SSOAR

Open Access Repository
www.ssoar.info

Position Paper regarding Data Act (Proposal of the European Commission, 23.02.22)

Efroni, Zohar; Hagen, Prisca von; Völzmann, Lisa; Peter, Robert; Sattorov, Mariam

Erstveröffentlichung / Primary Publication
Stellungnahme / comment

This work has been funded by the Federal Ministry of Education and Research of Germany (BMBF) (grant no.: 16DII121, 16DII122, 16DII123, 16DII124, 16DII125, 16DII126, 16DII127, 16DII128 - "Deutsches Internet-Institut").

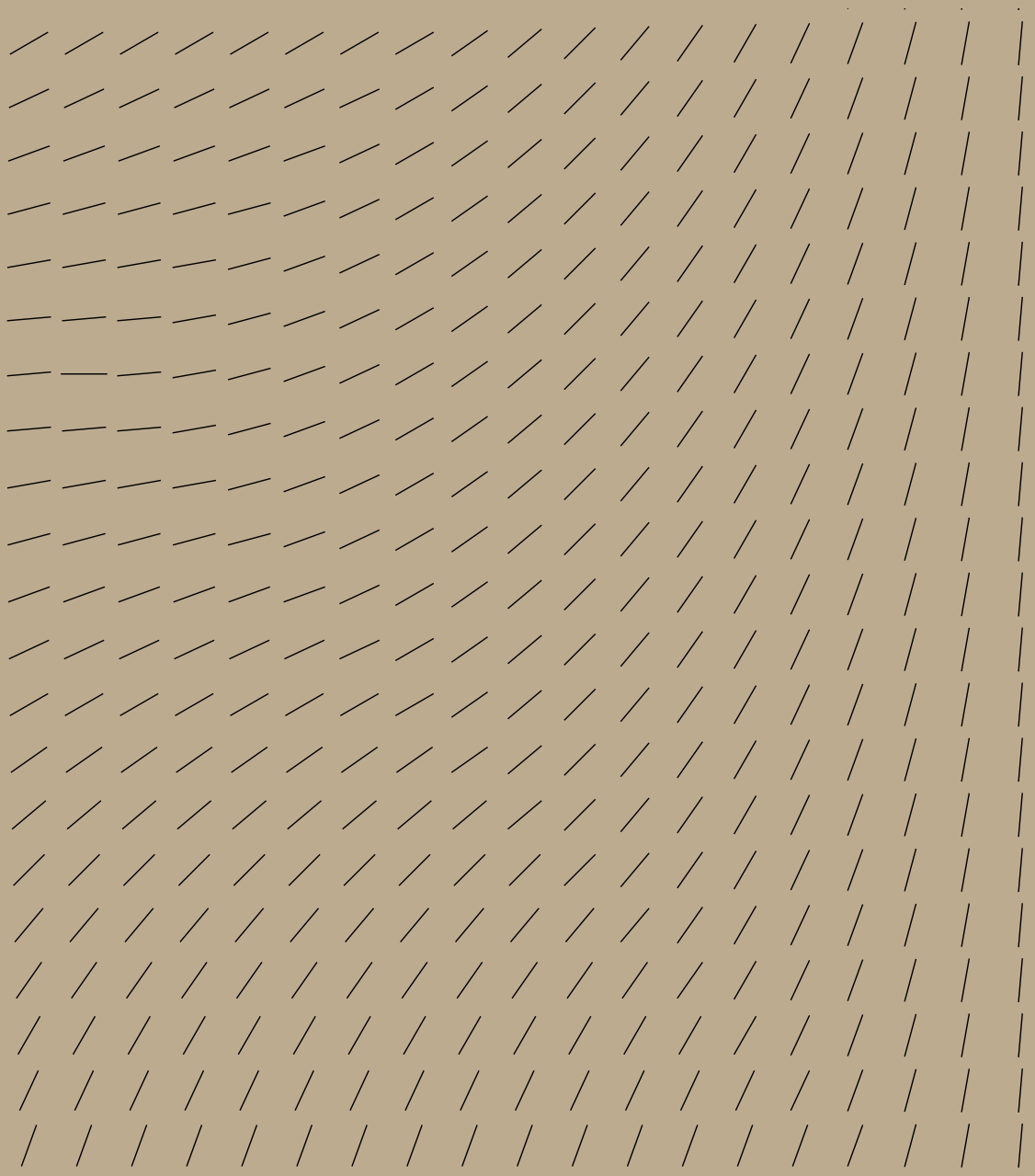
Empfohlene Zitierung / Suggested Citation:
Efroni, Z., Hagen, P. v., Völzmann, L., Peter, R., & Sattorov, M. (2022). *Position Paper regarding Data Act (Proposal of the European Commission, 23.02.22).* (Weizenbaum Policy Paper, 2). Berlin: Weizenbaum Institute for the Networked Society - The German Internet Institute. https://doi.org/10.34669/WI.WPP/2

Nutzungsbedingungen:
Dieser Text wird unter einer CC BY Lizenz (Namensnennung) zur Verfügung gestellt. Nähere Auskünfte zu den CC-Lizenzen finden Sie hier:
https://creativecommons.org/licenses/by/4.0/deed.de

Terms of use:
This document is made available under a CC BY Licence (Attribution). For more Information see:
https://creativecommons.org/licenses/by/4.0

gesis
Leibniz-Institut
für Sozialwissenschaften

Mitglied der
Leibniz-Gemeinschaft



JUNE 2022

Weizenbaum Institute for the Networked Society

Position Paper regarding Data Act

(Proposal of the European Commission, 23.02.22)

Imprint

Authors

Zohar Efroni \ zohar.efroni@rewi.hu-berlin.de
Prisca von Hagen \ prisca.von.hagen@rewi.hu-berlin.de
Lisa Völzmann \ voelzmann@rewi.hu-berlin.de
Robert Peter \ robert.peter@weizenbaum-institut.de
Mariam Sattorov \ sattorom@hu-berlin.de

DOI 10.34669/WI.WPP/2

Editors: The Managing Board members of the Weizenbaum-Institut e.V.
Prof. Dr. Christoph Neuberger
Prof. Dr. Sascha Friesike
Prof. Dr. Martin Krzywdzinski
Dr. Karin-Irene Eiermann

Hardenbergstraße 32 \ 10623 Berlin \ Tel.: +49 30 700141-001
info@weizenbaum-institut.de \ www.weizenbaum-institut.de

For inquiries regarding this position paper please contact Zohar Efroni at: zohar.efroni@hu-berlin.de

The Weizenbaum-Institut e.V. adheres to the Code of Conduct of the EU Transparency Register. Its ID in the register is: 194885445254-71

COPYRIGHT: This policy paper is available open access and is licensed under Creative Commons Attribution 4.0 (CC BY 4.0): https://creativecommons.org/licenses/by/4.0/

WEIZENBAUM-INSTITUT: The Weizenbaum Institute for the Networked Society - The German Internet Institute is a joint project funded by the Federal Ministry of Education and Research (BMBF) and the State of Berlin. It conducts interdisciplinary and basic research into the transformation of society through digitization and develops design options for politics, business and civil society.

This work has been funded by the Federal Ministry of Education and Research of Germany (BMBF) (grant no.: 16DII121, 16DII122, 16DII123, 16DII124, 16DII125, 16DII126, 16DII127, 16DII128 – “Deutsches Internet-Institut”).

