weizenbaum institut

Position Paper

concerning

Data Act - Inception Impact Assessment

Submitted by the Weizenbaum Institute Research Groups:

Framework Conditions for Data Markets
Shifts in Norm Setting

About the Weizenbaum Institute: The Weizenbaum Institute conducts interdisciplinary and fundamental research on the transformation of society through digitalization. Its aim is to contribute to a better understanding of the dynamics, mechanisms and implications of digitalization. To this end, the Weizenbaum Institute investigates the ethical, legal, economic and political aspects of the digital transformation and creates an empirical basis for shaping it. The Institute develops options for policy, the economy and civil society by combining interdisciplinary, problem-oriented research while exploring concrete solutions and opening up a dialogue with the society at large. 'Weizenbaum Institute for the Networked Society – The German Internet Institute' is a joint project funded by the Federal Ministry of Education and Research (BMBF).

I. INTRODUCTION

The EU Commission has recently published an Inception Impact Assessment (IIA) concerning the envisaged Data Act[1] and requested feedback on this initiative. The Data Act has been already mentioned in general terms in the Commission's EU Data Strategy.[2] Now, the IIA provides more details regarding the anticipated areas of regulation the Data Act will cover and possible regulative approaches it will take. The IIA describes the Data Act in broad strokes, and this Position Paper correspondingly addresses some of the relevant questions raised therein from a high-level perspective. The main purpose of this Position Paper is to highlight some of the most pressing issues regarding the scope and modus of regulation the Data Act may (and in some cases - should) assume.

While approaching the Data Act analytically, it is of utmost importance to ascertain a number of **framework questions**. These questions include the **motivation** or **purposes** of regulative intervention (what is the problem?), what **kinds of data** are covered (what subject matter?), which **market players** are to be directly affected by the new instrument (e.g., who can exercise data access and use rights against whom?), which **legal instruments** are to be applied, and finally (but not conclusively), what is the preferred **mechanism for implementing** the new scheme of rights and duties and which principles the scheme should be based on.

In the following, we address a number of areas the Data Act is expected to encompass. In doing so, the framework questions sketched above serve as a **rough roadmap** for this initial analysis. The intention is to chart the regulatory landscape the Data Act will need to navigate through and the questions it will need to address at later stages of the legislative process.

[1] European Commission, Inception Impact Assessment, Ref. Ares(2021)352715, 28.05.2021 (IIA).
[2] European Commission, A European strategy for data, COM(2020) 66 final 19.2.2020, p.13.

According to the IIA, the Data Act is "about ensuring fairness in the allocation of economic value among actors of the data economy".[3] The concept of "**fairness**" here is challenging. The context includes data sharing activities within data markets that operate as part of the larger data economy and which are guided in principle by economic parameters. Integrating the principle of fairness will require breaking it down to **goal-oriented, specific, easy-to-understand and easy-to-implement rules** that take notice of, and are compatible with the legal terrain within which the new rules ought to operate.

The principal deficits in the EU data economy the Data Act seeks to confront can be described essentially as the **lack of incentives to share data** held by commercial entities, **power imbalances** in data markets and economic sectors that rely on data as a crucial resource, current **legal barriers and uncertainties** which curtail the desired large-scale data sharing, and perhaps to a lesser degree, insufficient **infrastructure** to facilitate large-scale data sharing under existing law.[4]

II. B2G DATA SHARING

The Commission's efforts in the past few years focused partly on facilitating data flow from the public sector to other sectors and stakeholders.[5] The relevant part of the Data Act would operate in the opposite direction: It will strive to **invigorate sharing of privately held data with the government**. The problem identified is that not enough such data is being shared with the public sector, and hence, the public sector is hindered in finding ways to use the data to benefit the public or develop its own data models. The IIA mentions high economic barriers for B2G data sharing as well as fragmentation across sectors and between Member States.[6]

We observe that a key reason for this state of affairs is the **lack of economic incentives** to voluntarily share data with the public sector. This is coupled with a host of **economic and legal disincentives** to do so, a situation which is aggravated by a lack of well-established structures for voluntary B2G data sharing within and across economic sectors as well as the lack of user friendly and cost effective technical infrastructure to facilitate such sharing. The desire to defend data assets as trade secrets in a competition-oriented environment or as a type of intellectual property likely contributes to sharing aversion tendencies, joined by **legal uncertainty** and **compliance risks**, e.g., when personal data is involved.[7]

The strategic mission of the regulator is hence to create the missing incentives and/ or remove existing disincentives to share data and mitigate aggravating factors. From the perspective of measures, there is an important difference between creating the conditions for a **voluntary data sharing** and creating new legal rules for **involuntary data sharing**. The IIA advocates for creating a "flexible framework" that takes into account and will likely include both types of measures.

---

[3] IIA, p.1.
[4] This Position Paper does not touch upon the topics of smart contracts and safeguards for nonpersonal data in international contexts that are mentioned in the IIA.
[5] Open Data Directive, (EU) 2019/1024; Data Governance Act (DGA) proposal, COM(2020) 767 final, 2020/0340 (COD), (25.11.2020), Chapter II.
[6] IIA, p.2.
[7] The IIA indicates that both personal and nonpersonal data will be covered by the new rules. *id.*

Especially in the case of nonvoluntary sharing (the assumption being that voluntary sharing or acquiring the data under the current market conditions does not suffice), such framework will have to establish precise rules concerning, among other things, the following aspects:

(1) Which **commercial actors** are subject to B2G data requests and under which formula should they be classified (type of services, economic sector, size, market influence)?

