European standards for interoperability

Yet, Art. 26 (3) requires any provider of a data processing service at the PaaS and SaaS layer to ensure **compatibility with open interoperability specifications or European standards for interoperability**. The criteria and development of such interoperability standards are further detailed in Art. 29. In particular, Art. 29 (4) empowers the European Commission to adopt delegated acts to publish the “reference of open interoperability specifications and European standards for the interoperability of data processing services”, such that these would become binding interoperability standards in accordance with Art. 26 (3). To this end, the Commission may also request “one or more European standardisation organisations to draft European standards applicable to specific service types of data processing services” based on Art. 29 (3).

Next to our concerns about the unconditional scope of the mandatory interoperability regulation rules in the DA, we are **sceptical about the effectiveness of the envisioned processes to establish mandatory standards** for a seamless multi-vendor cloud environment and **fear that mandatory interoperability regulation could inadvertently promote further market concentration to the detriment of smaller providers of data processing services and potential market entrants** if mandatory standards are not tied to an assessment of specific market characteristics or subject to additional conditions.

In our view, standardisation processes in practice can only work bottom-up and not top down, due to the technical expertise and industry knowledge required. In consequence, this implies that established service providers with large services ecosystems and strong market positions will have a strong influence on what the final (mandatory) standards will look like. Moreover, the potentially most innovative voices may not be participating in the standardisation process at all, as they may not yet have entered the market at all. In consequence, **such standardisation processes could run the risk of tailoring standards to the benefit of established providers, while reducing the potential for differentiation for competitors**. From a competition perspective, this is especially problematic as Art. 26 (3) of the DA would legally require all service providers to adopt such a standard if their service is deemed to be of the same service type as the specified standard. Whereas such risks can be mitigated by procedural arrangements that would require standardisation organisations to hear from smaller providers, such arrangements themselves can be prone to further complicating and slowing down the standardisation process.



In addition, **processes for mandatory standardisation would face significant technical challenges**, due to the technical status quo of the data processing services landscape as outlined in Section 2. On the one hand, there is a large variety of heterogeneous services, especially at the PaaS and the SaaS layers of the data processing services stack, which makes it **already difficult to classify services of the same service type that should be subject to a common mandatory standard** (see above). Even in cases where services provide common functionalities of the same service type, most services are likely to be differentiated with respect to other functionalities (think of different features in SaaS services such as Microsoft Teams and Slack). This raises **questions about the feasibility to specify a common standard for heterogeneous services and the value of partial standardisation in practice**. On the other hand, most data processing services are still evolving and are subject to rapid innovation cycles. In contrast, standardisation procedures between parties with diverging interests have proven to take a long time and are difficult to update once they are adopted.²⁵⁶ Therefore, **mandatory standards run the risk of slowing down innovation and eliminating the emergence of new services** that do not comply with the existing standards. If, instead, a standard were only adopted under the DA if all service providers would voluntarily agree, the benefit of additional regulation seems limited, to begin with. Such a regulatory approach based on unanimous agreement also entails the risk that any service provider could “veto” a standard by non-cooperation, which is likely to render convergence to a final mandatory standard unfeasible.

Despite these costs and challenges of mandatory interoperability regulation, **there could be cases where the benefits of interoperability regulation outweigh the costs**. To identify such cases a more in-depth assessment of the costs and benefits of mandatory interoperability standards in the specific context of the data processing services under consideration is required. Therefore, **while mandatory interoperability regulation can represent a suitable tool to promote the goals of the DA, the introduction of mandatory interoperability standards should be tied to additional conditions**. In particular, we suggest that mandatory interoperability regulation should be considered if data portability is found to be ineffective in facilitating customer switching in specific markets or if interoperability rules can mitigate identified market failures (see Recommendation 4 in Section 5).

²⁵⁶ The standardisation of the “Rich Communications Standard”, a communication protocol for a richer mobile text-messaging service intended to replace SMS can serve as an anecdotal example for the complexity of standardisation processes even when providers’ interests are generally aligned and the focus is on a specific service. See, e.g., Shim, Y., Lee, H., & Fomin, V. (2019). What benefits couldn’t ‘Joyn’ enjoy?: The changing role of standards in the competition in mobile instant messengers in Korea. *Technological Forecasting and Social Change*, 139, 125-134.