Table of Contents

Preliminary note 4

Executive Summary 5

I. General Observations 6

A. Goals of the Data Act 6

B. Justifications for a Regulatory Intervention 7

\ 1. Normative Justification 7

\ 2. Economic Justification 7

C. Legal Instruments (Means) and Legal Definitions 9

II. Access Rights to Data 10

A. The Position of Data Users 10

B. The Position of Data Holder 11

C. The Position of Data Recipients and Third Parties 14

D. Interface with the Protection of Trade Secrets 16

III. Contracts Concerning the Use and Transfer of Data 18

A. Requirements Cconcerning Contracts and Ttheir Content 18

B. Specific Restrictions on Contractual Provisions 18

\ 1. Concept(s) of Ffairness in the Data Act 18

\ 2. Non-Ddiscrimination 21

\ 3. Compensation 21

C. Dispute Settlement 22

IV. Data Portability, Switching between Providers, Interoperability 23

A. “Data Portability” Right 23

B. Switching between Providers 24

C. Interoperability 24

V. Business-to-Government (B2G) Data Transfer 25

A. Scope and Content 25

B. Safeguards against Misuse by Public Bodies 25

C. Access Right for Fulfilling a Specific Task in the Public Interest (Art. 15(c) DAP) 26

VI. Recommendations 28

Preliminary note

As members of the Weizenbaum Institute, we greatly appreciate the opportunity to comment on the European Commission's Data Act proposal.

About the Weizenbaum Institute

The Weizenbaum Institute conducts interdisciplinary and basic research into societal transformation through digitalisation developing design options for policymakers, business, and civil society. The goal is to better understand the dynamics, mechanisms, and implications of digitalization. To this end, the Weizenbaum Institute investigates the ethical, legal, economic, and po-litical aspects of the ongoing digital transformation. The Weizenbaum Insti-tute is a research association funded by the German Federal Ministry of Edu-cation and Research (BMBF) comprising five universities - Freie Universität Berlin (FU Berlin), Humboldt-Universität zu Berlin (HU Berlin), Technische Universität Berlin (TU Berlin), Universität der Künste Berlin (UdK Berlin), Universität Potsdam - as well as the Fraunhofer Institute for Open Communica-tion Systems (FOKUS) and the Berlin Social Science Center (WZB). The central administration and legal representation are carried out by the Weizenbaum-Institut e.V., which, as the coordinator of the association, is responsible for the overarching areas of public relations, knowledge transfer with poli-cymakers, business and civil society, networking and internationalization, as well as academic career development.

Executive Summary

With the publication of the Data Act proposal in February 2022, the European Commission approached an important milestone in the implementation of the data strategy it had announced two years earlier. The legislative proposal includes a package of measures that are supposed to make more IoT data available to data-driven enterprises. The legislation is expected to bring about more competition in the aftermarkets for IoT devices and related services, more value generation from such data and more technological innovation enabled by access to data.

The most innovative and far-reaching regulative instrument applied in this context is, without doubt, the mandatory access rights regime that would facilitate flow of data from private (mostly large) enterprises to other (mostly smaller) enterprises and to the public sector. This regime is accompanied by rules about the necessity and content of commercial contracts that define private entitlements concerning access to as well as use of co-generated IoT data, including statutory requirements concerning fairness, non-discrimination and compensation.

This Position Paper primarily addresses the access rights regime and its accompanying rules focusing on contracts regarding access to data. It also briefly touches upon the provisions on data portability, rules for switching between providers and trade secrets. We conclude that the consolidated impact of the access rights regime on IoT device manufacturers, third parties and the data economy at large is hard to predict. At the same time, we argue that the legal positions and entitlements the Data Act would create require further scrutiny and that there is certainly room for clarifications and improvements in the legislative proposal. The analysis concludes with several specific recommendations.

I. General Observations

A. Goals of the Data Act

The Data Act is a significant component in the implementation of the European data strategy announced by the European Commission in February 2020.[1] The central problem identified in the Explanatory Memorandum to the Data Act Proposal (DAP) is the fact that, although the volume of data generated by humans and machines is increasing exponentially, **most of the data remain underused**. The main reasons for this underuse are said to be low trust, conflicting economic incentives and technological obstacles.[2]

Based on this observation, one of the general aims of the Data Act is to **ensure fairness** in the allocation of value from data among economic actors and to foster broader access to and use of data. Specific objectives of the Data Act toward this end include the **facilitation of data access and use** while at the same time **preserving incentives** to invest in value-generating enterprises that rely on data, providing the **public sector** access to data in private hands where there is an exceptional data need, the facilitation of **switching** between data processing services and establishing rules for **interoperability** and technical standards.

The Impact Assessment accompanying the DAP offers a comprehensive analysis of the problems at hand and it compares between intervention approaches of various intensity. The Data Act introduces a package of measures that follow an **intermediate intervention** approach ("Policy Option 2").[3] This approach includes measures **empowering customers**[4] that are using connected products and related services regarding co-generated data and acting against **unilaterally imposed contractual arrangements** that contain unfair or abusive clauses concerning access and use of co-generated data.

The Commission essentially brings forward two types of justifications for the regulatory intervention in the operation of markets and the freedom of contracts – one is **normative** in nature, and the other is **economic**. These justifications are, however, intertwined and

[1] European Commission, A European strategy for data, COM (2020) 66 final 19.2.2020.

[2] European Commission, Proposal for a regulation of the European parliament and of the council on harmonized rules on fair access to and use of data (Data Act), COM (2022) 68 final, 23.2.2022, Explanatory Memorandum, p. 1.

[3] Commission Staff Working Document, Impact Assessment Report Accompanying the document Proposal for a Regulation of the European parliament and of the council on harmonized rules on fair access to and use of data (Data Act) SWD (2022) 34 final, 23.2.2022, p. 43 ff.

[4] Neither the Impact Assessment nor the DAP clearly distinguish between individual, human consumers and companies located on the customer side of a B2B relationship with a data holder. Hence, the term "B2C" might cause confusion in the context of the Data Act.

reflect a strong **market-orientated, pro-competition and user-empowering approach**, as described below.

B. Justifications for a Regulatory Intervention

1. NORMATIVE JUSTIFICATION

The normative justification emphasizes the need to intervene in cases of **power imbalance** between economic actors, to support smaller enterprises in their dealings with incumbent players, to curb **discriminatory and unfair** contractual arrangements, to create more trust in sharing data and to enhance **legal certainty** regarding the utilization and transfer of data. Some of the most noteworthy concepts developed and implemented in the DAP and its accompanying documents are the "**unfairness test**", the specific prohibition on **discriminatory** terms and **price** controls. All these instruments manifest a direct, albeit limited, **intervention in the freedom of contracts** and the ability of commercial actors to shape agreements according to their individual interests, predominantly in the **B2B** context.

Fairness is indeed a central theme in the Data Act, so much so, that it even made it to the title –stating that the Data Act is a regulation "on harmonized rules on fairness and use of data". Fairness, from a legal-regulatory point of view, is a challenging concept, especially in the context of private contract law. Someone's personal view on what is (commercially) fair or unfair almost necessarily encapsulates value judgements that are often driven by a desire to help the weaker or more vulnerable party. Further, a fairness evaluation depends on the circumstances of a given case (or a category of cases), and as **a regulatory principle for free markets**, it resists being confined to a general, objective legal standard.[5] The unfairness test as well as the non-discrimination and compensation rules are discussed in more detail in Section III.

2. ECONOMIC JUSTIFICATION

The principal economic/market justification for regulatory intervention rests on the assumption that lowering barriers for data access and releasing more data currently held exclusively by private entities into data markets will **have a significantly positive effect on innovation and the economy at large**. The Explanatory Memorandum (p. 9) as well

[5] For a recent attempt to formulate a legal fairness standard in the context of co-generated data, *see* Cohen/Wendehorst, ALI-ELI principles for a data economy – data transactions and data rights, ELI Final Council Draft, Principle 19 ff, available at https://www.principlesforadataeconomy.org/fileadmin/user_upload/p_principlesforadataeconomy/Files/Principles_for_a_Data_Economy_ELI_Final_Council_Draft.pdf.

as Recitals 6 and 36 DAP reiterate the argument that data are non-rival in access and use. Namely, providing access and use opportunities to others is not supposed to diminish the ability of the data holder to make use of the same data. The assumption is therefore that an increased availability of data to multiple market actors will almost necessarily increase utility, value generation and innovation.

