

Sharing Data (Anti-)Competitively

Will European data holders need to change their ways
under the proposed new data legislation?

The logo for data.europa.eu features the text 'data.europa.eu' in a white, lowercase, sans-serif font. Each letter is punctuated with a small, colored dot (yellow, red, blue, or orange) positioned above or below the letter.

data.europa.eu

The official portal for European data

This study has been prepared as part of data.europa.eu. Data.europa.eu is an initiative of the European Commission. The Publications Office of the European Union is responsible for contract management of data.europa.eu.

For more information about this paper, please contact the following.

European Commission

Directorate-General for Communications Networks, Content and Technology
Unit G.1 Data Policy and Innovation
Email: CNECT-G1@ec.europa.eu

data.europa.eu

Email: info@data.europa.eu

Authors:

Hans Graux

Last update: Month 2022

<https://data.europa.eu/>

DISCLAIMER

The information and views set out in this publication are those of the author(s) and do not necessarily reflect the official opinion of the Commission. The Commission does not guarantee the accuracy of the data included in this study. Neither the Commission nor any person acting on the Commission's behalf may be held responsible for the use that may be made of the information contained therein.

Luxembourg: Publications Office of the European Union, 2022

© European Union, 2022



The reuse policy of European Commission documents is implemented by Commission Decision 2011/833/EU of 12 December 2011 on the reuse of Commission documents (OJ L 330, 14.12.2011, p. 39). Unless otherwise noted, the reuse of this document is authorised under a Creative Commons Attribution 4.0 International (CC-BY 4.0) licence (<https://creativecommons.org/licences/by/4.0/>). This means that reuse is allowed provided appropriate credit is given and any changes are indicated.

OA-08-22-326-EN-N ISBN 978-92-78-43383-3

doi: 10.2830/913446

Contents

1. Introduction – how does data sharing relate to competition law?.....	5
2. Looking at the world today: when and how does existing EU competition law impact data sharing practices?.....	7
3. Competition challenges in European data markets	10
4. New legislative intervention proposed via the Data Act – what is the impact on competition?	11
5. Observations and guidance on compliant data sharing practices	14
6. Bibliography	16

1. Introduction – how does data sharing relate to competition law?

In the digital economy, data has been referred to as the ‘new gold’ for a long time, and for good reasons. When Vice-President of the European Commission for the Digital Agenda Neelie Kroes [used this analogy in 2011](#), the digital economy was already growing rapidly, and the first business giants had already established some degree of dominance in cloud computing and other online services.

It was becoming clear that more and more markets were facing so-called network effects: the more data a company could hold, the better and more efficiently it could work. A company that could increase the volume and quality of its data continuously and more quickly than its competitors would be able to provide better services to its customers, thus extending its market leadership.

As a corollary, it became increasingly clear that the ability to collect and retain exclusive control over data could also be used as a market control mechanism. If a competitor or an innovator would require access to certain data to build or expand its own services, and this data would only be accessible with the cooperation of the data holder, then that data holder could in principle exercise significant influence over its market. Its competitors would not be able to offer their services, and innovators would not be able to bring their new ideas to fruition, outside of the terms that the data holder would be willing to support.

By way of a simple example, a company might offer an energy management platform to consumers, which allows them to track their energy consumption, and steer the behaviour of smart devices (e.g. polling electricity capacity in a battery, production from solar panels, charging needs of an electric vehicle, operating times of dishwashers or laundry machines). If the data from those devices is not made easily accessible by their manufacturers, then such energy management platforms could only be provided by (or with the cooperation of) the smart device manufacturers. An aspiring competitor, who has created a similar platform, but is unable to access the devices’ data, would not be able to compete in the same market. In such cases, consumers have fewer (or no) choices for a platform, and competition is hampered.