5. POLICY RECOMMENDATIONS

With respect to rules for data processing services, the DA mixes data portability and interoperability goals. To facilitate switching between data processing services it is important that data portability ensures customers' ability to export and import necessary data and metadata at the time of switching. In contrast, a general interoperability regime aimed at establishing a seamless multi-vendor cloud environment requires standardised interfaces of a wide variety and number of services to support continuous data flows. With respect to individual obligations, the DA should be clearer about the goals and purposes that should be achieved by the respective rules.

In this context, our main recommendation is that **the focus of the DA should be on strengthening data portability** and facilitating the switching between providers of data processing services by reducing barriers to switching and by lowering the transaction costs of customers. In this vein, **we agree on the essence of those proposed rules in the DA that aim to promote and facilitate effective data portability**. We believe that simplicity and clarity of these rules are of utmost importance for the DA's effectiveness. Therefore, we make specific recommendations on how to revise the functional equivalence criterion. Moreover, as a symmetric, horizontal regulation the main objective of the DA should be on establishing **a general framework of basic rules** that also considers regulatory costs and potential side effects on service providers of different size and variety. We are therefore more sceptical about the unconditional and potentially wide scope of mandatory interoperability regulation envisioned by the DA and recommend that **interoperability regulation and mandatory standards in the context of the DA should be tied to further justifications based on an assessment of specific market conditions and the effectiveness of data portability in the respective market**.

Recommendation 1: Keep obligations that ensure effective data portability (Art. 24, Art. 25), but remove the general right of customers to terminate any contractual agreement (Art. 23 (1) (a))

To this end, the **gradual withdrawal of switching charges** in Art. 25, a **mandatory maximum transition period** as specified by Art. 24 (1) (a) and the **definition of a minimum scope of portable data** as stated in Art. 24 (1)(b) represent suitable and targeted instruments. Switching charges here should refer to any extra charges tied to the switching process. Thus, customers still need to bear costs for regular performances of the service provider as agreed upon in their service contract. Obligations on the maximum transition period and the minimum scope of portable data should be **complemented by safeguards against anti-competitive use**. With respect to a maximum transition period, the customer and the destination service provider should bear the burden of proof that they have completed their own necessary actions to allow for a timely switching. With respect to the minimum amount of portable data, the original service provider should be allowed to exclude selected data points on an exceptional basis if it can demonstrate that such data will reveal IP protected information or trade secrets.

In contrast, a general maximum notice period for the termination of any contractual agreement as introduced by Art. 23 (1) (a) could have significant unintended economic effects and could even be detrimental to the interest of smaller providers of data processing services. In consequence, such a general limit on the freedom to conduct a business runs the risk of impeding competition and innovation in these markets and could indirectly hurt even customers of data processing services.



Thus, **we suggest removing Art. 23 (1) (a) on customers' general ability to terminate a contractual agreement of the service within 30 days.** Instead, a special right of termination in case of price increases or non-fulfilment of the contract should be sufficient to safeguard customers against potential exploitation of vendor lock-in.

Recommendation 2: Make Art. 26 (4) and Art. 24 (1) (b) the default data portability requirement for all data processing services

To ensure effective data portability, the DA should be foremost concerned with the scope as well as the quality and completeness of the exportable data. Therefore, we suggest that the obligation in **Art. 26 (4) should be the default requirement for all portable data** specified by Art. 24 (1) (b), and accordingly, **all exportable data should be made available "in a structured, commonly used and machine-readable format"**. This should ensure that a customer is able to export all data and metadata required to replicate the service at the destination service and guarantee that the ported data is available in an accessible and readable format that can be imported by the provider of the destination service. Given that these mandatory obligations would apply symmetrically to all data processing services, this represents a significant step beyond the current self-regulatory regime.

Recommendation 3a: Replace the functional equivalence criterion with a hypothetical "service replication test" that refers to the original service provider instead of the specific destination service

Related to the previous recommendation, we propose to significantly **revise the definition of functional equivalence and reconsider its applicable scope**. The functional equivalence criterion as defined in the DA proposal can be viewed as an additional safeguard for ensuring that exportable data is of sufficient quality and completeness to allow for the replication of the original service at the same output, performance, and quality level at the destination service provider. While the intention behind this is laudable, we believe that **making the original service provider responsible for actions and outcomes of another service provider stretches beyond the due responsibilities of the original service provider, possibly creates adverse economic incentives and would be difficult to enforce coherently in practice**. Moreover, such an implementation is likely to raise frequent controversies between the involved service providers about who would be responsible for a lack of service quality or performance, which in the extreme case could lead to excessive litigation. In consequence, this would complicate rather than simplify switching between data processing providers.

