Data access and sharing in Germany and in the EU: Towards a coherent legal framework for the emerging data economy

A legal, economic and competition policy angle

- Final Report -
8 July 2022

Prof. Dr. Heike Schweitzer

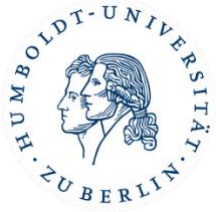
Prof. Dr. Axel Metzger

Prof. Dr. Knut Blind

Dr. Heiko Richter

Dr. Crispin Niebel

Frederik Gutmann



Overview

Executive Summary (English)

I. Introduction

The Bundesministerium für Wirtschaft und Klimaschutz (BMWK) has commissioned a study on the legal framework for access to data in the EU and in Germany from a legal, economic and policy angle. Data is at the heart of the ongoing digital transformation of the economy and society. In many different ways, access to data is becoming a precondition for innovating and for competing effectively. Against this background, both the European and the German legislator are striving to develop a legal framework for the data economy that facilitates voluntary agreements on data access and sharing and mandates data portability and/or data access where it is needed to protect – and sometimes to promote – competition. At the EU level, the most relevant initiatives include the Data Governance Act (DGA), the Draft Data Act (DA) and the Digital Markets Act (DMA). At the national level, §§ 19(2) No. 4, 20(1a) and 19a GWB are representative for an effort to enable market actors to compete effectively in data-driven markets.

The BMWK has asked the consortium consisting of lawyers and economists to determine whether the emerging legal framework is fit for the task of protecting and, where necessary, promoting competition, and to outline options for action in case of deficiencies. In order to answer this question, this study addresses the following issues:

- What limits do Article 101 TFEU/§ 1 GWB impose on voluntary agreements on data access and data sharing or other forms of data cooperation? Are undertakings provided with the legal guidance that is needed in order to enable innovative and potentially welfare-enhancing forms of data cooperation, and not to disincentivise it?
- When should data portability and/or data access be mandated in order to protect – or possibly promote – competition? How does the Draft Data Act contribute to the legal framework in this regard? Under which conditions does a refusal to ensure data portability and/or data access amount to an abuse of dominance (Art. 102 TFEU/§ 19 GWB), and when would it qualify as an abuse of relative market power (§ 20(1a) GWB)? Which obligations can be imposed on undertakings of paramount cross-market significance within the meaning of § 19a GWB in this regard? And which obligations are imposed on gatekeepers under the DMA? Is the legal framework appropriate, given the role of access to data for competition in the emerging data economy? Should possible deficiencies rather be corrected by way of changes to the general rules of competition law or by way of sector-specific data access regulation?
- Which role does access to data play in the realm of merger control?
- Are there general principles of ‘data governance’ to be applied where data access is mandated? What roles do data intermediaries play?
- Does a coherent legal framework for access to data and data sharing emerge from the plethora of different legislative initiatives at EU and national level – a legal framework that comes with the potential to support the transformation towards an innovative data economy?

II. The role of the state

In order to assess the adequacy of the emerging legal framework, the role of the European and national legislator must be considered. Generally, market failure analysis provides a good starting point for identifying where regulatory intervention may be needed. For example, the existence of data-related market power can justify the imposition of data-related remedies, including obligations to grant access to data.

The recent legislative initiatives at the EU level reach beyond addressing well-defined market failures, however: the EU is adopting a very pro-active stance. A justification for such an approach may be provided by the literature on failures in innovation systems. A clear and consistent legal infrastructure can enable or encourage market actors to exploit the opportunities that may come with the sharing of or access to data in data-driven markets. The goal of the various legal initiatives of the EU should then be to reduce uncertainty, increase transparency, support directionality and foster interactions among stakeholders. In addition to a clear and coherent legal framework, room for experimentation should be created. The lack of experience with data sharing and data access regimes suggests that different data access rules and regimes should be tested, e.g. in the context of sector-specific regulatory sandboxes. Apart from a very general 'infrastructural' legal framework for data, the creation of horizontal rules should be considered with a significant degree of caution.

III. Empirical analysis of data sharing

An analysis of the adequacy of the existing legal framework and a possible need for new rules on data access must start with an understanding of how markets currently function. In our study, we provide an overview of various recent surveys on data markets and data sharing in Europe and Germany, tentatively matching them with insights we gained from some selected interviews with relevant market actors. Our analysis of pre-existing surveys shows two things: firstly, there are only few companies, and mostly larger ones, that consider data sharing as relevant for their business model. Less than half of the companies express a need for external data. Whereas a small number of digital B2B platforms have experience with the purchasing or selling of data, most companies see no option to share data at all. Secondly, companies consider that the largest barriers to data sharing are of a legal nature, followed by organizational, technical or economic obstacles. When it comes to legal obstacles, compliance with the GDPR figures prominently – a point that was also stressed in the interviews.