(2) What **kind(s) of data** shall be subject to such requests?[8]

(3) For which **purpose** may the government use the obtained data (e.g., public health, developing smart mobility infrastructure and solutions, enhancing energy efficiency, environmental improvements, improving various public services)?[9]

(4) May the government **share** the obtained data further **with private sector partners** to achieve its legitimate purposes?

(5) What is the role of **data intermediaries** in implementing such a B2G program?[10]

In addition, interface questions with legal protection of databases and trade secrets (*infra* Sections V. and VI.), which cut across several subject areas of the Data Act, will have to be answered in this specific context of B2G data transfer as well.

A persisting question that is relevant also here concerns the choice between **sector-specific** and **horizontal regulation.** Each option has its advantages and disadvantages. In the context of B2G data sharing, a focus on a sector-specific approach appears in principle more appropriate yet without excluding *certain* horizontal standard setting. Data often constitutes a critical resource for businesses, and creating mandatory government access rights to such data might turn into a complex and delicate balancing act, especially when taking into account negative backlashes on the market, unintended consequences, over-regulation effects, new legal uncertainties, etc.

The rules therefore should be as **clear, transparent, fine-tuned, adjustable and balanced** as possible. It is more likely to achieve such structure of B2G access rights within sectors while being mindful of the specific conditions, realities, requirements, deficiencies and possibilities in the affected industry. **A sector-specific nuanced approach** will help to better define the purposes, appropriate modalities and other details of such access rights. This approach, however, does not exclude seizing the opportunity to clarify some general concepts and principles horizontally, for instance, providing a general definition to purposes "in the public interest"[11] or establishing a **competent authority** to oversee the implementation of B2G access rights. Hence, we advocate for **a mixed approach with an emphasis on effective sector-specific regulation**.

The Open Data Directive ((EU) 2019/1024 - ODD) already reflects a mixed approach model. On the one hand, it provides a list of general principles (e.g. concerning format, transparency,

[8] One possible differentiation is between raw data, processed data and data driven insights. *see* "Towards a European strategy on business-to-government data sharing for public interest – Final report prepared by the High-Level Expert Group on Business-to-Government Data Sharing" (2020), p.22 ff. https://www.euractiv.com/wp-content/uploads/sites/2/2020/02/B2GDataSharingExpertGroupReport-1.pdf).

[9] In addition, should data requests be limited only to (pre-defined) purposes in the public interest, or are other purposes equally legitimate? How should a purpose "in the public interest" be defined?

[10] The IIA refers to "[i]ntermediation structures or bodies [that] could aggregate demand, support professionalization, convene public sector bodies interested in certain data as well as private sector data holders, including at sectoral level. Their mandate could be to facilitate agreement on the conditions of use of such data, including remuneration." IIA, p.5.

[11] Towards a European strategy on business-to-government data sharing for public interest, n. 8. at p.16.

non-discrimination). On the other hand, it contains a list of categories of high-value data sets (Article 13(1) ODD, in connection with Annex I), with respect to which the Commission is empowered to provide more specific regulation *via* adopting delegated acts (Article 13(2) ODD).

The Commission's High-Level Expert Group on Business-to-Government Data Sharing report has already formulated some basic principles for B2G data sharing: Proportionality, purpose limitation, minimizing of harm to legitimate interests, consideration of the public interest in contractual conditions, data quality management and transparency.[12]

In order for the Digital Single Market to remain attractive for data-driven business, designing a B2G data sharing framework will need to make sure that commercial actors in general do not suffer disproportional economic disadvantages or face new risks under the new rules. It would seem reasonable and fair to establish a **compensation scheme** for businesses that contribute the data,[13] a proportionated scheme of non-compliance consequences as well as clear and transparent rules regarding further sharing of the acquired data with third parties (joint ventures).[14] Regarding licensing and compensation, the new scheme might draw inspiration (at least roughly) from established legal fields and concepts in private law, for instance, compulsory licenses in IP law (patents, copyrights) and on the interface between IP licensing and antitrust law.[15]

We also deem reasonable and fair the building into the framework of a system of **exceptions**, **objection** and **dispute resolution mechanism**,[16] for instance, in cases where the harm to the private interests of the data holder clearly outweighs the benefits to the public interest. Such harm could be established *inter alia* in the case of compromising - *via* compulsory sharing - IP rights, trade secrets or fundamental rights. A designated **competent authority** with a structure that could draw on Chapter V of the Data Governance Act (DGA) proposal may be endowed with the task of evaluating and deciding on contested access requests, subject to effective judicial review.

In case commercial companies wish to simply **contribute data** in their possession to the public sector for whatever reason or purpose, either directly or collectively (e.g., through collaboratives that function as data intermediaries), such initiatives should be subject to a **simple, trustable and cost effective process**, alongside the obligatory data sharing course. A data intermediaries governance model for data altruism exists already in the Data Governance Act proposal. This model could be expended also to facilitate direct data contribution from the "corporate data donor" - subject to similar assistance, safeguards and standards.