As the example shows, this challenge is not limited to fully digital environments. Physical devices are increasingly ‘smart’, in the sense that they collect, generate, or analyse ever more data, and that this data is critical to enable their use. Not being able to access that data means that users have only a single point of contact for any services relating to that device, and that competition becomes impossible. In very simple terms: a smart fridge, car or elevator can only be diagnosed, maintained and repaired by a service provider who can get to the data and understand it. If the manufacturer refuses to share such data, it monopolises all these corollary services, preventing the market entry of competitors and hampering potential innovations related to the device.

Essentially, a large and powerful data holder can hold the market to ransom, by imposing unreasonable terms for access to data – e.g. by charging excessively or by forbidding any use that could pose a risk

to its bottom line – or simply refusing data access outright – e.g. to buy enough time to develop a competing or superior service.

In some cases, this behaviour occurs in a competitive market, where alternative data sources are available. Restraining access to a data source can then be considered as normal and healthy: companies often try to control the key assets in which they've invested, and competitors or innovators have no inherent right to benefit from those investments. If they wish to generate their own business opportunities, they should just invest in creating an alternative. But in other cases, the behaviour can be considered as anti-competitive, notably when there is no alternative data source, the data holder has a dominant market position, and abuses this position to limit competition or innovation. In those instances, the behaviour must be measured by the yardstick of competition law.

This issue is not entirely new, of course. Competition law has been a staple ingredient of European economic policy and legislation for many decades now. Its central importance in the EU is immediately apparent from the fact that the main provisions of competition law can be found directly in the [Treaty on the Functioning of the European Union](#) itself (mainly in Articles 101 and 102). The application of these rules to the digital economy and to digital data, which are also within the EU's competences as a part of the (digital) single market, is however not always easy, and recently proposed new legislation – notably the proposal for a Data Act – could impact how competition law questions are dealt with.

While some studies have examined the application of competition law to the data economy – as shown in the bibliography of this report – none have examined the anticipated impact of the Data Act on the behaviour of data holders, or on its potential remedies available to aspiring data users. The data.europa.eu portal does contain multiple studies on openness in general, and on the expected potential of data spaces as an enabler to data sharing, none thus far have examined competition law challenges in any detail.

With that in mind, this legal research paper will examine how existing general EU competition law has affected data holders and data markets in the past, and how the newly proposed legislation is likely to affect the status quo. The goal is not only to describe general principles and trends, but also to summarise the main practices that are likely to be labelled as anti-competitive. These are the questions that will be addressed in this short analytical paper.

2. Looking at the world today: when and how does existing EU competition law impact data sharing practices?

In the past, EU competition law has been used repeatedly to tackle a range of anti-competitive data management practices, based on the general provisions of the Treaty on the Functioning of the European Union (TFEU). Without entering into the details, Article 101 of the Treaty generally prohibits any agreements or practices that may affect trade between Member States and “*which have as their object or effect the prevention, restriction or distortion of competition within the internal market*”. For instance, the TFEU references practices that limit or control markets and technical developments, which are to be considered legally void. This provision could be applied when a data holder uses data sharing agreements that e.g. limit the development of new services which are built on top of already accessible data.

There is always a risk that an overly rigid interpretation of Article 101 can actually have negative effects on competition and innovation. Horizontal cooperation agreements (between companies operating at the same level in the market) can also create benefits by allowing them to bundle and link their complementary activities, skills or assets. To enable such favourable cooperations – which inevitably require some data sharing – to exist, the EU supports a mechanism of so-called Horizontal Block Exemption Regulations (HBERs). The HBERs are [a set of two Regulations from the Commission](#) - Regulation No 1217/2010 and No 1218/2010 – which allow certain well delineated and regulated agreements to be exempted from the application of Article 101. The scoping of these HBERs are set out in specific guidelines, and include certain information exchange agreements.

Information exchange can include data shared directly between competitors, data shared indirectly through a common agency or a third party, or data shared through the companies’ suppliers or retailers. Such exchanges can be beneficial for the companies concerned, and for consumers and society as a whole, through their ability to accelerate innovation and increase efficiency. Under the HBER framework, information exchange agreements are only considered to restrict competition where competitors exchange individualised information regarding intended future prices or quantities. The HBERs effectively create a safe harbour for those narrowly scoped categories of data sharing agreements.

