cerre Centre on Regulation in Europe

EUROPEAN PROPOSAL FOR A DATA ACT

A FIRST ASSESSMENT

ASSESSMENT PAPER

July 2022

Giuseppe Colangelo

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, Huawei, Institut National de l'Information Géographique et Forestiére, and Vodafone. However, they bear no responsibility for the contents of this report. The views expressed in this CERRE report are attributable only to the authors in a personal capacity and not to any institution with which they are associated. In addition, they do not necessarily correspond either to those of CERRE, or of any sponsor or of members of CERRE.

info@cerre.eu – www.cerre.eu

TABLE OF CONTENTS

ABOUT CERRE

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

CERRE's added value is based on:

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

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

ABOUT THE AUTHORS

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).

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 Assessment[2], the DA complements two other major instruments shaping the European single market for data, such as the Data Governance Act[3] 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 sharing[5]. 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 individuals[6], the Regulation on the free flow of non-personal data facilitated business-to-business data sharing practices[7], the Open Data Directive aimed to put government data to good use for private players[8], 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 spaces[9]. Sector-specific legislations on data access have also been adopted or proposed to address identified market failures, such as in the automotive[10], payment service providers[11], smart metering information[12], electricity network data[13], intelligent transport systems[14], renewables[15], and energy performance of buildings[16].

[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.
[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.

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) applications[17]. 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 services[18]. The issue of (limited) access to machine-generated data has been raised in the 2017 Communication on the European Data Economy[19], 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 data[20]. 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 intervention[21].

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 development[22]. 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 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 users[23]. Against this backdrop, interoperability is deemed to play a crucial role in improving consumer choice and preventing lock-in into providers' products.

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

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.

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 - SMEs**[25]**) 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 data[26]. 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 data[27]. 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 data[28]. Legal uncertainties regard the question of the applicability of the Database Directive to machine-generated data[29] 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 consent[30]. 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 innovation[31]. 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 holder[33]. 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 terms[34].

Furthermore, although data is essential for driving evidence-based policymaking, it is mainly created outside of the public sector[35]. 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 possibilities[36].

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 market[37]. **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 players[39]. 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 dynamics[40].

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 services[41].

---

[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 actors[43]. 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 services[44]. 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 services[46].

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 power[47]. 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 position[48]. 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 unfair[49].

[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 rights[50], and a right to share the generated data with third parties[51], 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 users[52].

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 players[53]. Therefore, users' empowerment apparently prevails over other goals or at least indirectly incorporates them[54]. 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 originates[55]. 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 fulfilled[56]. 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 agreement[57]. 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 data[58].

---

[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 default[59], 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 possible[60]. 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 available[61].

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 it[62]. 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) terms[63]. 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 precedence[64]. 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 terms[65], **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/edpbedps-joint-opinion/edpb-edps-joint-opinion-22022-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 data[68].

Finally, for the same reason, as already mentioned, although the user is entitled to use the data for any lawful purpose[69] and the third party receiving data can process such data for the purposes and under the conditions agreed with the user[70], their rights are limited to uses which do not compete with the product from which data originates[71].

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 products[72]. 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 flavour[74], 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 data[75] and rebalancing their bargaining power vis-à-vis large players[76].**

Under this logic, with regard to the former goal, **micro and small enterprises are exempted** from abiding by the data sharing obligation[77]: given the current state of technology, it is considered overly burdensome to impose over them design obligations[78]. Micro and small enterprises are also exempted from the obligation to provide public sector bodies and EU institutions data in situations of exceptional need[79]. 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 recipient[80]. 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 indirectly[81], given their "unrivalled ability" to acquire data[82]. 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 banks[84]. 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

[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.

services on secondary markets. Therefore, if current and future competitive risks are already under 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 stake[85].

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 terms[86]. 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 dealing[87].

To provide a yardstick to interpret such unfairness test for B2B relationships[88], 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

[85] Kerber, supra note 68, 18.
[86] Ibid., Recital 51.
[87] Ibid., Article 13(2).
[88] Ibid., Recital 55.

own activities on access to data controlled by another enterprise[89]. In a similar vein, the Italian Annual 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 data[90].

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 chain[91] 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

[89] GWB Digitalization Act (2021), Section 20.
[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.

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 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 copyright[92]. 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 DA[93].

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 industry[94]. 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

[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.

IoT[95]. Therefore, the Database Directive is among the legal instruments that was expected to be revised in light of the DA[96].

The envisaged solution raises some doubts[97]. 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 fulfilled[98]. However, as pointed out by several IP scholars[99], 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 law[100].

Promoting data access and sharing also requires the "clarification" of certain provisions of the Trade Secrets Directive[101]. 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 invest[102], 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 parties[103]. 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 secret[104]. However, Article 4(3) and Article 5(8) are at odds with the provision included in Article 8(6), which instead, regardless of any

[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.

[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 Agonon 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).

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.

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 cases[105]. 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 request[106].

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 charge[108], 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 body[109].

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 Supervisor[110].

[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 issues[111]. 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 companies[112]. Nonetheless, the DA finds that the self-regulatory approach promoted by such Regulation has been largely ineffective so far[113].

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 type[115].

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 gatekeepers[116]. However, it is worth noting that, unlike the DA, the DMA does not limit the freedom of contract of gatekeepers[117].

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 interoperability[119]. To this aim, the Commission can mandate the use of European standards for interoperability or open interoperability specifications for specific service types[120].

It is not immediately obvious why IaaS are excluded from the technical duties about open interfaces and interoperability specifications[121]. 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 market[122].

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 agreement[124]. 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 requirements[125].

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 scope[126].

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 countries[127]. 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 standardisation[128]. 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 that[129]:

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 standards[130]. 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 contracts[131].

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 users[133]. Further, the majority of participants in the sector inquiry expressed the need to prioritise standardisation to guarantee higher levels of interoperability[134].

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 differentiation[135].

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 DA[136]. 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 competence[137]. Therefore, in contrast with the policy choice adopted in the DMA and partially in the Digital Services Act[138], but in line with the Data Governance Act[139] and the Artificial Intelligence Act[140], 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 authority[142], 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.

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