Unsurprisingly, the interviews provided evidence of a broad range of perspectives regarding the introduction of data access/data sharing obligations. Generally, companies that collect data or already have access to data do not support mandated data sharing. With regard to B2B industrial data, respondents expressed concerns how data sharing obligations could possibly result in their clients not providing data in the first place. Other stakeholders see mandatory data access/data sharing as an opportunity.

IV. The current market order for data portability, data access and data sharing

Our inventory of the legal rules relating to data access and data sharing currently in place provides evidence of a great degree of legal uncertainty. Legal institutions, i.e. well-defined (intellectual) property rights, contract law principles and competition law principles, are only emerging.

1. Contract law

The traditional contract law principles do not provide for a general access right of the contracting parties to the data transmitted, created or observed, be it during the contractual relationship or after its termination. The existing information, access and return duties are case-specific and for the most part of a non-mandatory nature. They presuppose a contractual relationship between the parties and additional special circumstances of 'good faith' etc., which may sometimes be met when it comes to access to co-generated data. Neither EU law nor national German contract law foresee specific mandatory or default rules for contracts under which one of the parties grants access to data to the other party. Contract law is also lacking rules on how to handle data access rights mandated on non-contractual legal grounds, especially by competition law or regulatory law, which will then need to be implemented by way of a contractual regime.

2. Competition law

When concluding data sharing agreements, firms have to ensure compliance with Article 101 TFEU – regardless of whether they share data on a voluntary basis or based on a legal obligation. However, the discussion about the precise boundaries of data sharing agreements under Article 101 TFEU is still at an early stage. Substantial legal uncertainty remains even after the publication of the Commission's Draft Horizontal Guidelines in March 2022.

Data access obligations may be imposed under competition law pursuant to Article 102 TFEU/§§ 19(2) No. 4, 20(1a) GWB if the refusal to share data qualifies as an abuse of dominance or 'relative market power'. Companies may request access to infinite types of data in a myriad of market settings which cannot be predicted or categorized ex ante. In this study, we focus on access to machine usage or behavioural data, and we look at three specific data access scenarios in particular, which may be considered relevant in the emerging data economy where data becomes an input for providing complementary services or for innovating:

(1) market participants who have had part in the generation of relevant data may request access to that data and the possibility to use them, or to let third parties make use of them ('data access by data co-generators' or 'data portability'– scenario 1);
(2) third parties who offer complementary services within the framework of a data-driven value creation network or digital ecosystem may request access to large sets of bundled individual level or aggregate data to develop and improve their complementary services (scenario 2);

(3) third parties may request access to holders of large, unique datasets that are needed to develop and train artificial intelligence (AI – scenario 3).

In 'scenario 1', competition law may be an appropriate instrument to address data-related customer lock-in in the absence of other rights to data portability or data access such as Article 20 GDPR, Article 6 No. 9 and 10 DMA or Articles 4 and 5 of the Draft Data Act. In the context of digital ecosystems, the 'aftermarket doctrine' may be revived and adapted to the role and specifics of data in data-driven ecosystems. Where data access is of systemic relevance, sector-specific regulation will typically be preferable, however. Under scenario 2, competition law may come into play if a dominant undertaking or a company with relative market power refuses access to aggregated data that is necessary to compete in an aftermarket or a complementary market. Scenario 3 is difficult to address under competition law, since it is not based on foreclosure concerns but implies a special responsibility to promote innovation.

So far, much of the debate in competition law has focused on scenario 2-cases. In those cases, most authors have considered the 'Essential Facilities Doctrine' (EFD) to be the relevant test. Given the difficulties in applying the criteria of the EFD to data access, there is a broad discussion about the need to redefine or reinterpret the EFD conditions and thresholds in light of the particularities of the data economy. Interestingly, there is little case law on abusive denial of access to data, however. The new GWB provisions, in particular §§ 19(2) no. 4, 20(1a) GWB, are currently being tested in the Bundeskartellamt's proceedings against Deutsche Bahn.

3. DMA/§ 19a GWB

The DMA primarily addresses data access in scenario 1-settings: while Article 6 No. 9 DMA establishes a right to data portability for end users to data provided or generated through their activity in the context of the relevant platform service, Article 6 No. 10 DMA constitutes a comparable right to data access for business users to data provided or generated by them or their end users. The same is true for § 19a GWB: according to § 19a(2), 1st sentence, No. 5, the Bundeskartellamt may impose data portability obligations upon norm addressees if the refusal to grant data interoperability would hamper competition.