Article 101 is however not particularly useful in situations where a data holder simply refuses to make data accessible to a third party. In those instances, Article 102 of the TFEU is more relevant, since it in general bans any abuse of a dominant position within the internal market, or in a substantial part of it. Examples of such abuse listed in the TFEU include the imposition of unfair pricing or other unfair trading conditions; limiting production, markets or technical development to the prejudice of consumers; or applying dissimilar conditions to equivalent transactions with other trading parties, thereby placing them at a competitive disadvantage.

These provisions are not trivial to apply in the data economy. The central question is what exactly constitutes a dominant position, and how exactly one should define the relevant market in which the dominance supposedly exists. Guidance on the definition of a market is addressed by a [1997 Commission Notice](#), which still remains valid today, and which is also applied to data markets. The Notice stresses that this requires a combined consideration of the product and geographic markets. The product market comprises all products and/or services which are regarded as interchangeable or substitutable by the consumer, by reason of the products' characteristics, their prices and their intended use. The geographic market comprises the area in which the undertakings concerned are involved in the supply and demand of products or services, in which the conditions of competition are sufficiently homogeneous and which can be distinguished from neighbouring areas because the conditions of competition are appreciably different in those area.

These criteria can be applied to digital environments and data markets as well, since they also allow the consideration of which data (if any) can serve as substitutes, and in which geography the data is usable. In extreme situations – e.g. there is no substitute for the data, and the market covers all of the EU – the market is effectively a monopoly, and dominance of the data holder is trivial to determine. Most cases are however a bit more complicated, since there may be partial or imperfect substitutes for certain data, the use of the data (and thus the market for them) may change rapidly, and there can be discussions on whether a data holder is actively providing its services in a certain geographic region.

All of these challenges make it complex to determine what exactly could constitute a 'market' for data, or even whether a market for data exists independently of the market for products or services that are built around such data. Continuing the example from the introduction, one might reasonably question whether there is a market for smart device data as such (e.g. a market for solar panel electricity production data, or for crop yield data), or rather whether there is only a market for ancillary services that require this data (such as maintenance and repair of devices, or for agricultural analytics services). The distinction is not trivial, considering the market definition factors mentioned above: a repair service may e.g. operate only locally in a market where there is only one (therefore clearly dominant) manufacturer, whereas the manufacturer is a part of a global market in which it has only a marginal market share. The analysis of the market can therefore be very different from the perspective of the data holder or from the perspective of the data user.

The 1997 Notice is currently undergoing evaluation, precisely to clarify these points, and their applicability to data. The revision is expected to create greater flexibility and agility in the assessment of what constitutes the relevant market, taking into account e.g. that data sharing can be multi-sided (with many different types of parties acting as data providers *and* data consumers simultaneously), and that data ecosystems can evolve rapidly, with use cases for the data being added – thus potentially expanding the relevant market – or removed – thus shrinking it.

As the [2019 report on Competition Policy for the Digital Era](#) noted, *"in digital markets, we should put less emphasis on analysis of market definition, and more emphasis on theories of harm and identification of anti-competitive strategies. At the same time, even if in some consumer-facing markets – according to their own account – firms compete to draw consumers into more or less comprehensive ecosystems, markets for specific products or services will persist from a consumer's perspective, and should continue to be analysed separately, alongside competition on (possible) markets for digital*

ecosystems. Where the firms' lock-in strategies are successful, and consumers find it difficult to leave a digital ecosystem, ecosystem-specific aftermarkets may need to be defined."