The Impact Assessment predicts that, as a result of more (nonvoluntary) data sharing, not only data recipients will benefit directly from the new rules, but also **manufacturers**[6] of connected products will profit from a wider customer base, despite the additional costs, legal duties and restrictions imposed on them.[7] However, the **consolidated effect on IoT manufacturers** remains quite opaque, and so does the actual impact of nonvoluntary access rights and contractual restriction on their commercial incentives and overall economic strategy and performance. It is conceivable that IoT manufacturers might incorporate the loss of exclusivity/control over co-generated data in the **price of products paid by customers**. Further, it is possible that business models based on **exclusivity over data in lieu of price**, in whole or in part, could lose their viability, assuming that manufacturers will no longer be able to maintain such exclusivity *via* technical and/or legal means.

Notably, the regulative approach reflected in the Data Act does not focus on identifying existing **market failures** and attempting to correct them. Instead, the general approach demonstrates an attempt to facilitate economic activity in the **aftermarket** for data-driven products and related services, enhance competition, create a legal framework that would animate the flow of data to the aftermarket and then regulate, to some degree, under which conditions commercial actors may utilize the data.

The focus of the access rights stipulated in the Data Act (Chapter II and Chapter III) lies on **co-generated IoT data** while implicitly excluding data that is co-generated by using device-independent products and services (such as "pure" software products). It is not immediately clear why the same economic logic should not apply in the latter case as well. One possible answer is that the Commission might wish to first **test the access rights regime in the field of IoT** before expanding it to other segments. Another explanation could be the wish to permit more flexibility in the design of business models that rely on the exclusive use of data instead of charging money for digital content or digital services ("payment with data") outside the realm of IoT.[8]

---

[6] The DAP explicitly recognizes a distinction and a possible identity split between IoT manufacturers and data holder (*see e.g.,* Recital 24). However, the operative provisions of the proposal apply exclusively to "data holders" as defined in Article 2(6) DAP, whereas Article 1(2)(a) merely indicates generally that the Data Act applies *inter alia* to "manufacturers of products".

[7] Commission Staff Working Document, Impact Assessment Report Accompanying the Data Act, p. 44 ff.

[8] Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services, Art. 3(1).

C. Legal Instruments (Means) and Legal Definitions

While implementing "Policy Option 2" (intermediate intervention), the DAP introduces a package of measures to achieve its policy objective. As noted, these include the instruments of nonvoluntary access rights to data and objective-regulatory control over the content of commercial contracts. Terms that do not pass the unfairness test, for instance, are **not binding** for an SME upon which they are imposed (Art. 13(1) DAP), and terms *vis-à-vis* data recipients that do not live up to the "Fair, Reasonable and Non-Discriminatory" (FRAND) requirements are **subject to a dispute resolution mechanism and judicial review**. Mandatory rules supporting data portability and such that enable easy switching between service providers are also included in the package.

Whether this collection of measures will ultimately **lead to the desired results** depends on a number of important questions, including (1) how, to what extent and for which purposes users and data recipients will exercise their data access rights and rights of use; (2) what the overall economic costs and benefits of the new regime are; (3) how IoT manufacturers will react to the new set of duties and restrictions imposed on them, given their diminished capacity to legally protect assets such as trade secrets and certain databases; (4) how smoothly data markets in general, and specific sectors in particular, are able to absorb standard contractual clauses, the unfairness test and FRAND scrutiny; (5) to what extent the new regime will genuinely increase legal certainty, and (6) the overall impact of the system on economic incentives in data markets.

In light of its conceptual, normative and economic assumptions, it is perhaps possible to view the Data Act as a **daring experiment** and pay attention to the **evaluation and review** provision (Art. 41 DAP). Under this provision, the European Commission shall assess this legislation, two years after its date of application, in particular regarding aspects such as other categories or types of data made available, among other things. With these questions in mind, the rest of this Position Paper is dedicated to taking a closer look at the proposal and offering some improvements already during the legislative process.

II. Access Rights to Data

A. The Position of Data Users

A "user" in the terminology of the Data Act is "a natural or legal person that owns, rents or leases a product or receives a services (sic!)" (Art. 2(5) DAP). The regulation aims to secure the right of users to access data generated by their use of a product. Accordingly, upon request (in the absence of direct accessibility), the data holder is obliged to make the data available to users "without undue delay, free of charge and, where applicable, continuously and in real-time" (Art. 4(1) DAP). This provision represents **an unprecedented horizontal regulation** that establishes access rights to **personal and non-personal data** alike, and especially to non-personal data that have, until now, been unattainable due to technical and contractual restrictions. The Data Act hereby **strengthens the legal position of users** *vis-à-vis* data holders.

The user may use the data for "any lawful purpose" (Recital 28 DAP), implicitly including the opportunity to **make the data commercially available to third parties**. The DAP explicitly seeks to enable *via* access rights supplementary services such as repairs and maintenance,[9] which are likely to benefit the user. The user is merely subject to a statutory prohibition not to use the data to develop a competing product (Art. 4(4) DAP). Importantly, the proposal does not contain a provision that **prevents users from receiving data at no cost and then transferring the data to third parties** that otherwise, if directly dealing with the data holder, could be charged for the same data. In fact, it is conceivable that **sophisticated users** will have a **commercial interest** to do so. Such a scenario would shift wealth from data holders to users.

At the same time, access rights under the Data Act do not apply outside the realm of co-generated IoT data, for instance in the case of supplying device-independent digital content and digital services in the meaning of the DCSD.[10] It is reasonable to assume that effective access rights might **diminish the value and monetization opportunities for data holders** as well as the attractiveness of "payment with data" business models, which are explicitly recognized under the DCSD, albeit only with respect to personal data. The prospect of being obliged to pass on data to third parties under the Data Act and the negative impact of this obligation on the value of the data for data holders seem antithetical to such business models.

Importantly, data holders are only allowed to use non-personal data on the basis of a corresponding contract with the user (Art. 4(6) DAP). At first glance, this requirement

[9] European Commission, Data Act Proposal, Explanatory Memorandum, pp. 6, 13.

[10] Directive (EU) 2019/770 of the European Parliament and of the council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services, Art. 2.

promises greater self-determination for users regarding the data. However, a closer inspection reveals possible weaknesses in the scheme. To begin with, it is not unlikely that **data holders will draft the contract unilaterally** and then require the users to accept it as a condition for using the product. The problem is intensified if the contract is too long or too complex for users to effectively understand it and be in the position to object to its terms.

In fact, determining the content of a contract between a data holder and a user, and specifically, the provisions about a **data holder's rights of use**, is left almost entirely to the parties.[11] Quite surprisingly, the DAP does not include a clear prohibition for data holders to insert an exclusivity clause in contracts with users, although such a clause would directly conflict with the obligation to make data available to third parties upon a user's request and would therefore likely be held unenforceable.

This flexibly permits data holders to draft favorable terms, for instance, while addressing situations of multiple users of the same device or data rights of use after the termination of a contract. A contract between a data holder and a user would likely limit the concept of co-generated data to data created through **lawful use** (based on ownership, rental, or lease) of a device. For example, if the device is used by an unauthorized person or for unauthorized purposes, the data generated through such use might not be subject to access rights. Yet, it is **important to ensure that data holders cannot overly limit in this way the application of their obligations** under the Data Act. This might happen if the contract defines "lawful use" of the device too narrowly. **Model contractual terms**, which under the current proposal lack binding force (Art. 34 DAP), could play a more significant role as presently prescribed.