---

[12] n. 8 at p.79 ff.

[13] There are various conceivable pricing methods, ranging from zero compensation though return of marginal costs, marginal costs plus fair ROI, tax exemptions, to full market price. Id, p.39. For more discussion, *see* Martens, B., Duch-Brown, N., The economics of Business-to-Government data sharing, European Commission, Seville, 2020, JRC119947 https://ec.europa.eu/jrc/sites/default/files/jrc119947.pdf.

[14] Re-use may include cases where the government wishes to enter into partnerships with third parties but also when third parties file (e.g., under the Open Data Directive) a request to obtain a document that contains data retrieved from a business under involuntary B2G data sharing rules.

[15] *cf* Case C-418/01, EU Court of Justice, 29.04.2004 (IMS Health). There has been a larger, ongoing discussion on whether data as such can be treated as (intellectual) property and whether certain antitrust doctrines (e.g., the "essential facilities" doctrine) are applicable to data, which cannot be elaborated on here.

[16] Judicial or administrative review mechanisms already exist in the area of compulsory licenses under patent law and antitrust law, for instance.

III. B2B DATA SHARING

The key points mentioned in the context of B2G data sharing can be reiterated, sometimes even with greater force, in the context of businesses that share data with other businesses. The Commission so far has been very cautious with establishing mandatory rules in this area. Instead, the focus was on creating non-binding recommendations and formulating best practice principles.[17] The IIA provides indications that the Commission now endeavors to make a step forward towards binding rules on the subject.

The impetus for the new approach is the desire to assist SMEs in their efforts to gain access to data they need for developing their business. The required data is often held by large players who are reluctant to sharing it. The Digital Market Act (DMA) proposal already includes certain obligations imposed on gatekeeper platforms to provide access to certain information they hold and systems they operate to other businesses.[18] The Data Act reflects the ambition to expand the scope of mandatory "B2B access rights"[19] to data beyond gatekeeper platforms, or at minimum, impose mandatory requirements regarding access to and use of data inside contracts between large players and SMEs in order to promote fairness and combat power asymmetries such contractual arrangements often mirror.

There are important differences between the various regulative approaches mentioned in the IIA on a scale of growing intensity. The higher the intensity is, the deeper is the expected impact on the market. The options range between mere transparency obligations,[20] pre-setting or scrutinizing the content of B2B contracts (possibly *via* a "fairness test" or model contract terms), or even imposing a duty to deal and provide access and use rights.[21]

Such measures are familiar in the areas of antitrust law, unfair competition law and consumer protection law. Importing them into the general realm of the B2B economy would require **extreme care**, especially in the case of **involuntary data sharing**. Inasmuch as the new scheme endeavors to **intervene in the freedom of contracts**, it will need to include balancing mechanisms, for instance, affording the affected company (similar to the case of mandatory B2G data sharing) with a reasonable opportunity to object B2B data access requests based on justified grounds.

Here as well, clearly defining the **category of actors** that are potentially subject to mandatory data access requests is of critical importance. Although not sufficiently underscored in the IIA,[22] this category should include only private corporations with a **market dominance, monopolistic position, market power or strong impact on primary markets and on aftermarkets** (e.g., related services, supplemental products, repair, maintenance).[23] Alongside

[17] Communication, Guidance on sharing private sector data, SWD(2018) 125 final (25.4.2018) (providing specific recommendation for private sector data sharing on matters such as transparency, shared value creation, respect for each others' commercial interests, ensuring undistorted competition and minimizing data lock-in).
[18] Digital Markets Act proposal, Art. 6.
[19] The term "B2B access rights" is used here as a shorthand for legal rights-claims of third parties to gain access to information in the possession/ under the control of the data holder, essentially, "rights of access" or rights to access information. For an analytical discussion on the difference between access rights and rights of access (which is applicable also beyond the copyright law context), *see* Z. Efroni, Access-Right: The Future of Digital Copyright Law (OUP 2011) p.144 ff.
[20] *cf* Fairness and Transparency Regulation (EU) 2019/1150.
[21] IIA, p.5.
[22] *cf* IIA, p.2 (containing references to "data holders with a stronger negotiation power"); p.7 (companies with "privileged positions … in particular OEMs of IoT objects").
[23] A comparable attempt to define very dominant market players (platforms) and subject them to special legal requirements is demonstrated in Art. 3 of the DMA proposal.

the affected market players, the **circumstances** that give rise to a compulsory access to data must receive a clear definition, possibly drawing inspiration from competition law/ antitrust principles that check abuse of market dominance in forms such as blocking access or offering it under monopolistic prices and terms.

Compulsory access must be a **measure of last resort**, meaning, that it is applicable only after all other access avenues have been exhausted. For example, the applicant is required to convincingly demonstrate that (1) access under fair and reasonable terms has been affirmatively denied by the data holder, (2) there is no alternative way to gain access to the data at all or under fair and reasonable terms, (3) the data is essential for the development and implementation of the applicant's business model.[24]

It is further necessary to define the **beneficiaries** of B2B access rights, which are referred to in the IIA as "in particular start-ups and SMEs"[25] as well as the **type of data** subject to this process. One important determination is whether the access rights can apply only to nonpersonal data or rather to personal data as well. Including **personal data** would add a layer of complexity with the obligation to make sure that all data transfers are performed in compliance with data protection law. To avoid this, the data holders may be allowed (or even required) to sufficiently anonymize the data.