Within the emerging framework of 'gatekeeper regulations', only one DMA obligation reaches beyond data portability: Article 6 No. 11 DMA obliges online search engine providers with gatekeeper status to provide access to their ranking, query, click and view data to third party competitors in the online search engines market, and thereby strives to make the search engine gatekeeper position contestable.

4. Merger control

Competition authorities around the globe increasingly deal with data-driven mergers. So far, the European Commission has not yet blocked a merger on the grounds that accessing or combining data would give rise to competition concerns. But in recent merger decisions (most notably Google/Fitbit and Meta/Kustomer), the European Commission accepted a bundle of

commitments to remedy competition concerns that include data access, data separation and interoperability mandates – and hence commitments of a behavioural nature. Data-related mergers before the Bundeskartellamt have been rare so far.

The Meta/Kustomer acquisition has recently spurred the debate on the appropriateness of the current merger review regime in Germany and the EU. Some reforms have already taken place: on the EU-level, the Commission's guidance on referrals pursuant to Article 22 EUMR of March 2021 and the new information duty on mergers of gatekeepers under Article 14 DMA are the most recent changes in practice and legislation. The German legislature has made some legislative amendments and clarifications regarding digital markets and the role of data. The last amendments to the GWB have added a notification duty if the transaction value exceeds EUR 400 Mio. and explicitly spelled out that the undertaking's access to data relevant for competition is to be taken into account when assessing the market position of an undertaking.

V. Policy options and discussion

On the basis of this stocktaking exercise, the study discusses the need for reform and explores policy options.

1. The Draft Data Act

The Draft Data Act proposes to create new legal rights of access to the data generated by the use of products – both for the product users and, derivatively, for third parties acting on their behalf. These rights of access – which in our categorisation belong to the data access scenario 1 (data portability) – shall exist irrespective of a position of market dominance of the data holder or a position of dependence of the product user. The Draft Data Act thereby goes beyond addressing well-defined market failures. Rather, it strives to establish a general legal infrastructure in order to facilitate the transformation towards a data economy. While such a pro-active stance of the legislator is legitimate, we should keep in mind how little we know about the precise needs of the market actors and the frictions that will likely arise in future data markets. A novel legal framework should therefore remain flexible and leave room for market adaptations.

While we support the Draft Data Act's fundamental decisions regarding the allocation of rights in product usage data, the draft contains a number of incoherencies, and some of its provisions should be rethought.

Recalibration of the rights of the data holder and the product user/allowing for a waiver of access rights absent an imbalance of power:
The legal positions of the data holder and the product user under the Draft Data Act should be recalibrated. The basic approach, which is to not touch the data holder's ability to technically exclude others from using machine-generated data, but to introduce access rights for product users and third parties, deserves support. However, the Draft Data Act should strive for a more balanced approach with regard to the different rights to use data. Both the data holder and the

product user should be provided an independent right to use the data without the approval of the other party. Article 4(6) should be revised. In light of the goals of the Draft Data Act, the mandatory nature of the product user's access right in Article 4(1) should be reconsidered. An alternative approach would be to allow a waiver as long as the product user retains the right to revoke this waiver after some time.

Third parties may benefit from the new access rights regime by receiving data either from product users or directly from the data holders at the request of the user, Article 5(1). Articles 6(1) and 6(2) set out a number of obligations to be respected by the third party. In light of the diversity of actors, *inter alia,* with regard to size, and the different access scenarios at stake, the legislature should reconsider the mandatory nature of the requirements in Articles 6(1) and 6(2), at least for scenarios in which the product user is not a consumer or SME.

Reconsideration of the non-compete clause:
The non-compete clauses in Articles 4(4) and Article 6(2) lit. e of the Draft Data Act are overbroad and should be reconsidered.

Specification of conditions of access:
According to Article 8 Draft Data Act, a data holder, where obliged to make data available to a data recipient under Article 5 or "under other Union law or national legislation implementing Union law", shall do so on FRAND terms and in a transparent manner. Given the fact that the data holder is the only entity that can grant access to the specific user data in question, it seems necessary to protect the third party from unfair or discriminatory access conditions. However, the provision raises a number of questions which can only partly be answered by reference to the experience with other FRAND scenarios.

Also, the Draft Data Act does not specify how data access rights will be implemented technically. The legislature should reconsider whether the technical requirements of Article 28, which address data spaces, should be generalised for making them suitable also for data access requests under Articles 4 or 5, or whether a similar but independent provision should be introduced in Chapter III for that purpose. Such a provision on the technical side of access requests should include the technical requirements which are essential to facilitate access to and the further use of the data.