Finally, it is essential to emphasize that that position of a data user might be legally powerful but at the same time of **little practical significance** for many data users having no incentives at all to demand access. If the Data Act is ever going to mobilize a real and sustainable shift in the way large data sets are being shared between enterprises that can derive additional value from that data, this is likely to happen mostly through **third parties offering incentive** to users to issue data access requests under Article 5 DAP (discussed under Section II.C).

B. The Position of Data Holder

To some extent, the position of the data holder is a mirror image of the position of users in their bilateral relationship concerning the use of IoT devices. Data holders are defined as the actors that have the **legal right or obligation**, under the Data Act or national

[11] Perhaps with the exception of the unfairness test under Chapter IV.

legislation implementing Union law, to **make data available** (Art. 2(6) DAP).[12] The definition includes actors (legal or natural persons) that, through **control over the technical design** of the product or related services, can factually make non-personal data available. Data holders are not necessarily the device manufacturers, although this is often the case. Specifically, there is no clear distinction between **product manufacturers** and parties with legal or factual access control capacities that are not manufacturers. The assumption is that a product manufacturer with *de facto* access control over co-generated data will typically fall under the definition, but it is less clear whether **transferring factual control** from a manufacturer to a business partner effectively transforms the latter into a data holder.[13] To the extent that the position of a data holder is fairly easily transferrable between device makers and other commercial actors, we do not consider this a major problem, since, as indicated immediately below, this position is laden with new obligations, restrictions and costs, which render it unattractive, unless the data can be sold for profit to third parties at a low liability risk.

Chapters II through IV of the proposal impose a series of extensive **obligations and limitations** on data holders. Among other things, they are required to design products and related services in such a way that would allow direct data access by users (Art. 3(1) DAP – **data access by design and default**). At the same time, they are subject to detailed, pre-contractual **transparency** obligations regarding data use (Art. 3(2) DAP).

Further, data holders must comply with a user's request to share data with the user or with a third party indicated by the user. The data holder's own eligibility to use non-personal, co-generated data must be underpinned by a contract with the user, which means that **no lacunas regarding use rights are allowed** in that contract. It follows that the ability to exploit technical-factual control is significantly diminished.

It is important to stress that the DAP does **not create any new, substantive rights for manufacturers** or parties with factual control regarding the data they hold. Further, a claim that the data is protected as a trade secret or is part of a *sui generis* protected database cannot in principle justify an objection to a data access request (Art. 35 DAP regarding database rights).

Despite the aim to insert more legal certainty, the horizontal scheme still suffers from several gaps and ambiguities. For instance, it is not clear whether the data holder has any **obligation to collect and retain certain data for a minimum period** to facilitate

[12] Art. 2(6) DAP ("'data holder' means a legal or natural person who has the right or obligation, in accordance with this Regulation, applicable Union law or national legislation implementing Union law, or in the case of non-personal data and through control of the technical design of the product and related services, the ability, to make available certain data").

[13] At least with respect to access rights under Chapters II and III DAP, the definition of "data holder" appears circular: data holders are initially defined as persons who have "the right or obligation, *in accordance with this Regulation*… to make available certain data" (emphasis added). Then, Chapters II and III list obligations to make data available imposed on "data holders".

effective access rights. Such an obligation might serve the interests of the user or a third party on the one hand, yet it would create additional costs for a data holder that might not be interested in all that data on the other hand. Generally, there are very few statutory instructions regarding the **content** of the contract between data holder and user. Such matters could (and in the case of potential abuse on the part of the data holder – should) be addressed **by sector-specific regulations and possibly in model contract clauses**.

Additional hovering uncertainties concern the **type of data** subject to sharing obligations, the required **form and format** in which shared data must be provided as well as the obligation to share the data in **real time**,[14] which can be of critical importance in certain use cases, such as smart mobility. The problem of form and format has already been debated, for instance in the context of Article 20 GDPR,[15] but it is not resolved in the DAP, which, in fact, is even less specific on the issue than the GDPR's portability provision.

To touch only briefly upon the difficult question of **what types of data** are subject to access rights and obligations: The definition of "data" provided in Article 2(1) DAP and the rights and obligations concerning data in other Chapters of the DAP do not specify the meaning of data generated by the use of IoT products and related services. Recital 14 DAP excludes from the scope of the Data Act information that is **derived or inferred** from data, as distinguished from the (raw) data that represent the digitalization of "user actions and events". According to Recital 17, the data concept in the Data Act includes both data **recorded intentionally** by the user and data **generated as a by-product** of using the device, or even such data collected without any use of the product (stand-by mode). However, "any software process that calculates derivative data from [the aforementioned data]" is excluded from the scope of the access rights.

Generally speaking, a concept for co-generation of data could adhere to a **technical-factual test**: The user has "done something" with a smart device which triggered the generation of data, and therefore, the user is eligible to access and even to monetize the data. By contrast, a **normative test** would draw the line around "co-generated data" not based on a specific action performed by the user, but rather, based on considerations such as fairness or competing entitlements. The Data Act seems to represent a **mixed approach**, which supports the view that anything beyond "raw data" is also beyond nonvoluntary access rights. Raw data can be understood, based on Recital 17, to be "data in the form and format in which they are generated by the product". An important related question is at **what stage** in the (often complex and extensive) operation of data processing the data cease to be "raw data" under the system of the Data Act and thereby exit the realm of the

[14] Art. 4(1) DAP provides that the data should be made available "[...] where applicable, continuously and in real time" at the user's request. The phrase "where applicable" opens an interpretation leeway for data holders that are resentful about real-time data sharing.

[15] *see e.g.*, Schweitzer, Datenzugang in der Datenökonomie: Eckpfeiler einer neuen Informationsordnung, GRUR 2019, 569, 574.

access rights. Arguably, the problem can only be solved in sector/ industry-specific contexts.

C. The Position of Data Recipients and Third Parties

Third parties may benefit from the new access rights regime by receiving data directly from the holders at the request of the user (Art. 5(1) DAP). While third parties as such are not defined independently, they are mentioned as part of the definition of a "**data recipient**". Accordingly, data recipients are persons to whom holders make data available, and **third parties form a sub-category** of recipients receiving the data following a Data Act request issued by the user or in accordance with a legal obligation to do so (Art. 2 No. 7 DAP). The reference to third parties comes into play in situations of nonvoluntary data sharing by the holder with a party other than the user. It follows that the category of third parties excludes persons that receive the data directly from the user, yet this point is not very clear in the language of the DAP. **It is also not readily clear why the distinction is necessary at all.** A possible answer might be that the Data Act sometimes wishes to focus on regulating **nonvoluntary** data transfer (to "third parties") and sometimes it wishes to address the transfer to "data recipients" more generally.

One important question concerns the application of the access rights regime to data intermediation services (or, **data intermediaries**). Data intermediaries in the meaning of the Data Governance Act proposal[16] are explicitly mentioned in Recital 35 as possible third parties. However, the Data Act appears to be particularly focused on **providers of secondary/related services** in connection with using smart devices as third parties, such as providers of repair, maintenance and supplementary services.

The lack of consideration given to data intermediaries is unfortunate because such entities could actually play an important role in achieving the goals of the Data Act. Such entities specialize, almost by definition, in the management of data access and rights of use on a large scale. In a typical data access scenario, a small or medium-sized innovative company would incentivize users to facilitate access to co-generated data, but the innovative company would need data generated by a large number of users. If data intermediaries are expected to fulfil the promise of professionally and responsibly managing large amounts of data for users, they should be the natural partners of the demand side of data markets, and essentially, **the archetypical "third party"** under the Data Act.

[16] *see* text adopted by the European Parliament on 06 April 2022 on Data Governance Act, P9_TA(2022)0111, especially the definition of "data intermediation services" under proposed Article 2 nr. 11.