In addition, the functional equivalence criterion would raise frequent questions about what would qualify as a service of the same service type and what services would fall outside of this scope. This creates additional uncertainty for both the original service provider and the destination service provider. Therefore, we suggest **replacing the current functional equivalence criterion with a (hypothetical) "service replication test" that refers to the original service provider instead of the destination service provider** to ensure the quality and completeness of the exportable data. According to this revised functional equivalence test, the original service provider shall ensure that the exportable data is sufficient to replicate the original service at the same output, quality and performance within the environment of the original service provider without the need for additional internal data. In other words, the test ensures that the data, which can be exported from the original service provider could, in principle, be imported again at the same service provider and the customer



would end up with a replication of the same service as before. **This approach has two major advantages over the current DA proposal: i) service providers are not held responsible for the actions and conduct of other service providers and ii) there is no need for a general classification of service types for all data processing services.**²⁵⁷ Overall, this would significantly simplify the implementation of the functional equivalence test and remove the inherent problem of requiring the original service provider to guarantee performances or outcomes that are under the control of the destination service provider. Moreover, it would allow customers to port data in sufficient quality and completeness to services that are not of the same service type, which may be a frequent use case, depending on how narrow a service type would ultimately be defined.

A potential drawback of this approach may be that if exported data was only available in a proprietary format, such data may be readable and processable by the original service provider but not by other service providers. In general, this should be prevented by making Art. 26 (4) a default requirement, which requires exportable data to be in a “commonly used and machine-readable format” format (see Recommendation 2). This could be further strengthened by **clarifying that exportable data must be in a non-proprietary format** that is readable and processable for service providers other than the original service provider.

The simpler “service replication test” could not only be applied to services at the IaaS layer, but could serve as **an approach that can universally be applied to all data processing services** (spanning across IaaS, PaaS, and SaaS layers) in order to ensure quality and completeness of the exportable data. In consequence, this would remove the need to distinguish IaaS services from PaaS services, which has been acknowledged to be very difficult if not unfeasible in practice.²⁵⁸

Recommendation 3b: In case the original functional equivalence criterion is maintained, clarify that the original service provider can only be held responsible for its own best effort

If, contrary to the previous proposal, the original concept of functional equivalence was maintained in the DA, Art. 2 (14) and Art. 26 (1) should be carefully **rephrased such that the original service provider shall only be subject to undertaking its best effort** in supporting the customer to replicate the service at the destination provider at the same output, quality, and importance. It should be clarified that the original service provider cannot *ensure* such outcomes at the destination service provider. In this case, the application of the functional equivalence criterion should remain limited to the IaaS layer, as the heterogeneity of PaaS and SaaS services make an assessment of functional equivalence and classification of the same service type even more difficult.

²⁵⁷ In its spirit, the proposed test can be compared to the “equally efficient operator test” for a margin squeeze, which bases the test for a possible margin squeeze on a dominant firms’ own retail operations rather than on the retail operations of the competing firm that would actually rely on the access input of the dominant firm. See Notice on the application of the competition rules to access agreements in the telecoms sector [1998] OJ C 265/2, para 117.

²⁵⁸ ACM market study, *supra* note 12.



Recommendation 4: Mandatory interoperability standardisation and interventions based on delegated acts should be tied to the ineffectiveness of data portability in specific markets or the identification of market failures (Art. 26 (3), Art. 29)

Finally, we view **mandatory interoperability standardisation** as an approach that should be considered if either i) data portability and the obligations described above are found to be ineffective to facilitate customer switching in a specific data processing services market or ii) if other market failures are identified. Thus, Art. 26 (3) and Art. 29 should be amended accordingly to qualify that **mandatory compatibility with interoperability specifications and the publication of delegated acts should be subject to one of the two conditions** described above.

Such an amendment would clarify that effective data portability is the preferred general approach to address obstacles to customers' ability to switch between data processing services. Given the broad scope of the DA rules on switching between data processing services, which spans across a large variety of heterogeneous services, data portability rules are much more scalable than mandatory interoperability standardisation. Moreover, we fear that even for specific markets mandatory standardisation efforts could prove too slow to keep up with the highly dynamic and quickly evolving markets and technologies of data processing services. Therefore, universal obligations to comply with interoperability standards run the risk of endangering innovation in these fast-moving markets. These costs should be assessed and compared with the expected benefits of interoperability regulation. Moreover, as outlined in Section 4, we are sceptical that unconditional interoperability regulation can effectively address the underlying economic issues in the markets for data processing service. Finally, market forces could promote open interoperability standards based on voluntary approaches, which would have several advantages over mandatory interoperability regulation.