Legal principles as those rooted in data protection and privacy regulation reflect **societal, values-based considerations** that go beyond economic efficiency and competition considerations. IIA does not elaborate on this tension beyond stating that the new framework will have to be compatible with existing European data protection and data privacy instruments.[26] The experience so far with discussions around the Data Governance Act proposal demonstrates how intricate such a task can be.[27]

The Data Act will follow an approach making sure that "access to data could be based on fair, reasonable, proportionate, transparent and non-discriminatory terms" (IIA at 5). In the B2B data sharing realm too, the advantages of a **"mixed approach"** (i.e., high-level horizontal regulation of general principles supplemented by sector-specific, granular and adjustable data sharing rules)[28] are considerable. A set of flexible **compensation guidelines** (similar to the one discussed in the context of B2G data sharing) will need to be installed. These guidelines may take into consideration the **size and market position** of the relevant parties, the **economic value** of the data (to the extent this can be determined), the **purpose** of the data access requests and relevant surrounding **industry-specific factors.**

IV. DATA PORTABILITY RIGHTS

The IIA mirrors the ambition to expand existing data portability rights *via* a "legal instrument" both in regard of **personal and nonpersonal data**. In the area of personal data, Article 20 GDPR has been criticized for being too narrow in scope. Its explicit wording covers only personal data the data subject "has provided" actively - under explicit consent or a contract -

[24] *cf* Peitz/Schweitzer: Ein neuer europäischer Ordnungsrahmen für Datenmärkte? NJW 2018, 275, 279.
[25] IIA, p.2.
[26] IIA, pp.2, 4.
[27] *see* EDPB-EDPS Joint Opinion 03/2021 on the DGA proposal (10.03.2021).
[28] *cf* IIA, p.5 (the Data Act would "allow for the modalities to be further specified in sector specific legislation (e.g rules on in-vehicle data are being assessed as part of the review of the Type Approval Regulation")).

but (possibly) not data that has been otherwise collected by the controller.[29] In addition, direct transfer from one provider to another is only covered under the right to data portability "where technically feasible" (Article 20(2) GDPR). Finally, Article 20(2) GDPR lacks mandatory technical specifications to facilitate the exercise of the data portability in case of a direct transfer between controllers.

In light of this critique, **supplementing Article 20 GDPR** with new rules that would render its application more inclusive are **certainly desirable**, possibly by creating a new and independent portability right that fills in these gaps. Efforts in this direction can be observed already in the DMA (applicable to gatekeeper platforms)[30] and the Digital Content and Services Directive that covers return to the consumer of nonpersonal data in the case of termination of certain consumer contracts.[31]

The new or upgraded data portability rights ("Article 20 GDPR-plus" rights) should ideally **apply to both personal and nonpersonal data** and cover instances **beyond data "generated by individual"** (*cf* IIA, at 6) to include also data collection that does not involve an affirmative action of the individual to generate or forward the data to the provider. The coverage of **data collected by IoT devices** is very important, certainly including data which devices collect in the course of using them and without the explicit intention of the individual to send the data to the provider. At the same time, the right should **not necessarily be limited to IoT devices** and also cover online services such as messenger applications, social networks, media streaming services, etc. In certain sectors or classes of products, there might be a need to introduce a **real-time data transfer** (or sharing) right that would allow the end-user to effectuate sharing between providers, a situation that currently is not covered by Article 20 GDPR.

The Data Act should seize the opportunity to provide further instructions to providers regarding **data format and data interfaces** (technical specifications, interoperability, APIs, etc.) in order to facilitate direct and seamless transfer/ sharing between provider at the request of the individual for both personal and nonpersonal data. At the same time, it might be advisable to limit the application of such requirements to certain sectors. Sometimes, data transfer between providers from entirely different industries would not be reasonable or required (e.g., transferring car fuel consumption data to the provider of a fitness application).

In the area of **cloud computing services**, the intention is to expand the data portability rules already laid out in the DMA proposal beyond gatekeeper platforms. The idea is, in this specific data portability context, to enable switching between service providers, make the market more competitive and prevent lock-ins. As opposed to mandatory access rights along the B2B trajectory, here, the cloud service providers would be subject to mandatory portability duties triggered by their customers concerning the *customers'* business data. As compared to Article 20 GDPR-plus rights, the direct issuer of the data transfer request must not necessarily be the individual – it could also be a competing service.

---

[29] Article 29 Working Party (2017), Guidelines on the right to data portability, WP 242 rev.01 16/EN, p.8. At the same time, the Working Party opined that the data portability right should "include the personal data that are observed from the activity of users", naming as examples raw data processed by smart meters or other smart devices. *id* at 10.

[30] Art. 6(1)(a) DMA: Gatekeepers would have to "provide effective portability of data generated through the activity of a business user or end user and shall, in particular, provide tools for end users to facilitate the exercise of data portability, in line with Regulation EU 2016/679, including by the provision of continuous and real-time access".

[31] Art. 16(4) DCDS. In the event of termination of the contract "the trader shall, at the request of the consumer, make available to the consumer any content other than personal data, which was provided or created by the consumer when using the digital content or digital service supplied by the trader".