The lack of attention paid to data intermediaries as third parties becomes apparent at several points: data intermediaries often facilitate the sharing of data for a variety of lawful purposes. Their main activity – their core service – is to manage access and use rights, rather than providing services that relate to the operation of a smart device. They should necessarily be in the position to share data with multiple recipients for a variety of purposes, depending on their agreements with the user. However, the DAP stipulates that third parties may only make the data available to other third parties if this is **necessary for the service requested by the user** (Art. 6(2)(c), Recital 33 DAP).

The first question is whether providing data to a third party by a third party under the condition of Article 6(2)(c) DAP requires an **explicit contractual basis** between the user and the sharing third party. A second question is whether the Data Act allows for a (flexible) contractual definition of the **purpose**. Flexibility here will accommodate the operation of data intermediaries as third parties. They should be able, also without a specific request of the user, to share the data with other third parties, possibly even for not-yet-determined purposes.

A narrow interpretation of Article 6(2)(c) DAP might seriously handicap the operation of data intermediaries as third parties providing access to **non-personal data**, an operation that is already constrained by **purpose limitation** restrictions under data protection law in the case of personal data.[17] Furthermore, the structure of the DAP might result in **price discrimination** between data intermediaries that are not SMEs (data holders can charge a "reasonable compensation" per Art. 9(1) DAP) and third party SMEs that seek direct access from the data holder (compensation may not exceed the costs directly related to making the data available per Art. 9(2) DAP). In the former case, access becomes more costly and could discourage SMEs from collaborating with larger intermediaries. In addition, data altruistic organizations (to be regulated under Chapter IV of the Data Governance Act) as third parties might also be subject to higher costs. It therefore seems reasonable to **equal the position of data intermediaries –** at least those that are recognized and regulated under the DGA proposal, including data altruism organizations – **with the position of SMEs** on the issue of access prices charged by the data holder.

Like users, third parties are also subject to the **prohibition on developing products that compete** with those of the data holder (Art. 6(2)(e) DAP). Interestingly, here too the restriction is limited to "a product that competes" while leaving a path to developing **competing services**. That said, assuming that data might be passed on from one third party to another (under the limitation of Art. 6(2)(c) DAP), it is not clear how holders can keep track of the activity of third parties down the line unless they find a way to make this restriction "run with the data" through the entire chain of transactions.[18]

[17] Art. 5(1)(b) GDPR.

[18] A further complication that cannot be addressed here in length is how to determine that a competing product was in fact developed based on the data obtained by a third party as a result of a Data Act access request. Particularly in

Last but not least in this partial list of third party issues, Article 5(2) DAP stipulates that **gatekeepers** in the meaning of the Digital Markets Act proposal[19] cannot qualify as third parties under Chapter II, and therefore may **not solicit or incentivize** users to gain access to data for themselves (lit. (a)), for one of their services (lit. (b)) or even **receive data directly from the user** if the data were obtained by that user under a Data Act access request. This provision might suggest *e contrario* that all the actions specified in lit. (a)-(c) **are permissible** for actors that *do* fall under the definition of a third party. Such an interpretation in connection with lit. (c), however, would conflict with the meaning attributed to the concept of a "third party" suggested under the Data Act, namely that the terminology of a "third party" indicates nonvoluntary access entitlements. It is also interesting that the DAP trade secrets provisions (discussed immediately below) speak only of third parties – not of data recipients.

D. Interface with the Protection of Trade Secrets

During the preliminary stages of the Data Act's inception, a key question has been how to consolidate the legal protection of trade secrets on the one hand, and mandatory access rights on the other hand, in a coherent legal scheme. The Trade Secrets Directive defines a "trade secret" as being

"information which meets all of the following requirements: (a) it is secret in the sense that it is not, as a body or in the precise configuration and assembly of its components, generally known among or readily accessible to persons within the circles that normally deal with the kind of information in question; (b) it has commercial value because it is secret; (c) it has been subject to reasonable steps under the circumstances, by the person lawfully in control of the of the information, to keep it secret".[20]

It is undisputed that **data could qualify as a trade secret**.[21] At the same time, a statutory obligation to reveal data to a third party, in some cases even to a commercial entity that

---

view of the fact that a space for innovation is to be created, it should be determined when a product is a competing product and when it is an innovative product. Otherwise, legal uncertainty could impede the development of new products. Further clarification should also be provided regarding the development of parts of a product - such as spare parts. Although not a fully competing product, spare or replacement parts offered by a third party may negatively affect data holders.

[19] European Commission, Proposal for a Regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act), COM/2020/842 final, 15.12.2020.

[20] Directive (EU) 2016/943 of the European Parliament and of the Council on 8 June 2016 on the Protection of Undisclosed Know-How and Business Information (Trade Secrets) Against Their Unlawful Acquisition, Use, and Disclosure (Trade Secrets Directive, Art. 2(1).

[21] The Trade Secret Directive provides a general definition (*cf* Art. 2(1)), but it does not specify what kind of data may qualify for trade secret protection. This point can become relevant in connection with the following question: At which point of processing IoT data do the data meet the requirement of having a commercial value through its secrecy? While data in a syntactic form (e.g., source code) can more easily fall under trade secret protection, isolated raw data might be considered trivial, even worthless, although they could be(come) part of an important (and valuable!) information asset when aggregated, enriched, refined, processed, etc.

potentially competes with the owner of the trade secret, almost by definition undercuts the efforts to keep the information secret and might negatively affect its value.

The DAP attempts to square the circle in the following way: It declares that, generally, the protection of trade secrets within the meaning of Directive 2016/943 should be preserved.[22] But trade secrets protection cannot shield data holders from compliance obligations with access requests to the information that constitutes a trade secret. Instead, Articles 4(3) and 5(8) DAP provide that access to trade secrets should be facilitated under **confidentiality safeguards**. Disclosing a trade secret to a third party is required only if the information is strictly necessary to fulfill the purpose agreed between a user and a third party.[23] Essentially, these safeguards can (and are likely to) be represented in contracts between holders and users, as well as between holders and third parties. In addition, the data holder is allowed to apply **appropriate technical protection measures** in order to ensure compliance *inter alia* with trade secrets obligations of third parties under Article 5 DAP (Art. 11(1) DAP).

Article 5(8) DAP requires that "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." The crux of the matter is how to determine what constitutes "**all specific necessary measures**". It is not unlikely that holders and third parties will disagree on these specific necessary measures. And if data holders use technical protection measures, a point of dispute could be whether these TPMs are "appropriate" in the meaning of Article 11(1) DAP or rather facilitate excessive control.

On a more fundamental level, it is unclear how the requirements for attaining trade secret protection and maintaining the secrecy of information **can be aligned with a mandatory access rights regime**. Under the Trade Secrets Directive, information must be kept secret *via* reasonable measures and sustain a commercial value derived from that secrecy in order to qualify. Under the DAP, however, the data holder is required to share this secret information with a potentially indefinite number of users and third parties. Even if non-disclosure agreements are strict and enforceable, having numerous such agreements with numerous parties would render secrecy illusory. Also, the "purpose limitation" provision in Article 5(8) DAP falls short of providing sufficient safeguards. This limitation, which is tied to the purpose agreed with the use, is quite vague. And the **scope of such a purpose depends on agreements to which the holder** (and the trade secret owner) **is not a party**.

[22] Art. 8(6) DAP; S. 5, DAP.

[23] Under Article 5 (8), trade secrets shall only be disclosed to third parties "to the extent that they are strictly necessary to fulfil the purpose agreed with the user and the third party.".