Since no specific guidance on data markets exists yet, the interpretation of Article 102 should be informed by looking at comparable prior cases. The Court of Justice has issued five landmark decisions that could be particularly useful in this respect; specifically the cases [Magill \(C-241/91 and C-242/91\)](#), [IMS Health \(C-218/01\)](#), [Bronner \(C-7/97\)](#), [Microsoft \(T-201/04\)](#) and [Huawei \(C-170/13\)](#). Through these cases, the Court in practice applied the so-called "essential facility" doctrine – without explicitly referring to it as such – under which dominant firms can be compelled to provide access to inputs or assets that are essential for competitors in order to enter a related market. According to a number of legal academics, this doctrine could be applied to data as well.

Based on an [analysis of these cases](#), four conditions generally need to be fulfilled for an action based on competition law principles to lead to an obligation to make an essential facility (potentially including data) available to a third party:

- that the data is indispensable for the creation of a downstream product or service; if alternative data exists, there is no obligation for a data holder to share.
- that there would not be any effective competition between the upstream and downstream product (i.e. the downstream product will compete with other downstream products, but a competitor cannot claim data access rights purely to create a direct copy of the data holder's original (upstream) service);
- that refusal would prevent the emergence of the second product; and
- that there is no objective reason for the refusal – i.e. it must be practically feasible to allow access to the essential facility.

If all four factors are present, data could be deemed an essential facility. A refusal of that data holder to grant a third party access to their data on reasonable terms would be qualified as an abuse of dominance. A data monopolist could thus be forced in certain cases to make parts of their unique data available, allowing competition law to be used in cases of a 'refusal to deal' – i.e. when a data holder simply refuses to enter into negotiations.

Reliance on existing competition law is thus theoretically possible to address some potentially abusive cases. However, the approach is not without its limitations. Leaving aside the complex issues of identifying markets and assessing dominance, the requirements of the essential facility doctrine are quite strict. Alternative data often does exist, but is simply less accessible, less perfect, or more expensive. Nonetheless, if an alternative is available, the doctrine cannot be applied.

Moreover, the data holder's refusal to share must impede the development of a new and non-competing product; if a company merely wants to enter an existing market with a directly competing service, the doctrine also does not apply. The Court has also interpreted the criteria to mean that the dominant firm must itself already be active in the related market. In other words, if the data holder is not serving a given market (e.g. analytics services of a given data set), and an innovator wishes to enter this market, data access cannot be compelled. Clearly, not all challenges can be resolved through

existing competition law. With that in mind, the EU has been examining new initiatives, as will be explored below.

3. Competition challenges in European data markets

The section above described the potential application of existing competition law to any market for data. It also showed however that it has some shortcomings and weaknesses. Largely, these are linked to the fact that the TFEU provisions are generic, and don't focus specifically on data, or on data economies. The complexity of applying competition law (and concepts like a market, dominant position, or essential facility) to a data environment make the outcome unpredictable.

Moreover, competition law is not designed to address every possible challenge in detail. As the analysis above showed, it can be useful in cases where a data holder has a dominant position in a specific market for data where no alternative exists, and where the intention is to enter that same market; but this hardly covers all possible challenges. Innovators who depend on data access have no real recourse under competition law if they want to build a service that is not provided by the data holder. Moreover, as was highlighted in a [2022 European Commission Study on model contract terms and fairness control in data sharing](#), competition law is not particularly accessible to SMEs, since it is largely dependent on ex post competition enforcement through legal procedures – i.e. SMEs need to engage in potentially complex, lengthy and expensive proceedings in order to determine whether a breach of competition law exists.

As a result, that same study found that current data sharing practices in the EU were suboptimal from an economics perspective. Market failures occur specifically when there is a lack of competition for data, and data providers are thus in a data monopoly situation, according to the study, thus linking insufficient data sharing directly to a lack of competition. The study also noted that market failures can happen when a data holder is able to implement a value chain model that enables gatekeeping. In those cases, new services or products are inhibited because of a data holder whose cooperation is required to access relevant data. This observation is relevant as well, in light of the analysis of EU competition law above, since it is precisely a challenge that the application of the TFEU would be unlikely to cover appropriately. The economic impact is significant, and the study estimated that optimal data sharing could trigger an additional EUR 185 billion of profits over a period of 10 years (2021-2030).