Indeed, there should be a **clear differentiation between B2B access rights and B2B portability rights** of the type mentioned in the context of cloud computing. One point of distinction could be the identity of the **rightsholder**, another could be the **purpose of transfer** and a third could be the identity of the **transferee**. In the case of B2B portability rights, the involvement of a competent authority appears less urgent, and some technical aspects might require a high-level harmonization.

It should be noted that, generally, creating mandatory requirements concerning format, technical specifications and portability infrastructure (also when sector-specific) is a challenge both in terms of drafting such rules and implementing them by affected businesses. The Data Act therefore should be mindful of factors such as costs and investment private actors will have to carry. To the extent that the said intervention in the market for and contractual relations[32] concerning cloud computing services will render this market **more competitive**, it is **certainly welcome**.

V. INTERFACE WITH LEGAL PROTECTION OF DATABASES

One issue that cuts across various subject areas of the Data Act is its interface with the legal protection of databases, and especially, *sui generis* protection.[33] The IIA emphasizes that the Databases Directive (DB Directive) should not pose an obstacle to the sharing of machine generated data. The Data Act will likely include a review of, and possibly revisions to that Directive. This can be done either by explicitly **limiting the scope** of the DB Directive, introducing **new exceptions** to databases protection it mandates, or both.

A recent evaluation of the DB Directive corroborated earlier assessments that could not establish clear-cut evidence showing that the purpose of the *sui generis* protection, namely, stimulating investments in the European databases industry, has been achieved.[34] The Data Act provides an opportunity to revise the DB Directive or, at minimum, ascertain its limited scope of application to certain type of data(bases) but not to others.

Clearly, the Data Act should not create rules of access to data that (diametrically) contradict the legal protection of databases in the EU. At the same time, the agenda of the DB Directive on the one hand and the agenda of the Data Act on the other hand are quite different. More precisely, the **legal instruments** used for achieving their respective goals are **rather opposite**, namely, imposing restrictions on use of data without the permission of the data holder vs. positive rights-claims of access to and use of data held by another. Whereas the DB Directive seeks to protect private investments by virtue of exclusivity rights[35], access rights proclaimed in the Data Act would compel private actors that have invested in creating data resources to share these resources with the government or with private-commercial entities.

---

[32] An example for imposing binding requirements in B2B contracts (albeit in the limited context of transparency obligations) can be observed in the Fairness and Transparency Regulation (EU) 2019/1150, Art. 3.

[33] Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases, Chapter III.

[34] Commission Staff Working Document, Evaluation of Directive 96/9/EC on the legal protection of databases, SWD(2018)147 final (25.04.2018).

[35] DB Directive, Recital 42 ("Whereas the special right to prevent unauthorized extraction and/or re-utilization relates to acts by the user which go beyond his legitimate rights and thereby harm the investment; whereas the right to prohibit extraction and/or re-utilization of all or a substantial part of the contents relates not only to the manufacture of a parasitical competing product but also to any user who, through his acts, causes significant detriment, evaluated qualitatively or quantitatively, to the investment).

There are essentially three ways to consolidate the two instruments: (1) Exclude data covered by (*sui generis*) databases protection from Data Act access rights, in full or in part; (2) clarify or modify the scope of protection to databases in a way that leaves certain data that is subject to Data Act access rights outside the scope; or (3) carve out exceptions in the DB Directive to accommodate Data Act access rights. The IIA emphasizes that the *sui generis* databases rights should in particular not pose an obstacle to access and sharing of "machine generated data" in the specific context of IoT (IIA at 5-6). Broad exclusion per Option (1) is therefore less viable here, and the general tendency of the IIA actually points in the direction of **modifying or limiting databases protection**.

Options (2) and (3) would require, for a start, a definition of the data (or of specific data requests) that might fall under databases protection but nonetheless be subject to Data Act access rights. An interesting question pertains to **exempting machine generated data**. The data at issue can be considered the data generated by the machine of the potential data *owner*.[36] Excluding such data would require amending the *scope* of database protection. Alternatively, the rule could focus on the technology applied be the *user*, for instance, the method of extracting data from a database, similar to the text and data mining exception in Article 4 of the DSM Copyright Directive.[37] Negating *sui generis* protection in such cases would require a designated *exception* that would exonerate a *prima facie* infringement.

If the main purpose of the Data Act here is to carve out a pathway for B2G and B2B access requests concerning machine generated data (in the IoT context) only, a possible strategy could be simply to add a **statutory exception for such specific access requests under the DB Directive**. A revision of Article 9 DB Directive ("Exceptions to the *sui generis* right") could draw on recent copyright legislation, specifically the text and data mining exception in copyright mentioned above.[38] Alternatively, it can be provided that involuntary data sharing under the Data Act does **not constitute an act of "extraction" or "re-utilization"** covered by Article 7 DB Directive.[39]

A more far-reaching approach could be to **entirely eliminate *sui generis* protection** to databases or at least determine that certain databases or action with respect to certain databases are explicitly outside its scope. For instance, it seems feasible to declare databases composed of machine generated data *ab initio* as not fulfilling the "substantial investment" requirement.[40]