III. Contracts Concerning the Use and Transfer of Data

A. Requirements Cconcerning Contracts and Ttheir Content

We have seen that the Data Act would impose conditions and restrictions on the ability of data holders to make use of IoT data that are technically under their control. The holder must **conclude a contract** with the user if the holder wishes to use co-generated, non-personal data for his own needs and purposes (Art. 4(6) DAP). Also, providing data access to third parties must be underpinned by a contract between the holder and the third party (Art. 5(1) DAP). It follows that **private contracts will play a very significant role** in the implementation of the Data Act regime, and the **content** of these contracts is expected to be influenced by the regulation in several important ways.

First, contracts with data recipients are subject to **FRAND** requirements to ensure the consistency of data sharing practices across the Internal Market and to promote fairness of data sharing practices (Art. 8(1), Recital 38 DAP). Second, there are some specific restrictions concerning the **compensation** which holders can charge for making data available. The compensation must be "reasonable" for data recipients in general (Art. 9(1) DAP), and it may not exceed the cost of production for SMEs (Art. 9(2) DAP). Third, Chapter IV sets forth a detailed scheme **against unfairness in contractual terms unilaterally imposed** on SMEs that concern access to and use of data and related contractual terms.

B. Specific Restrictions on Contractual Provisions

1. CONCEPT(S) OF FFAIRNESS IN THE DATA ACT

a) Fairness Obligation Under Chapter III

As part of the FRAND requirements, Article 8(1) DAP provides that where an obligation to provide access to data exists, the terms for such access must be fair. Chapter III does not elaborate on the content of this fairness requirement. Instead, it contains a reference to the unfairness test in Chapter IV (*infra*). In addition, Recital 40 provides, rather

vaguely, that "the general rules on data access rights should refer to the rule on avoiding unfair contract terms."[24]

Unlike the fairness test in Chapter IV, however, fairness requirements under Chapter III are not limited to SMEs upon which the terms have been unliterally imposed. This means that fairness under the **FRAND** provisions has a **broader application scope** than the unfairness test, and that the latter will not be directly applicable in many cases subject to the FRAND requirements.

b) The Unfairness Test Under Chapter IV

Chapter IV confronts the challenge of devising an objective fairness standard for commercial contracts by creating a three-tiered structure: It defines a **general standard** for identifying unfair contractual terms; these are terms that "grossly deviate […] from good commercial practice in data access and use, contrary to good faith and fair dealing." (Art. 13(2) DAP). It then provides a list of contractual terms that are **always considered unfair** (Art. 13(3)(a)-(c) DAP) and a list of such terms that are **presumed unfair** (Art. 13(4)(a)-(e) DAP).

The application of the unfairness test is limited in several important ways. First, it applies only to contracts that are **unilaterally imposed** on **SMEs** (i.e., micro, small or medium-sized enterprises).[25] Thereby, it seems that both (1) natural persons that are not "engaged in an economic activity"[26] and (2) larger enterprises – as categories of data recipients – are excluded.[27] Second, it only applies to such terms in the contract that concern making data available, access and use of data as well as liability or remedies for breach and termination of data-related obligations (Recital 53 DAP).

Recital 54 DAP introduces a distinction between "**excessive contractual terms**" in favor of one party to the bargain that are subject to the unfairness test on the one hand, and terms that are "**normal**" in B2B contracts reflecting a "normal expression of the principle of contractual freedom" on the other hand. The unfairness test does not apply to such "normal" terms. The test further does not apply to terms defining the **subject matter** of the contract or to **price** (Art. 13(4)(7) DAP).

---

[24] Recital 40 DAP is vague insofar as it is not clear *who* should refer to the rules of avoiding unfair terms conditions and *when* and *where* this should be done. This could be the parties of the contract or the person who interprets/implements the law. Or, it may simply be an explanation why Chapter III refers to Chapter IV on this point.

[25] This is explained in the DAP by the fact that SMEs in particular are at a disadvantage in contract negotiations for access to data (Recital 51 DAP).

[26] Commission Recommendation 2003/362/EC (06.05.2003), Art. 1 (defining "Enterprise").

[27] Commission Recommendation 2003/362/EC (06.05.2003) provides the following definition: "The category of micro, small and medium-sized enterprises (SMEs) is made up of enterprises which 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.".

The unfairness test triggers several questions concerning its interpretation and implementation. To name just a few: (1) the general standard of unfairness is composed of **unspecific legal terminology** such as gross deviation from good commercial practice or terms that are contrary to good faith and fair dealing. In the absence of a clear understanding of what commercial good practice means, or what manifests a lack of good faith, **legal uncertainty will cloud the application of the test to a specific case.** Parties will need to wait until courts or other relevant authorities render opinions while resolving disputes and establishing thereby something akin of a "caselaw" that would make the application of the unfairness test more predictable.[28]

Further, (2) a contractual term is "**unilaterally imposed**" only if the party upon which the term is imposed was unable to influence the term **despite an attempt to negotiate it** (Art. 13(5) DAP). At the same time, the burden of proof is on the "imposing party", which is required in effect to **prove a negative fact**. Under this arrangement, the imposing party faces the challenge of how to prove that the other party **has *not* tried** to negotiate the term.

In addition, (3) it is not clear whether the **imposing party** can also be an **SME** for the unfairness test to apply. Unlike Chapter IV, the DAP explicitly carves out small enterprises from the scope of the duties and restrictions it creates in other sections (e.g., in Chapter II). If the whole idea of fairness in private commercial dealing is to protect the weaker party, what is the rationale for imposing an unfairness test on a small company negotiating a contract with another small company?[29] The underlying assumption might be that one small company cannot impose unfair terms on another small company (a "take it or leave it" situation). But this is not necessarily the case.[30]

In fact, Chapter IV **entirely departs from the terminology** of "data holder", "user" and "data recipient" as defined and applied elsewhere in the Data Act. Instead, it uses a language of contractual terms unilaterally imposed "by an enterprise" on a micro, small or medium-sized enterprise (Art. 13(1) DAP). The forgoing critique hints to a more general problem, which is the **relationship between the FRAND fairness requirement and the unfairness test**. Given the structure of the DAP, their scopes of application do not always overlap. Resulting discrepancies regarding their respective scopes, contents and consequences of infringement should either be lifted or better explained. Among other things, it should be considered whether **applying the unfairness test to a broader group of**

---

[28] Chapter IV is silent on the question which authority is responsible to *adjudicate*, in the case of a dispute, whether at contractual term passes the unfairness test or not. Dispute settlement under Article 10 DAP does not directly apply, unless triggered indirectly via Chapter III. Possibly, a national competent authority under Chapter IX of the DAP will oversee this task, or, by default, the national court system.

[29] Recital 46 DAP suggests that it is not necessary to intervene when the data holder is an SME and the data recipient is a large company, albeit in a different context.

[30] Consider a situation in which the SME imposing the allegedly unfair term is providing a unique service, has special know-how or holds IP rights that secure some form of exclusivity.

data recipients, including consumers (i.e., natural persons not engaged in an economic activity) and larger enterprises, could aptly further the goals of the Data Act.

2. NON-DDISCRIMINATION

Non-discrimination comes into play in the context of the FRAND requirements stipulated in Chapter III, which generally concern data holders that are legally obligated to make data available "under **fair**, **reasonable** and **non-discriminatory** terms and in a transparent manner". Unlike in the case of the fairness requirement, Chapter III indeed specifies a certain non-discrimination standard. Specifically regarding non-discrimination, Article 8(3) DAP provides that data holders "shall not discriminate between **comparable categories of data recipients**, including partner enterprises or linked enterprises". Discrimination is negated if different contractual terms are justified by objective reasons. The data holder carries the **burden of proving** that the terms of providing data are non-discriminatory. (Art. 41 DAP).

Especially the phrase "**comparable categories of data recipients**" is likely to trigger uncertainty and disputes, and hence, parties could benefit from more specific instructions on how to comply. **Model contractual terms** (Art. 34 DAP) could be helpful here as well. In cases where data holders and data recipients cannot agree on allegedly discriminatory terms, the dispute settlement mechanism may be triggered.