Exclusion of 'sui generis' database rights:
The general approach taken by the Draft Data Act with regard to 'sui generis' database rights and trade secrets deserves support, but the wording of Article 35 should be revised, and Article 8(6) should be deleted.

Clarify anonymisation requirements under the GDPR:
The Draft Data Act does not provide a legal basis for the processing of personal data. Consequently, the GDPR may hamper the provision of data access where personal data is at issue. A possible solution could be to clarify the requirements of anonymisation of datasets and to oblige data holders, users and third parties to use all available and economically reasonable

means to anonymise datasets before they are shared, especially if consent cannot be obtained from the data subjects.

Private enforcement:
The Draft Data Act does neither provide nor exclude private enforcement actions before national courts. It should be clarified that private enforcement by the product user and third parties is permitted.

An experimental approach:
The Data Act will serve as a testing ground for a new allocation of data access rights in the data economy. Its effects on the markets should therefore be closely monitored and evaluated after a relatively short period of time in order to assess whether this approach should be refined or expanded.

2. Competition law

Creating legal certainty regarding compliance with Article 101 TFEU for firms wishing to enter into data sharing or access agreements is a difficult endeavour. Given the dearth of pertinent case law, an established body of tested principles is still missing. Grey zones remain. This, as well as the heterogeneity of potential data sharing agreements, suggests that a comprehensive 'Data-Block Exemption Regulation (BER)' is not a realistic option as of now. However, in order to create room for experimenting with different forms of data cooperation, a shift from an 'adversarial' to a more 'cooperative' (or 'participatory') approach to antitrust enforcement is called for in this field. The newly introduced right to obtain a non-infringement decision from the Bundeskartellamt in the absence of meaningful precedents (§ 32c(4) GWB) is a starting point. At the European level, the reform of the Commission's 'Notice on informal guidance' and the upcoming review of Reg. 1/2003 offer opportunities to create comparable mechanisms.

Regarding obligations of dominant undertakings to grant access to data under Article 102 TFEU/§§ 19, 20 GWB or under § 20(1a) GWB, the small number of cases and lack of complaints is notable. In light of the insights from our empirical overview, the absence of relevant competition law action may not be driven by the inherent restrictions of the competition law doctrine. The data economy is still at an early stage. Frequently, requests for data access by innovators and complementors would presuppose a good understanding of what types of data are available, as well as the availability of sufficient resources and skills to work with potentially large amounts of data. In many cases, this may be lacking. At this point of market development, it seems plausible, therefore, to focus primarily on making data portability function effectively, i.e. to enable those who participated in the generation of data to access, port and make use of the data. With regard to data portability, a legal framework is about to emerge outside the field of competition law, however, which comprises the Draft Data Act (with regard to data generated by the use of products), the DMA (with regard to data generated by the use of core platform services offered by gatekeepers), § 19a(2), 1st sentence, No. 5 GWB (with regard to data controlled by designated norm addressees under § 19a(1) GWB) and sector-specific legislation for those areas where data portability is particularly important for

competition to emerge in complementary markets. Under German competition law, § 20(1a) GWB may close gaps.

While competition law action currently does not seem to focus on data access in scenario 2-settings, it does make sense to revisit competition law doctrine in this regard. We suggest that, generally speaking, the EFD provides a sound test for establishing when a dominant undertaking's refusal to grant access to data constitutes an abuse. Where access to the relevant data is determinative for the possibility to effectively compete within a data-driven ecosystem, a different test may be appropriate, however. In that case, the indispensability criterion, which is rightly construed narrowly under the EFD, should be replaced by a broader balancing of interest specific to the role of data for competition in data-driven ecosystems or value creation network. In these settings, refusals to grant access to data may be considered abusive where they constitute a change from a prior policy of open access once the ecosystem has become dominant. Even without such a change, more far-reaching obligations to grant access to data in scenario 2-settings may be imposed on ecosystem orchestrators who have become gatekeepers (Art. 3 DMA) or undertakings of paramount cross-market importance (§ 19a(1) GWB). Where a data holder continues to be subject to competition on the primary 'ecosystem market', access to data obligations may be more confined.

Next to data-sharing in digital ecosystems, it may be appropriate to develop a specific test for data sharing in data-driven markets – both within the framework of § 19 GWB and within the framework of § 20(1a) GWB. Simultaneously, it seems preferable to gain experience with data sharing in these settings based on competition law and/or sector-specific regulation instead of establishing a full-fledged horizontal regulatory regime for data sharing in data-driven markets as suggested by some.