The crux of the matter is not in the legal technique of consolidating between the two instruments. Rather, it is rooted deeper in the fundamental question of whether and to which extent *sui generis* protection should continue to exist in its present form in the face of changing realities and the ambition of the Commission to boost data markets and facilitate free flow of data in the Digital Single Market. **The problem with *sui generis* databases protection** is not

[36] The term "machine generated data" is often used to describe indeed nonpersonal data generated by sensors or similar means in machines operated by the potential owner or possessor of the data. *cf* European Commission, Building a European Data Economy, COM(2017) 9 final, SWD(2017) 2 final (10.01.2017).
[37] Directive (EU) 2019/790 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC, Art. 4.
[38] *id* Art.4(1) ("Member States shall provide for an exception or limitation to the rights provided for in […] for reproductions and extractions of lawfully accessible works and other subject matter for the purposes of text and data mining").
[39] Applying a similar technique, "public landing" is not considered an act of "extraction" or "re-utilization". *see* Art. 7(2) DB Directive.
[40] n. 34, Evaluation of Directive 96/9/EC on the legal protection of databases (2018), pp.46-47.

only that such a right might handicap involuntary data sharing anticipated by the Data Act. **It handicaps data sharing in general.**

Therefore, the Commission is well advised in seizing the opportunity to re-examine and potentially revise the DB Directive. The revision should not be limited only to interface questions with the Data Act or specifically to machine generated data in the IoT context. Creating a better functioning data economy requires the removal of legal barriers and uncertainties pertaining to data flows across all economic sectors. In light of this, the option of **elimination *sui generis* protection should be considered as one plausible solution.** To the extent the Commission reaches the conclusion that private investments in creating, arranging or maintaining data in special, narrow cases (e.g. clear cases of market failure and lack of economic incentives to create valuable datasets in specific contexts), the Commission may revisit ideas to secure limited proprietary interests, subject to appropriate exceptions, in such special cases beyond protection afforded under copyright.[41]

VI. INTERFACE WITH PROTECTION OF TRADE SECRETS

The potential tension between the Data Act and **trade secrets** protection is analyzed alongside (and separately from) the tension in the context of databases protection. The two discussions share some similar outlines, however.

The Trade Secrets Directive[42] seeks to harmonize legal protection of trade secrets throughout the EU (Recitals 7-10 Trade Secrets Directive). Trade Secrets are instruments that explicitly secure certain **exclusivity in information** the possessor of which has made clear efforts to keep secret, namely, *not* to share it with third parties. Accordingly, Member States are required to "provide for the measures, procedures and remedies necessary to ensure the availability of civil redress against the unlawful acquisition, use and disclosure of trade secrets."[43] Infringing on a trade secrete can be described as a commercial tort established when the relevant acts (acquisition, use, disclosure) are done **unlawfully**.

It is worth noting that the Trade Secrets Directive is a fairly recent piece of legislation. It includes a number of concepts and requirements that to some extent are still open to interpretation. For example, Article 2(a) Trade Secrets Directive contains the condition that the information "has been subject to *reasonable steps under the circumstances*, by the person lawfully in control of the information, to keep it secret" (emphasis added).

The caselaw at EU and national levels concerning the interpretation and the application of the new Directive are still developing.[44] Indeed, one important interpretation issue concerns the **definition of a trade secret** and whether, when and which data falls under this definition.[45] To the extent certain business data qualifies as a trade secret under the terms of the Trade Secrets

[41] *cf* European Commission, Building a European Data Economy, COM(2017) 9 final, SWD(2017) 2 final (10.01.2017, p.11 ff (including the idea to provide a narrowly tailored "data producer's right", p.13).
[42] Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure.
[43] Trade Secrets Directive, Art. 6.1.
[44] E.g. in Germany, courts are only beginning to develop the jurisprudence interpreting the German Trade Secrets Law that had transposed the Trade Secrets Directive. The German Federal Administrative Court established lenient standards for what constitutes sufficient steps for keeping the information secret. *see* BVerwG. 10 C 22/19, 17.06.2020.
[45] The German Federal Constitutional Court has recently ruled that also metadata of source code files such as file name, type and size can be protected as trade secrets. BVerfG. 20 F 3.19, 05.03.2020.

Directive, obligating the owner to share such data with others would significantly **diminish its proprietary position**. The IIA states that "[p]rotection of confidential business data and trade secrets should also be safeguarded."[46] The IIA, however, does not elaborate on how consolidation between the two legislations can be achieved.

Measures for consolidation can be found already in the language of the Trade Secrets Directive. It provides that acquisition, use and disclosure of information must be "unlawful" to be infringing. Furthermore, Section 5(d) of the Directive provides that "Member States shall ensure that an application for the measures, procedures and remedies provided for in this Directive is dismissed where the alleged acquisition, use or disclosure of the trade secret was carried out […] for the purpose of protecting a legitimate interest recognised by Union or national law." Inasmuch as the Data Act establishes that certain **data sharing requests are lawful or carried out for purpose of protecting a legitimate interest,** trade secrets protection would step back. The fact that the IIA mentions the problem multiple times in multiple contexts, however, suggests that the solution is perhaps not that simple.

If the intention behind these statements is not to compromise trade secrets protection at all, the Data Act could declare that all data sharing requests under its regime are **without prejudice** to trade secrets protection. Yet, such a rule might create a **perverse incentive to keep information secret** only or primarily in order to escape data sharing duties under the Data Act.