3. COMPENSATION

As mentioned, any **compensation** agreed between data holders and data recipients must be "**reasonable**" (Art. 9(1) DAP), and in case the data recipient is a micro, small or medium-sized enterprise, compensation shall **not exceed the costs directly related** to making the data available to the data recipient and which are attributable to the request (Art. 9(2), Rec. 44 DAP). The direct costs are those necessary to make the data accessible, which does not include the costs of data collection and storage. The costs for SMEs are limited proportionally to such costs that are attributable to an individual data request (Recital 45 DAP).

The idea is, again, to shield in the name of fairness smaller companies against abuse of superior bargaining power and from data holders prioritizing their own commercial interests. But the DAP goes one step further by **prohibiting data holders from generating profits** from nonvoluntary data sharing with small and medium-sized companies that are data recipients. The transparency provisions require that data holders provide sufficient and verifiable information on the basis for the calculation of compensation (Art. 9(4), Recital 47 DAP).

Calculation of a **reasonable compensation** for data recipients (excluding SMEs) takes into account "factors such as the volume, format, nature, or supply of and demand for the

data as well as the costs for collecting and making the data available" (Recital 46 DAP). Beyond that, determining a reasonable price is left to the parties, and it is clear that compensation here may **exceed direct costs** of making the data available.

The emerging picture is that the Data Act intends to reduce access costs of SMEs to minimum and to ensure that the price for access paid by other recipients remains within the realm of reasonableness. In this sense, a statement found in Recital 46 is somewhat confusing:

"It is not necessary to intervene in the case of data sharing between large companies, or when the data holder is a small or medium-sized enterprise and the data recipient is a large company. In such cases, the companies are considered capable of negotiating any compensation if it is reasonable…".

The statement seems inconsistent because imposing a reasonableness requirement **is already an intervention in price setting** between companies. The operative language of the proposal does not clearly exclude large companies as data recipients from this restriction on compensation. One way to understand this statement is as creating a **presumption** in favor of reasonableness when larger companies negotiate a price among themselves. This presumption could still be scrutinized and possibly rebutted under the Data Act's dispute resolution mechanism (described immediately below) or by a court.

C. Dispute Settlement

In case of a dispute regarding compliance with the FRAND requirements, data holders and recipients may turn to dispute resolution bodies (Art. 10 DAP). State-certified bodies, which have the appropriate expertise, should assist the parties in resolving their dispute (Art. 10(1)-(2) DAP). The decisions of the dispute settlement body are only binding if the parties to the contract have **explicitly consented to this arrangement before the start of the proceedings** (Art. 10(8) DAP). Dispute resolution under Section 10 DAP does not prevent parties "from exercising their fundamental rights to an effective remedy and a fair trial" and from seeking recourse before a court or a tribunal of a Member State (Recital 50 DAP). Dispute resolution bodies can provide an expedite and inexpensive alternative to the courts system. A particularly positive aspect is the obligation of the dispute resolution bodies to reach a decision within 90 days (Art. 10(7) DAP). In addition, the parties may benefit from the expertise of the dispute settlement body on the subject matter.

IV. Data Portability, Switching between Providers, Interoperability

A. "Data Portability" Right

In alignment with the aims of facilitating data flows, enhancing data sharing and improving the necessary infrastructure, the DAP introduces, as described above, a series of provisions that permit data usage by parties other than the original data holder according to a request issued by data users. It further enables **switching between providers of certain IT services**.

The right of users to demand and enforce data sharing with a third party of their choice in order to facilitate reception of services offered by that third party can be understood as a **"data portability" right**.[31] At the same time, the terminology of data portability *per se* does not suggest that transfer of data to a third party is accompanied by the data holder losing its right and ability to continue collecting and using data.

The access right of third parties under Article 5 DAP goes beyond comparable portability rights under existing EU legislative instruments of horizontal data regulation such as Article 20 GDPR or Article 16 of the Digital Content and Services Directive. It further goes beyond portability rights under Section 6(h) of the Digital Markets Act proposal. One unique aspect of this right is that it is supported by a **nearly unconditional obligation** of data holders to comply with data users' requests to **facilitate access data to a third party** – gatekeepers excluded (Art. 5(1)-(2) DAP) – even though the data holder is also considered a "co-generator" of the data.

As shown, the terms and conditions for data access rights as well as the scope of use rights by third parties are the subject matter of **a cluster of contracts** between data holders, third parties and users. Medium-sized enterprises and larger data holders are bound by the obligation to share data with third parties, and data holders apparently are not allowed to bypass this obligation *via* an exclusivity clause in their contract with the user. **Restrictions** on third parties obtaining data by virtue of the portability right regarding their use of the data include certain limitations on the content of contracts with users and with other third parties. In addition, the Data Act's portability right applies (also) to **non-personal data,** and "porting" the data should take place without any costs to the user.

---

[31] Explanatory Memorandum, p. 13 ("The proposal facilitates the portability of the user's data to third parties and thereby 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.") This statement indicates that the terminology of portability is also used in the context of access rights under Chapters II and III.

B. Switching between Providers

Chapter VI DAP, which regulates the process of switching data processing services, incorporates an explicit data portability provision (Art. 23(c) DAP) in connection with a broader scheme that is designed to facilitate **effective switching** between service providers. Chapter VI consists of both **contractual and technical requirements** to achieve this goal. Here as well, the right to switch between providers and the condition of exercising that right must be **explicitly stated in the contract** with the customer (Art. 24(1) DAP).

Next to the obligation of facilitating "**functional equivalence**" of the service in the technological environment of the other service provider,[32] contractual terms between the service provider and the customer regarding switching to another provider are subject to a **specific and detailed list of requirements**, including those enumerated in Article 24 DAP. These are highly customer-friendly and are designed to prevent lock-in situations.

C. Interoperability

Chapter VIII DAP represents another building block in the edifice by sketching a **horizontal framework to the technical infrastructure** for data sharing with a focus on interoperability. The resulting framework of "**essential requirements**" regarding interoperability is, however, quite abstract. More precise rules and technical standards, potentially sector-specific, are to be determined in further instruments such as delegated acts, implementing acts, proposals of standardization organizations and other guidelines.

Chapter VIII addresses several categories of actors. Article 28 DAP applies to "**[o]perators of data spaces**", Article 29 DAP applies to "**data processing services**" and Article 30 DAP applies to vendors or deployers of **smart contracts**. Unlike data processing services and smart contracts, data spaces or operators of data spaces are **not defined** in the DAP. The Data Act presumably relies on documents published by the European Commission in past years, including the European data strategy and the work on common European data spaces.[33] A specific definition, or at least a **clear reference to the concept** as explained elsewhere, would nonetheless be helpful.

---

[32] Art. 2(14) DAP ("'functional equivalence' means 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").

[33] *See e.g.,* European Commission, A European data strategy, COM/2020/66 final, 19.2.2020; European Commission, Commission Staff Working Document on Common European Data Spaces, SWD(2022) 45 final, 23.02.2022.

V. Business-to-Government (B2G) Data Transfer

A. Scope and Content

Chapter V DAP concerns nonvoluntary access to privately held data by public sector bodies. In this sense, it presents a novel[34] horizontal mechanism **pertaining to the access rights of governmental entities for a certain purpose** going beyond the commercial-economic stance of the Data Act's B2B and B2C mechanisms. Voluntary sharing of data between private and public actors is not preempted by the Data Act (Recital 59 DAP). Further, data holders that are small and micro enterprises are not subject to access requests under Chapter V (Art. 14(2) DAP). Importantly, according to Article 17(3) DAP, public bodies may not share data obtained this way while complying with existing instruments for re-use of publicly held data under the Open Data Directive (Directive (EU) 2019/1024).