For its economic assessments, the 2022 study was largely a meta-study that built on prior research, all of which pointed in the same direction: the market for data sharing is not optimally competitive, and the application of traditional competition hasn't been able to address this problem, leading to clear and substantial economic harms to companies and to society as a whole. Clearly, there was room for improvement.

4. New legislative intervention proposed via the Data Act – what is the impact on competition?

In the sections above, the analysis has focused principally on the general approach and functioning of traditional competition law, based on the principles enshrined in the TFEU. It is worth recognising that the TFEU is of course not the only source of EU law that affects how data holders and aspiring data users compete, and how they are encouraged or required to compete fairly. By way of non-exhaustive examples:

- The fundamental right to the protection of personal data is protected principally by the well known [General Data Protection Regulation](#). In addition to protecting individual rights, the GDPR however also provides a harmonisation of the European internal market for personal data processing activities. It ensures that data can flow freely within the EU, under a common set of principles, thus facilitating equal competition. In the absence of the GDPR, companies that collect, trade or otherwise process personal data could gain an unfair competitive advantage by making use of data in an unethical manner that would be unlawful for their competitors. In that sense, the GDPR is also a competition enabling instrument.
- Similarly, the so-called [Regulation on the free flow of non-personal data](#) sets out a framework enabling the free flow of data other than personal data within the Union, by laying down rules relating to data localisation requirements, the availability of data to competent authorities and the porting of data for professional users. Again, this provides a common ground that's conducive to innovation, e.g. by limiting the circumstances under which national law could require data storage within a Member State's borders, and by supporting a data portability principle that facilitates moving data from one service provider to another. Again, this creates a shared pro-competition framework in the EU.
- Other legal frameworks that focused on digital services and the digital economy similarly directly or indirectly supported fair competition, such as:
 - the [e-Commerce Directive](#), ensuring that so-called information society services would not be subject to prior authorisation regimes;
 - the successive public sector information (PSI) directives that culminated so far in the present [Open Data Directive](#), ensuring that companies could re-use and build on public sector information, including certain defined high value data sets, on equal footing across the EU
 - the [broad array of directives on intellectual property rights](#) that focus on the digital single market and digital services, including also database rights, ensuring that such exclusivity rights are harmonised to a large degree,
 - Directives on fair market practices, such as the recently amended [Unfair Commercial Practices Directive](#), which limit practices that could result in unfair competitive circumstances;
 - The recent [Regulation on promoting fairness and transparency for business users of online intermediation services](#), aiming to facilitate the use of such services in a B2B context, thus supporting the accessibility of enforcement mechanisms.

Through these instruments, and many others, the EU has contributed to the emergence of a competitive market for digital services in general. In the past few years however, this legislative framework has been expanded and refined extensively, and is still undergoing further finetuning. Notably, the [European Data Strategy and current EU data policies](#) were adopted to encourage, facilitate and sometimes mandate the sharing of data on fair terms, noting explicitly that *“Europe aims to capture the benefits of better use of data, including greater productivity and competitive markets”*.

This is also visible in the legislative package that was proposed as a part of the Strategy, including notably the proposed [Data Act](#) and the [Digital Markets Act](#), and the [adopted Data Governance Act](#) and [Digital Services Act](#). All of these aim to improve the efficiency and effectiveness of European data markets, thus increasing competition, innovation and socio-economic progress. None of the initiatives amend or change EU competition legislation, which thus remains usable in specific instances where abuse of a dominant market position can be demonstrated. However, in practice they do create a complementary legal framework that strongly affects how a lack of competition can be addressed.