A midway solution could apply the following four principles: (1) Trade Secrets protection is declared an **affirmative defense** against data sharing requests under the Data Act; (2) a **competent authority** in charge of overseeing the implementation of the Data Act has the power - in a discrete proceeding - to determine whether the information is in principle subject to trade secrets protection and whether the data access request would *prima facie* infringe on the trade secret; (3) if the answer to (2) is positive, the authority will perform a **balance of interests** analysis and determine whether private or public interests in favor of sharing outweigh the interest of the trade secrete owner in keeping the information secret; (4) in such case, that authority will determine the **terms and conditions** for sharing the information while making efforts to minimize the harm to the owner and at the same time fulfilling the purpose of the data sharing request.

VII. INTERFACE WITH REGULATION OF ARTIFICIAL INTELLIGENCE

The IIA points out to findings showing that there are "difficulties linked to the access to and the (legal and technical) ability to use data as key barriers to data-driven innovation using techniques of Big Data analytics and Artificial Intelligence in the EU" (IIA at 8). It is certainly conceivable that data access requests under the Data Act will be issued for purpose of developing AI systems. However, interface questions between recent regulation initiatives in the area of AI, particularly the Artificial Intelligence Act (AIA) proposal,[47] are not addressed in the IIA at all.

The AIA proposal provides *inter alia* requirements that apply to **high-risk AI systems** as defined in Article 6 thereto. Article 10 AIA sets forth a list of data types and data governance requirements that apply to such systems, and specifically, to training, validation and testing

[46] IIA, p4.
[47] COM(2021) 206 final, 2021/0106(COD).

data sets. For instance, Article 10(3) AIA provides that "[t]raining, validation and testing data sets shall be relevant, representative, free of errors and complete. They shall have the appropriate statistical properties, including, where applicable, as regards the persons or groups of persons on which the high-risk AI system is intended to be used."

Article 16 AIA states that the "**providers***"* of high-risk AI systems are subject to these (and other) requirements under the AIA. However, Article 28 AIA adds that also third parties, such as distributers, importers and users, can be considered "providers" to the extent that they modify the intended purpose of high-risk AI system (subsection (b)) or make a substantial modification to the high-risk AI system (subsection (c)).

A question arises whether the applicant of a Data Act sharing request should, specifically, **indicate its intention to make modifications** per the foregoing provisions. Further questions are whether such intention should have any influence on the decision whether to enforce data sharing as requested, and whether the transfer could have any adverse implications for the initial provider of a high-risk AI system in terms of liability and compliance with the AIA and other applicable regulation.

The AIA envisages the establishment of a **notification authority** "responsible for setting up and carrying out the necessary procedures for the assessment, designation and notification of conformity assessment bodies and for their monitoring."[48] This authority and the notification procedure (Article 32 AIA ff.) joins a number of existing and forthcoming authorities and procedures within the broader project of regulating data processing, data utilization, data markets and data flows in the EU. Examples alongside the AIA are data protection authorities under the GDPR, EU competition authorities, competent authorities under the proposed DGA and possibly a designated authority under the Data Act.

As a general, high-level comment regarding data regulation in the EU, the multiplication of supervision authorities within the Digital Single Market renders the regulative landscape ever more complex and the compliance efforts ever more cumbersome for data-driven enterprises and other stakeholders. The Data Act, in itself, is expected to introduce a complex regulative apparatus that will need to operate in harmony with all other apparatuses. It is advisable at this stage of executing the various initiatives under the EU data strategy to consider a certain institutional consolidation.

The creation of a smoothly functioning common European data space[49] could benefit from a more coherent and efficient compliance structure that provides regulated parties access to a one-stop-shop "clearing house". Such an institution can be imagined as a "meta-authority" with professional and legal competences to examine all, or at least the most critical aspects of a given regulated act or enterprise under EU law. The meta-authority could than approve, disapprove or set conditions (including providing guidance, requiring information and referring specific matters to specialized authorities) regarding data-related endeavors and thereby facilitate a less fragmented compliance matrix.

[48] Art. 30 AIA ff.
[49] Towards a Common European Data Space, COM(2018) 232 final (25.04.2018).

VIII. SUMMARY AND RECOMMENDATIONS

The Data Act will introduce important new rules concerning *inter alia* **access to data** held by the private sector, **data portability** rights, and the interplay between **proprietary interests** pertaining to data on the one hand, and the newly established **rights of access to the data** on the other hand. Such new rules are expected to have more than just a marginal impact on the EU data economy. The nature and magnitude of the impact will depend to a large extent on the **specific design** of the rules and the **balance of interests** they will strike.

Regulation of information markets is a **complex and delicate endeavor**. The success of the Data Act in achieving its goals will depend on the specific legal **formulation** of new rights and duties, the **mechanisms** applied for implementing and overseeing its implementation, and **interrelations** between the new legal instrument and existing/ forthcoming legal instruments. In approaching the challenge, we strongly recommend that the following points are taken into consideration:

A. B2G Data Sharing

1. Developing legal and technical infrastructure for effective Business-to-Government data sharing can have an **important contribution** to using data for common good purposes.

2. There is a crucial difference between facilitating **voluntary** data flows (or "data donation") from the business sector to the public sector and the creation of **legal duties** to share private-business data with the government.