At the same time, our proposed amendments of Art. 26 (3) and Art. 29 would still allow the European Commission to revert to **mandatory interoperability standardisation** if data portability proved ineffective in specific markets or if other market failures were identified. Thus, the DA would retain mandatory interoperability standards as a "coercive" regulatory instrument and maintain the current "carrots and sticks" approach to push providers of data processing services to facilitate customer switching. However, it is important to note that the lack of market-driven convergence to a common standard should not be considered a market failure that would warrant mandatory interoperability standardisation per se. Given the economic characteristics of data processing services markets, it is likely that service providers will frequently compete for a specific market segment based on incompatible standards. Whether mandatory interoperability standards can indeed improve outcomes in such markets depends on **the actual competitiveness of these markets and the costs of interoperability regulation and mandatory standards**, which should therefore both be assessed ex-ante.

If, in fact, competition issues are considered a major problem in markets for data processing services²⁵⁹, competition law and sector-specific regulation following an asymmetric approach are the

²⁵⁹ See e.g., the recent initiations of investigations into cloud services markets by national regulators: ACM market study, *supra* note 12; Ofcom (2022). Ofcom to probe cloud, messenger and smart-device markets. <https://www.ofcom.org.uk/news-centre/2022/ofcom-to->



more appropriate and more targeted approaches to address these issues. In this vein, one-off data portability should be established by the DA as the general rule for all providers of data processing services, whereas potential additional regulatory interventions, including mandatory compliance with standards, should be subject to an assessment of a markets' competitiveness and a provider's market power. Relying on the DA for such interventions without additional safeguards, would otherwise entail the risk that smaller firms would be disproportionately affected by regulatory obligations, which may even lead to heightened barriers for competition. In general, data portability has the potential to promote competition in data processing services markets, but its effectiveness hinges crucially on rule implementation and enforcement. This further calls for the symmetric regime of the DA to be as simple and clear as possible in order to avoid lengthy implementation procedures, regulatory uncertainty and ensuing litigation.

With respect to competition issues, it is important to note that the Digital Markets Act (DMA) designates cloud computing services as a core platform service and imposes data portability obligations on gatekeepers.²⁶⁰ Hence, there are considerable **overlaps between the DA and the DMA with respect to data processing services, which also raises questions about the consistency of these rules**. Remarkably, several obligations in the DMA seem less demanding than corresponding rules in the DA, although the DMA specifically targets larger gatekeeper firms to address market contestability and competition issues.²⁶¹ In particular, data portability obligations for cloud computing services under the DMA do not explicitly refer to metadata, which is included in the default minimum scope stipulated by the DA.²⁶² Moreover, the DMA does not consider interoperability obligations with respect to cloud computing services. In contrast, the DMA may go beyond the DA in requiring gatekeeper providers of cloud computing services to provide business users with “high-quality, continuous and real-time access” to their data, as part of the DMA's obligation on data portability.²⁶³ Ideally, **these overlaps and inconsistencies call for clarification and revision of the DMA rules on cloud computing services**. As a second best, the DA itself may clarify how its rules are supposed to interact with the DMA's provisions on cloud computing services from gatekeeper firms.

[probe-cloud,-messenger-and-smart-device-markets](https://www.autoritedelaconcurrence.fr/en/communiqués-de-presse/autorite-de-la-concurrence-starts-proceedings-ex-officio-analyse-competition); Autorité de la concurrence (2022). The Autorité de la concurrence starts proceedings ex officio to analyse competition conditions in the cloud computing sector.
<https://www.autoritedelaconcurrence.fr/en/communiqués-de-presse/autorite-de-la-concurrence-starts-proceedings-ex-officio-analyse-competition>

²⁶⁰ Regulation (EU) on contestable and fair markets in the digital sector (Digital Markets Act) [2022] OJ L 265/1, Article 2 (2) (i).

²⁶¹ Ibid, Recital 7.




²⁶² Ibid, Article 6 (9) and (10).

²⁶³ Ibid, Article 6 (10).

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