The Data Act will be discussed in greater detail below, but the general interaction and role of these instruments (particularly from a competition law perspective) can be briefly summarized as follows:

- The Digital Services Act is effectively a modernisation of the aforementioned e-Commerce Directive, which is amended by the Act. It revises the rules for so-called intermediary services (including e.g. hosting and caching services), by modernising the liability rules for such services, imposing specific due diligence obligations on them, and streamlining the implementation and enforcement of the Act. This indirectly supports competition by ensuring that comparable service providers are not subject to substantively different national laws.
- The Data Governance Act creates a specific legal framework to support data sharing, notably by regulating specialised data intermediation services, and by establishing principles for common European data spaces in strategic domains, in sectors such as health, environment, energy, agriculture, mobility, finance, manufacturing, public administration and skills. It furthermore establishes a European Data Innovation Board, whose remit includes the facilitation of data sharing through intermediation, standardisation, portability and interoperability (among other tasks).
- The proposed Digital Markets Act would identify a small subset of large online platforms as so-called “gatekeepers”, who have a significant impact on the internal market; provide a core platform service which is an important gateway for business users to reach end users; and enjoy an entrenched and durable position in its operations (or it is foreseeable that it will enjoy such a position in the near future). In practical terms, this would relate to large ICT companies that can effectively dominate their markets, potentially also via anti-competitive measures. The Act would both mandate certain pro-competitive activities (e.g. enabling interoperability, or allow users to access their own data) and forbid certain anti-competitive practices (e.g. favouring their own offerings in rankings over those of competitors, or cross-using the personal data of their end users across separate and unrelated services).

For the purposes of this report however, we will focus on the anticipated impact of the proposed Data Act. This Act generally seeks to stimulate business-to-business data sharing, including through the concept of data spaces. Although not directly linked to competition law, it aims to ensure that access

to certain data is possible more frequently, and on fairer terms, thus enabling data to be used as a resource for economic growth, competitiveness, innovation, and job creation, specifically by:

- making data generated by the use of a product or related service available to the user of this product or service (relevant specifically to connected devices, smart devices, and the Internet of Things),
- making data available by data holders to data recipients,
- mandatory business-to-government data sharing, where there is an exceptional need,
- addressing unfair terms contractual related to sharing of data,
- making the switching between data processing services easier,
- protecting EU non-personal data held by certain service providers.

Focusing specifically on the parts of the Data Act proposal that target data holders engaged in potentially anti-competitive practices, the proposed Act requires data holders to make connected device data available to any third party which acts upon a request by the user of the device. This right can be particularly useful for aspiring providers of repair or other aftermarket services (such as the smart fridges mentioned above). In this way, the Commission hopes to facilitate competition and innovation. It is worth noting that this is a useful complement to traditional competition law, since the TFEU would not be able to remedy such situations in all cases: if the data holder is not engaged in the market of maintenance services, it would not be required to provide fair data access to third parties under the TFEU. Under the Data Act however, this would be the case.

The obligation comes with some conditions, of course. The data holder will have to make the data available to third parties under fair, reasonable and non-discriminatory terms and in a transparent manner. In particular, it cannot discriminate between comparable categories of recipients, for example by giving different quality of data to its linked enterprises than to non-partners. The holder may charge a reasonable fee as compensation for the data access, comprised of the costs necessary for data reproduction, dissemination via electronic means and storage, but not of data collection or production. This is significantly more detailed as an obligation than under traditional competition law. Micro and small enterprises are exempt from these obligations as data holders, which could be seen as a recasting of the market dominance criterion under the TFEU (at least if one accepts that, as a general rule, micro and small enterprises struggle to dominate their markets).

Separate from this data access obligation imposed on some data holders, the proposed Data Act also contains provisions that govern contracts in relation to data sharing. Not all such agreements are affected: the proposed Act would intervene only when it comes to terms concerning access to and use of data which are unilaterally (i.e. without negotiation) imposed by an enterprise on a micro, small or medium-sized enterprise. The proposal provides a general test of unfairness, along with a series of examples that are always considered unfair (a black list), or which are presumed to be unfair but where that presumption can be refuted (a grey list). Examples of always unfair contractual terms include, for example, excluding or limiting liability of the party which unilaterally imposed the terms for intentional acts or gross negligence. Grey list examples include provisions allowing the imposing party to access and use data of the weaker contracting party in a manner that is significantly detrimental to the

legitimate interests of this other contracting party, or provisions enabling the stronger party to terminate the contract with unreasonably short notice.