Beneficiaries of the data access rights – namely, public sector bodies or Union institutions, agencies or bodies – may issue a request in case of an **exceptional need** to use data (Art. 14, 15 DAP). An exceptional need can be established under three alternative circumstances: (1) When the requested data is needed to respond to a **public emergency**; (2) when data access is required to **prevent or assist the recovery from a public emergency**; or, (3) when access is required and the **lack of available data** prevents the public body or Union entity from **performing a specific task in the public interest** that is explicitly provided for by law.

The latter category of data requests is subject to additional requirements: The public body must either be unable to obtain the data through any other means – which includes acquiring the data at market price and enacting legislative measures – or, obtaining the data through the process set forth in the Data Act would significantly reduce the administrative burden on data holders or other entities.

B. Safeguards against Misuse by Public Bodies

Access rights in favor of public bodies interfere with private autonomy and established freedoms, such as the freedom of contracts, or the freedom to conduct a business.[35] It is therefore important to constrain nonvoluntary access requests and provide appropriate

[34] Sectoral, national legislative efforts can be found for instance in regulations on data of general interest in France ("Données d'intérêt général"), Art. 17-24 of the Loi n° 2016-1321 pour une République numérique, 7.10.2016).

[35] Art. 16 to the EU Charter on Fundamental Rights.

safeguards in order to protect fundamental rights of private enterprises and to avoid excessive or improper interference.

The DAP sets out **formal and material requirements concerning data requests issued** by public entities (Art. 17 DAP). It further creates a mechanism under which data holders can **decline or seek modification of a data access request** (Art. 18 DAP). The DAP also provides for rules of compensation for data holders and, in some cases, for their technical and organizational costs (Art. 20(2) DAP). Unless agreed otherwise, the public entity has the **obligation to destroy the data once it is no longer necessary for the purpose** stated in its request (Art. 19 (1)(c), Recital 65 DAP).

The above-mentioned provisions, as well as the prerequisites for access requests in Article 15 DAP, may indeed be viewed as providing **safeguards** against excessive or inappropriate application of B2G access rights. At the same time, they trigger some uncertainties, only a few of which can be addressed below.

C. Access Right for Fulfilling a Specific Task in the Public Interest (Art. 15(c) DAP)

In case of a lack of data necessary for the fulfillment of **"a specific task in the public interest that has been explicitly provided by law"**, public sector bodies may demand access to the data controlled by a data holder (Art. 15(c) DAP). The requirements that the data (1) may not be obtained either in a timely manner by alternative means or in a timely manner by new legislative measures, or that (2) obtaining that data in this way substantively reduce the administrative burden for data holders or other enterprise, raise several questions.

First, it is not clear **how and why** a public entity is in the position to determine which way of obtaining data is **less burdensome** for a private entity and how such a circumstance can be established, and in the case of a dispute, proven by the public entity. Second, since Art. 15 (c)(2) DAP potentially has a very broad scope, it is necessary to clarify why and when a reduction of an administrative burden to private entities justifies an access claim and which examples of application the legislature has in mind.

Third, it is not clear whether the circumstance stated in Article 15 DAP that the data cannot be obtained by the public body in any alternative way applies only to its subsection (c)(1) or also to subsection c(2). The structure Article 15 DAP indicates application only in the former case. However, Recital 58 DAP provides as follows:

Such exceptional need [other than under Art 15 (a)-(b)] may also occur in other situations, for example in relation to the timely compilation of official statistics when data is not otherwise available or when the burden on statistical respondents will be considerably reduced. At the same time, the public sector body or the Union institution, agency or

body should, outside the case of responding to, preventing or assisting recovery from a public emergency, demonstrate that no alternative means for obtaining the data requested exists and that the data cannot be obtained in a timely manner through the laying down of the necessary data provision obligations in new legislation.

This Recital muddies the water because it mixes the prerequisites for data requests under lit. (c)(1) and lit. (c)(2) while creating the impression that proving the lack of availability of the data through alternative means and the time factor are also necessary in the latter case, namely, where obtaining the data under the Data Act's procedure would reduce the administrative burden for data holders or other enterprises. Such interpretation, however, challenges the logic of the provision of lit. (c)(2) that assumes that an alternative way *is* available but would be more burdensome. Hence, **Recital 58 should use clearer language** and be aligned with the structure and the logic of Article 15(c) DAP.

VI. Recommendations

\ The **consolidated impact** of the new access rights regime on the economic incentives of IoT device manufacturers and innovation in secondary markets should be **monitored periodically** and assessed based on empirical data, to the extent possible.

\ The focus of the Data Act only on co-generated IoT data and subjecting only such data to nonvoluntary access rights call for a **more rigorous and systematic justification** in light of the motivation behind this regulation, its economic assumptions and its normative underpinning.

\ The operative language of the Data Act should clarify that **users may use the co-generated data they obtain for any lawful purpose**. This includes the commercialization of the data but excludes development of a competing device (as stipulated under Article 4(4)) or infringing on a trade secret. Contractual terms to the contrary should be invalid or at minimum be justified by special circumstances.

\ The operative language of the Data Act should clarify that **contractual terms that secure exclusive use for data holders are not enforceable** against a user or against a third party, provided that the conditions set forth in the Data Act for data sharing beyond such an exclusivity clause are fulfilled.

\ The Data Act should elaborate with more precision **what categories of data are subject to the access rights regime**, especially in light of the different possible stages of collecting, analyzing and utilizing IoT data.

\ The Data Act should include **clearer rules on circumstances where providing access to data in real-time is mandatory** and whether there is any obligation imposed on holders to **retain** certain data for a certain period of time in order to facilitate access rights.

\ The **distinction between "data recipients" and "third parties"** as a sub-category of data recipients should either be removed or otherwise explained and implemented in a more consistent manner throughout the Data Act.

\ The **conditions for and limitation on third parties that wish to share data further with other third** parties should be clarified beyond the provisions of Article 6 DAP, especially with regard to the question of the necessity of a contractual agreement for such further sharing and the permissible flexibility of defining **purposes** in a contract with the user.

\ The Data Act should generally be **better attuned to the possibility and advantages of data intermediaries** assuming the role of a third party. If the core activity of the third party is, as in the case of data intermediaries, to mediate data and access entitlements between holders and recipients, we recommend equaling its position with the position of an SME on the matter of costs.

\ **Trade secrets should receive a more effective protection** in the face of access requests making them available to users and third parties. The meaning of the phrases "all specific necessary measures" and "appropriate technical protection measures" should be more specific, and it is recommended to consider **additional restrictions** on users and third parties that receive access to data protected under trade secrets. Essentially similar and strict confidentiality rules under the Data Act must bind all data recipients, third parties, users and governmental bodies.

\ The **non-discrimination** test under the FRAND requirements in Chapter III could benefit from **more clarity**. Precise instructions for the parties or a fact finder attempting to determine when different categories of data recipients are "comparable" and when they are not might be especially helpful.

\ The **consequences of non-compliance with the FRAND** requirements under Chapter III (beyond unfair terms under Article 13 DAP) should be stated. Non-compliant terms should be declared unenforceable against the aggrieved party.

\ **The relationship between the FRAND** requirements under Chapter III and the **unfairness test** under Chapter IV should be clearer. Inconsistencies in their respective coverage and the deviation in Chapter IV from the DAP terminology should be explained and possibly modified for a more coherent and consistent application of fairness obligations.

\ The **interoperability** requirements should include more explicit definitions of the actors subject to the duties listed under Chapter VIII, especially operators of data spaces.

\ The **conditions to and limitations on B2G access rights** must be stated **more clearly and restrictively**, especially in the cases regulated under Article 15(c) DAP where a lack of data prevents the public body from fulfilling a task in the public interest.