In all these cases, the interest balancing must take due account of the difference between 'provided', 'observed' and 'derived' data. We suggest that the interest balancing test we propose can be implemented within the existing competition law framework. No changes of general competition law are currently needed. Where access to data becomes particularly important for innovation and competition in a given sector, sector-specific legislation may be called for in order to specify the data access obligation and set up an appropriate data governance regime.

3. DMA/§ 19a GWB

The effectiveness of the data portability obligations under Article 6(9) and Article 6 No. 10 DMA will largely depend on their implementation. The provisions require gatekeepers to integrate data portability in the design of the platform service itself ('compliance by design'). However, none of these norms specifies the format in which and the interface through which data portability or data access are to be provided. Fundamental decisions about the specifications and conditions of data portability and access cannot be left to the gatekeepers alone, nor should they be set by the European Commission alone. Rather, the Commission should make sure that they are developed in an open process involving all relevant stakeholders,

and with the goals of the DMA in mind. If the DMA's data portability obligations are implemented effectively, they may help to promote more open and innovative complementary markets (Article 6 No. 9 DMA), and they may help business users to make better use of the data their business generates (Article 6 No. 10 DMA). The contribution of these provisions to make the gatekeepers' core position contestable will likely be modest, however. End users (Article 6 No. 9 DMA) and business users (Article 6 No. 10 DMA) will have access only to those data generated based on their own activity. The gatekeeper, on the other hand, will have access to the whole of the data trove. Given the economies of scale and scope in data analytics, this may continue to constitute a huge competitive advantage. Article 6 No. 11 DMA imposes a significantly more far-reaching data sharing obligation. Its purpose is to make the search engine provider's position contestable – not to promote data-driven competition on complementary markets. Arguably, only the largest competitors in the search engine market will benefit.

While § 19a(2), 1st sentence, No. 5 GWB enables the Bundeskartellamt to impose data interoperability obligations on designated norm addressees where competition would otherwise be hampered, it lags behind the DMA in that the Bundeskartellamt thereby reacts to specific competition concerns in a given context and in a differentiated manner, whereas the DMA aims to establish a coherent, overarching data portability infrastructure for all gatekeepers. The added value of § 19(2) GWB may lie in the imposition of targeted interoperability requirements with regard to non-core platform services. Like in the DMA, no provision is made in § 19a(2) GWB for the imposition of data access obligations in scenario 2-settings. Depending on the experience with § 19a GWB, an amendment of the provision in this regard may be called for.

4. Merger control

Merger review regarding data-driven business models is the subject of ongoing reform debates. These debates are part of the larger discourse on mergers in digital markets, including so-called 'killer acquisitions'. The current EU approach to rely on national referrals to the Commission under Article 22 EUMR appears questionable and insufficient. Also, the future effect of Article 14 DMA should not be overestimated. A lowering of the § 35(1a) No. 3 GWB notification threshold in Germany – from EUR 400 Mio. down to e.g. EUR 200 Mio. – could at least enlarge the number of cases that would fall under German merger review and that could therefore potentially be referred to the EU-Commission. We recommend that this option should be discussed by the legislature.

More fundamentally, the legislature should consider updating and strengthening current merger review laws and enforcement with special regard to data-driven markets and digital ecosystems. Such regulatory recalibration would need further, more targeted analysis and consultation. In particular, the German legislature should accommodate the particular effects of data-related mergers to competition, i.e. by modifying substantive rules of merger review with regard to undertakings of paramount significance for com-petition across markets according to § 19a(1) GWB. In particular, this means that merger review would consider the effects the merger would have on the whole 'eco-system' to avoid an overly segmented view on defined markets.

Such reforms should also be considered at the EU level. The current practice of the EU Commission to accept commitments on data access, data separation and interoperability in the course of merger proceedings should be revisited. Such behavioural commitments should not be accepted in data-related mergers that involve big tech players. Future reforms on the EU level should consider introducing an explicit provision that would allow only for structural remedies in such cases. In any case, the German government should advocate a reform of merger control at EU level, which would address the substantial criteria for review in digital ecosystem cases, the relationship with national rules and notification thresholds, and which would also require an update of the EU Merger Guidelines, with particular attention to conditions and effects of competition in data-driven markets.

5. Data intermediaries

Data intermediaries are entities which enable, control or facilitate data access and sharing between data holders and data users. They considerably impact the competitiveness and innovativeness of data-related markets, because they can fulfil several desirable functions in data-driven markets. In reality, several models of data intermediaries exist, but they are in a rather nascent phase.