Again, this is a useful complement to the general competition law provisions of the TFEU. The black list and grey list approach of the proposed Data Act is arguably more straightforward and accessible to SMEs, since it provides a clear list of examples of market practices that are deemed abusive, without requiring a separate identification of the relevant market or any consideration of dominance. Moreover, violations of the Data Act could be invoked before any commercial court with competence over B2B disputes, without requiring recourse to specialised competition law courts.

As a result, the proposed Data Act would complement, but not replace, the traditional competition law provisions, in a manner that is less ambiguous and more focused on the specific challenges of B2B data sharing.

5. Observations and guidance on compliant data sharing practices

As the overview above shows, at this time the TFEU is the main framework still to assess legal compliance of data sharing practices with competition law, since the Data Act is still in the proposal stage and under discussion. Moreover, the provisions and scoping of the relevant Articles of the TFEU are fairly generic and high level, and existing case law does not focus in particular on the data economy. Nonetheless, there are some clear observations and guidance that can be provided.

First and foremost, the data holder should have a clear **understanding of the market** (global, European, or local) in which they are active, or more precisely, which services they are offering in that market that generate or use data. This is a critical question to determine the effects of competition law. A data holder that refuses to allow third parties to develop innovative services that require data access when it is not offering equivalent services itself, is possibly behaving in an economically ineffective and irrational manner; but it is not as such acting in breach of competition law. There is no competition between the data holder and the aspiring innovator, so that the TFEU cannot be used as a stick to force a data holder to act. Denying innovation is likely to be harmful to the market value and perception of the service in the long run, but not necessarily unlawful under the TFEU.

The second important element for a data holder is to **assess its dominance** in the market, and its general market power; or in more practical terms the data holder should assess whether substitutes and alternatives to their data are reasonably available (meaning that a third party could generate or collect the data themselves, or obtain them from another source). If such substitutes or alternatives exist, there can again be no competition law issue. Refusal to share may be burdensome to the third party, but if the third party has reasonably accessible alternatives for the data, legal complaints based on competition law are unlikely to succeed.

A third element is **non-discrimination**. Both under the traditional criteria of the TFEU and under the proposed Data Act, the legal framework considers it unlawful to apply different conditions to equivalent data sharing transactions – i.e. granting a favoured position (lower price, more data, better

data) to some parties, thereby granting them a competitive advantage. To avoid this problem, it is advisable to formalize policies with respect to data sharing practices and procedures, in order to be able to demonstrate in case of complaints that there was no discriminatory treatment.

The Commission's proposal for the Data Act is currently under discussion in the European Parliament, and is awaiting a decision of the ITRE Committee (the Committee on Industry, Research and Energy). If it is adopted by the Committee, a consensus will still need to be reached between the Commission, Parliament and Council. Depending on any changes in its finalisation, it will also be necessary for data holders to correctly assess their own economic status, and the economic status of the data recipients. The Data Act consciously differentiates between **micro, small, medium and large** enterprises, and only imposes its full obligations on large enterprises. In instances where the Data Act will apply, the fairness criteria will need to be evaluated to ensure that fairness practices are not deemed unfair; and in case of doubts it is always recommended to engage in real and substantive negotiations with aspiring data users, since the Act would only apply to unilaterally imposed agreements.

Finally and perhaps most critically, a data holder should openly consider whether its practices are **conducive to fair competition and innovation**. In some situation, data sharing can be avoided entirely without legal recourse, e.g. when the data holder is a small enterprise, in a non-dominant position, and when requesting parties aim to build innovative services around the small data holder's data. Even in those situations however, it may be worth considering whether a positive, fair, reasonable, non-discriminatory and transparent data sharing policy may not simply be favourable to competition and innovation, and simply benefit the data holder as well by increasing the value of its data to the customers. After all, not every issue has to be resolved purely on the basis of legal arguments.