3. The later instrument (**mandatory B2G access rights**) requires an architecture that takes into account, alongside potential **benefits** to the public interest, also potential **risks to commercial interests** and broader effects of such rights on data markets, incentives, competition and fundamental rights.

4. A **mixed approach** is recommended, according to which general principles for B2G data sharing apply horizontally and are supplemented by a sector-specific set of adaptable rules that take into account the specific characteristics of and the (evolving) conditions within the affected sectors.

5. The horizontal and sector-specific regulations need to provide a set of **clear definitions and scope rules** concerning the **actors** subjected the new scheme, the **kinds of data** they cover, and the common good **purposes** for which data may be used.

6. The principles already identified by the European Commission should be observed and reflected in the new rules: Proportionality, purpose limitation, minimizing of harm to legitimate interests, consideration of the public interest in contractual conditions, data quality management and transparency.

7. It is recommended to draft flexible **compensation guidelines** for business subject to mandatory B2G access rights that take into account factors such as the **size** of the company, **market value** of the data, the **purpose** of obtaining the data as well as the anticipated **public benefits**.

8. A designated **competent authority** should be responsible for the implementation of the scheme, reviewing access requests, determining remunerations and deciding on disputes in case of oppositions.

B. B2B Data Sharing

1. The observations above are **applicable *mutatis mutandis*** to new regulation in the area of involuntary B2B data sharing (**B2B access rights**).

2. Adopting a mechanism similar to compulsory licensing and restrictions concerning the content of private contracts that are familiar from the areas of IP, competition law and consumer protection law **require extreme care**.

3. Involuntary B2B access rights should be a **measure of last resort**, namely, where access under fair and reasonable terms has been affirmatively denied by the data holder, there is no alternative way to gain access to the data at all or under fair and reasonable terms, and the data is essential for the development and implementation of the applicant's business model.

4. B2B access rights should be applicable in principle only against companies that occupy a **dominant position** in the relevant market(s) and only when such companies **abuse their market power** by withholding access or offering it under exploitative terms.

C. Data Portability Rights

1. Expanding the scope of the existing data portability rights (mainly under Article 20 GDPR) beyond their limited application area to cover, for instance, **nonpersonal data** or cases where the individual **did not actively "provide"** the data, is **desirable**.

2. Effective data portability rights ("Article 20 GDPR-plus rights") should apply in principle to **data collected by IoT devices**. In addition, such rights might also be warranted in cases where there is no smart device involved (pure online services), where Article 20 GDPR is inapplicable or insufficient, and where **real-time data transfer** between providers is required.

3. Harmonizing technical standards, technical requirements and interoperability would make sense, especially **within sectors** and while being mindful of factors such as costs and necessity/ justifiability of portability requests under relevant market and technology conditions.

4. Providing mandatory standards for **B2B contracts** in the area of **cloud computing services** is **warranted** especially when **market failures** and barriers to robust competition can be identified, for instance, to prevent lock-ins and abusive/ anti-competitive behavior.

5. There should be a clear **differentiation** between B2B access rights (under VIII.B) and B2B portability rights. Points of distinction can be the **identity** of the portability **rightsholder** and **dutyholder**, the **data transferee** and also the **purpose and scope** of the data transfer.

6. In general, B2B access rights should be **more restrictive** and subject to **more safeguards** than data portability rights.

D. Interface with Databases Protection Law

1. There is a basic **tension** between proprietary interests in data and a mandatory access rights regime.

2. ***Sui generis* rights** in databases should be **re-evaluated** and possibly abolished if concluded that their harms (overprotection, legal uncertainty, transaction costs, barriers for free flow of data and utilization) outweigh their benefits (effectively boosting the creation of more databases).

3. A revision of the *sui generis* databases protection could do away with proprietary claims not only in connection with **machine generate data in the IoT sector,** but also other data sets the creation, arrangement, management and utilization of which should not by subject to property exclusion rights from a normative and economic perspective.

E. Interface with Trade Secrets Law

1. The rationale and justifications for providing legal protection to **trade secret**s remain **valid** also in the data economy and also in light of the general endeavor to enable more data utilization, data re-use, data-driven innovation and value creation.

2. A mandatory access right regime **should not overly diminish the legal position of trade secrets owners**. Trade secrets protection may operate as an **affirmative defense** to data access requests subject to a dispute resolution mechanism.

3. A competent authority may assume an important role in examining data access **requests, defenses or objections** and determining whether and under which terms the data should be shared with the applicant.

F. Interface with AI Regulation and Institutional Consolidation of Compliance Mechanisms

1. Interface questions between access rights under the Data Act and regulation of **artificial intelligence** systems in the EU (especially the Artificial Intelligence Act) should be **examined more closely**.

2. Specifically, it should be examined whether access to data requests under the Data Act in the case of high-risk AI systems might **impact the legal positions** of the initial AI system provider and the data access applicant.

3. Generally, the envisaged supervision authority under the AIA, the proposal here concerning a competent authority under the Data Act and a myriad of existing and emerging authorities in other areas of data (markets) regulation create an ever more complex **legal and compliance matrix**. Institutional consolidation and harmonization efforts that cover the entire spectrum of data regulation in the EU are certainly encouraged.

***