The recently adopted EU Data Governance Act (DGA) provides a comprehensive legal framework for 'data intermediation services' (DIS), which are a subset of all data intermediaries. The DGA installs a mandatory compliance regime, which requires DIS to officially register their services as a precondition for lawfully providing them in the EU and obliges them to comply with various requirements. The DGA aims to foster their development and the creation of respective markets. This goal is indeed desirable. Yet, it remains an open question whether the DGA proves to be an effective regulatory means. So far, no actual effects can be observed, not the least because rules on DIS enter into effect only in September 2025. In the current phase, industry players are (re-)assessing their business strategies and models. At the time being, the DGA poses high legal uncertainty as for its scope (e.g. to what extent GAIA-X based intermediation models are covered) and requirements/obligations, which need further interpretation and application by authorities and courts. This adds to the generally high unpredictability of the regulatory effects of the DGA.

In general, the legal framework should facilitate the development of data intermediaries. Such coherent integration of data intermediaries in the legal orders of the EU and the Member States touches on several legal regimes and interfaces: Data protection rules should be designed to effectively integrate data intermediaries in the market order for data sharing. The integration of data intermediaries with contract law and FRAND principles can be improved, e.g. the EU legislature could consider extending Article 8(1) Data Act also to DIS under Article 12(f) DGA. The Data Act lacks consideration of data intermediaries and should clarify to what extent data can be shared with third parties via data intermediaries. In the context of competition law, data intermediaries can contribute to a more efficient data value creation by enabling and fostering data sharing as well as preventing sharing to ensure compliance with competition law. In merger

review, data intermediaries should be considered as a tool to strengthen the structural effect of commitments, which seek to prevent data from being merged or used for purposes that would increase data power and concentration. As for data intermediaries as enforcers of and subjects addressed by Article 101 TFEU, the EU and national legislature should consider that official guidance may provide legal certainty for evolving business models. Sector-specific legislation may introduce stricter rules for data intermediaries, but significant evidence of market failure or public policy grounds are needed that would justify such cutting market intervention.

Executive Summary (German)

I. Einleitung

Das Bundesministerium für Wirtschaft und Klimaschutz (BMWK) hat eine Studie zum rechtlichen Rahmen des Datenzugangs in der EU und in Deutschland in Auftrag gegeben. Die neuen Bedingungen der Datenverfügbarkeit und die neuen Möglichkeiten der Datenverarbeitung sind ein wesentlicher Bestandteil der digitalen Transformation von Wirtschaft und Gesellschaft. Innovations- und Wettbewerbsfähigkeit von Unternehmen sind zunehmend mit dem Versuch verbunden, datengetrieben Wertschöpfung zu generieren. Vor diesem Hintergrund haben sich sowohl der europäische als auch der deutsche Gesetzgeber die Entwicklung eines Rechtsrahmens für die Datenwirtschaft zum Ziel gesetzt, der Vereinbarungen über den Zugang und Austausch von Daten erleichtert und gesetzliche Datenzugangsrechte schafft, wenn dies zum Schutz des Wettbewerbs erforderlich ist. Hinzu tritt das Ziel einer proaktiven Förderung von Wettbewerb und Innovation. Zu den wichtigsten Initiativen auf europäischer Ebene gehören der Data Governance Act (DGA), der Digital Markets Act (DMA) und der Entwurf eines Data Act (DA). Auf nationaler Ebene stehen §§ 19 Abs. 2 Nr. 4, 20 Abs. 1a und 19a GWB stellvertretend für das Bemühen, einen effektiven Wettbewerb zugunsten aller Marktteilnehmer auf datengetriebenen Märkten zu ermöglichen.

Das BMWK hat die Autoren der Studie – ein interdisziplinäres Team, bestehend aus Juristen und Ökonomen – gebeten, zu untersuchen, ob der sich abzeichnende Rechtsrahmen zur Erreichung dieser Ziele geeignet ist, und im Fall von Defiziten Handlungsoptionen aufzuzeigen. Konkret befasst sich die Studie mit den folgenden Fragen:

- Welche Grenzen setzt Artikel 101 AEUV/§ 1 GWB freiwilligen Vereinbarungen über Datenzugang und Datenaustausch? Verfügen Unternehmen über das Maß an Rechtssicherheit, das notwendig ist, um innovative und potenziell wohlfahrtssteigernde Formen der Datenzusammenarbeit zu ermöglichen bzw. zu erleichtern?
- Unter welchen Bedingungen gebietet das Ziel des Wettbewerbsschutzes – und ggfs. der Förderung des Wettbewerbs – die Anordnung von Datenportabilität oder Datenzugang? Welchen Beitrag leistet der Entwurf eines Datengesetzes (im Folgenden: Data Act-Entwurf) in dieser Hinsicht? Unter welchen Voraussetzungen stellt die Verweigerung der Datenportabilität bzw. des Datenzugangs einen Missbrauch einer marktbeherrschenden Stellung dar (Artikel 102 AEUV/§ 19 GWB), und wann liegt ein Missbrauch relativer Marktmacht vor (§ 20 Abs. 1a GWB)? Welche Verpflichtungen können Unternehmen mit überragender marktübergreifender Bedeutung für den Wettbewerb im Sinne des § 19a GWB in diesem Zusammenhang auferlegt werden? Und welche Pflichten treffen die Gatekeeper nach dem DMA? Wird der gegenwärtige rechtliche Rahmen der Bedeutung des Datenzugangs für den Wettbewerb in der entstehenden Datenökonomie gerecht? Sollten etwaige Defizite eher durch eine Änderung der allgemeinen wettbewerbsrechtlichen Vorschriften oder durch eine sektorspezifische Datenzugangsregulierung behoben werden?
- Welche Rolle spielt der Zugang zu Daten im Bereich der Fusionskontrolle?
- Gibt es allgemeine Grundsätze der „Daten-Governance“, die anzuwenden sind, wenn der Datenzugang gesetzlich angeordnet wird? Welche Rolle spielen Datenintermediäre?

- Ergibt sich aus der Fülle unterschiedlicher Gesetzesinitiativen auf EU- und nationaler Ebene ein kohärenter Rechtsrahmen für den Zugang zu und den Austausch von Daten – ein Rechtsrahmen, der das Potenzial hat, den Wandel zu einer innovativen Datenwirtschaft zu unterstützen?

II. Die Rolle des Staates

Will man den in der Entstehung befindlichen Rechtsrahmen für Datenzugang einordnen, so ist zunächst nach der Rolle des europäischen und des nationalen Gesetzgebers in der Datenökonomie zu fragen. Grundsätzlich bildet die Theorie des Marktversagens einen guten Ausgangspunkt, um die Notwendigkeit regulatorischer Eingriffe zu bestimmen. So ist beispielsweise das Vorhandensein von datenbezogener Marktmacht ein wichtiger Grund, um Datenzugangsverpflichtungen aufzuerlegen.

Die jüngsten Gesetzgebungsinitiativen auf EU-Ebene zielen jedoch über die Behebung von klar definiertem Marktversagen hinaus: Die EU agiert vielmehr proaktiv. Eine Rechtfertigung für einen solchen Ansatz findet sich in der Literatur über Innovationssystemversagen. Eine klare und kohärente rechtliche Infrastruktur kann die Marktakteure in die Lage versetzen oder dazu ermutigen, die Chancen zu nutzen, die sich aus dem Datenaustausch oder -zugang in zunehmend datengesteuerte Märkte ergeben. Ziel der verschiedenen Rechtsinitiativen der EU kann es aus dieser Perspektive sein, Unsicherheit zu verringern, Transparenz zu erhöhen, Orientierung zu geben und die Interaktion zwischen den Akteuren zu fördern. Erforderlich ist hierfür ein klarer und kohärenter Rechtsrahmen. Darüber hinaus sollte Raum für Experimente geschaffen werden. Da die Datenwirtschaft noch in den Kinderschuhen steckt und es noch wenige Erfahrungen mit Datenaustausch und Datenzugangsregelungen gibt, ist zu empfehlen, verschiedene Datenzugangsregeln und -regelungen zu erproben, z. B. im Rahmen sektorspezifischer Reallabore. Jenseits eines allgemeinen „infrastrukturellen“ Rechtsrahmens für Daten ist hinsichtlich der Schaffung horizontaler (d.h. nicht sektorspezifischer) Regelungen hingegen gegenwärtig Vorsicht geboten.