It is also worth recognising that the legal and policy landscape is still shifting. The Data Act is still in its proposal stage, and the principal Commission Notice on the definition of relevant markets is currently under revision. Changes in these texts could substantially influence the obligations of data holders, and the rights of aspiring data users. Therefore, it is recommended that data.europa.eu monitors changes and evolutions in these frameworks, maps out new case law, and identifies any new EU level policies or guidance documents that affect the application of European competition laws to the data economy.

6. Bibliography

- 2022 draft revised Horizontal Block Exemption Regulations and Horizontal Guidelines from the European Commission (with updated chapter on information exchange with a view to providing more guidance to companies on the competitive assessment of such an exchange); see https://competition-policy.ec.europa.eu/public-consultations/2022-hbers_en
- 2020 JRC Technical Report on Business-to-Business data sharing: An economic and legal analysis; see <https://ec.europa.eu/jrc/en/publication/eur-scientific-and-technical-research-reports/business-business-data-sharing-economic-and-legal-analysis>
- 2020 OECD Report on Consumer Data Rights and Competition; see [https://one.oecd.org/document/DAF/COMP\(2020\)1/en/pdf](https://one.oecd.org/document/DAF/COMP(2020)1/en/pdf)
- 2020 CERRE Report on data sharing for digital markets contestability - towards a governance framework; see https://cerre.eu/wp-content/uploads/2020/09/CERRE_Data-sharing-for-digital-markets-contestability-towards-a-governance-framework_September2020.pdf
- 2019 Data markets: where data protection meets competition and consumer protection – 30 years CiTiP conference notes, see <https://www.law.kuleuven.be/citip/blog/data-markets-where-data-protection-meets-competition-and-consumer-protection-30-years-citip-conference/>
- 2019 TILEC Discussion Paper - Limits and Enablers of Data Sharing An Analytical Framework for EU Competition; see https://www.researchgate.net/publication/337595029_Limits_and_Enablers_of_Data_Sharing_An_Analytical_Framework_for_EU_Competition_Data_Protection_and_Consumer_Law
- 2015, Open Data and Competition Law Some Issues Regarding Access and Pricing of Raw Data; see https://www.researchgate.net/publication/282590351_Open_Data_and_Competition_Law_Some_Issues_Regarding_Access_and_Pricing_of_Raw_Data
- Commission Notice on the definition of relevant market for the purposes of Community competition law [1997] OJ C 372/5; see <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A31997Y1209%2801%29>
- Commission Call for Evidence on EU competition law – updating the market definition notice (revision); see https://ec.europa.eu/competition-policy/public-consultations/2020-marketdefinition-notice_en
- Study on model contract terms and fairness control in data sharing and in cloud contracts and on data access rights; see <https://ec.europa.eu/newsroom/dae/redirection/document/87362>
- 2019 report on Competition Policy for the Digital Era, see <https://op.europa.eu/en/publication-detail/-/publication/21dc175c-7b76-11e9-9f05-01aa75ed71a1/language-en>
- Rethinking the essential facilities doctrine for the EU digital economy, Inge Graef; see <https://research.tilburguniversity.edu/en/publications/rethinking-the-essential-facilities-doctrine-for-the-eu-digital-e>

- HBER Regulations; see https://competition-policy.ec.europa.eu/antitrust/legislation/horizontal-block-exemptions_en, comprising:
 - Council Regulation No 2821/71 on application of Article 85 (3) [now 81 (3)] of the Treaty to categories of agreements, decisions and concerted practices
 - Commission Regulation No 1217/2010 of 14 December 2010 on the application of Article 101(3) of the Treaty on the functioning of the European Union to categories of research and development agreements
 - Commission Regulation No 1218/2010 of 14 December 2010 on the application of Article 101(3) of the Treaty to categories of specialisation agreements