III. Empirische Analyse

Eine Bewertung des bestehenden Rechtsrahmens und die Ermittlung eines möglichen Bedarfs an neuen Datenzugangsregeln setzt ein Verständnis der Funktionsweise datengetriebener Märkte voraus. In unserer Studie geben wir einen Überblick über verschiedene neuere Erhebungen zu Datenmärkten und zum Datenaustausch in Europa und Deutschland und gleichen sie mit Erkenntnissen ab, die wir aus einigen Interviews mit ausgewählten relevanten Marktakteuren gewonnen haben. Bei der Literaturanalyse fallen zwei Beobachtungen auf. Erstens gibt es nur wenige und meist größere Unternehmen, die die gemeinsame Nutzung von Daten als relevant für ihr Geschäftsmodell betrachten. Weniger als die Hälfte der Unternehmen äußert einen Bedarf an externen Daten, die meist für ihre Produkte und weniger für ihre Prozesse benötigt werden. Während digitale B2B-Plattformen Erfahrung mit dem Kauf oder Verkauf von Daten haben, sehen die meisten Unternehmen keine Möglichkeit, Daten überhaupt zu teilen. Zweitens führen Marktakteure rechtliche Regeln – vor allem den Datenschutz und Regeln zum Schutz der Privatsphäre sowie Haftungsrisiken – als die größten Hindernisse für

die gemeinsame Nutzung von Daten an. Es folgen organisatorische, technische und wirtschaftliche Hindernisse.

Die Interviews zeigen wenig überraschend ein breites Meinungsspektrum der Unternehmen über die Einführung von Datenzugangs-/Datenteilungsverpflichtungen: Unternehmen, die Daten sammeln oder bereits Zugang zu Daten haben, lehnen solche Pflichten regelmäßig ab. In Bezug auf B2B-Industriedaten äußerten die Befragten Bedenken, dass eine Verpflichtung zum Datenaustausch dazu führen könnte, dass ihre Kunden Daten gar nicht erst zur Verfügung stellten. Andere Interessengruppen sehen den obligatorischen Datenzugang bzw. Datenteilungspflichten als Chance.

IV. Die bestehende Marktordnung für Datenportabilität, -zugang und -austausch

Eine Bestandsaufnahme geltender Rechtsvorschriften über den Datenzugang und -austausch zeigt, dass gegenwärtig ein hohes Maß an Rechtsunsicherheit besteht. Klar definierte Exklusivrechte, vertragsrechtliche und wettbewerbsrechtliche Prinzipien, sind erst im Entstehen begriffen.

1. Vertragsrecht

Das deutsche und europäische Vertragsrecht kennt keinen allgemeinen Anspruch der Vertragsparteien auf Zugang zu Daten, die die jeweils andere Partei während eines Vertragsverhältnisses erhebt und verarbeitet. Aus Treu und Glauben können Informationsrechte folgen. Dies hängt aber von den Umständen des Einzelfalls ab. Ein allgemeiner Anspruch auf Zugang zu „ko-generierten Daten“ lässt sich hieraus nicht ableiten. Zugleich gibt es bislang keine gesetzlichen Regeln für Verträge, in denen sich Parteien auf einen Zugang zu Daten einigen. Entsprechende Regeln fehlen auch für Situationen, in denen der Zugang zu Daten wettbewerbsrechtlich oder durch sektorspezifische Regulierung angeordnet wird, zugleich aber einer vertraglichen Durchführung bedarf.

2. Wettbewerbsrecht

Vereinbarungen zwischen Unternehmen über den Austausch von Daten sind durch Artikel 101 AEUV/§ 1 GWB Grenzen gezogen – unabhängig davon, ob Daten auf freiwilliger Basis oder aufgrund einer rechtlichen Verpflichtung ausgetauscht werden. Auch nach der Veröffentlichung des Entwurfs der Horizontalleitlinien der Europäischen Kommission im März 2022 besteht weiterhin erhebliche Rechtsunsicherheit darüber, wo genau diese Grenzen verlaufen.

Artikel 102 AEUV/§§ 19 Abs. 2 Nr. 4, 20 Abs. 1a GWB begründen Datenzugangsverpflichtungen, wenn die Verweigerung der Zugangsgewährung als Missbrauch einer marktbeherrschenden Stellung oder als Missbrauch „relativer Marktmacht“ zu qualifizieren ist. Die Zahl denkbarer Datenzugangskonstellationen ist vielfältig und lässt sich abschließend weder vorhersagen noch kategorisieren. In dieser Studie konzentrieren wir uns

insbesondere auf den Zugang zu Maschinennutzungs- oder Verhaltensdaten. Drei Datenzugangsszenarien stehen im Mittelpunkt:

(1) Marktteilnehmer, die durch ihr Nutzungsverhalten an der Generierung relevanter Daten beteiligt waren, begehren Zugang zu diesen Daten und das Recht, sie für eigene Zwecke zu nutzen oder Dritten zur Verfügung zu stellen („Datenportabilität" – Szenario 1).
(2) Dritte begehren Zugang zu großen Mengen gebündelter individueller Daten oder zu aggregierten Daten, um im Rahmen eines datenbasierten Wertschöpfungsnetzes oder digitalen Ökosystems komplementäre Dienste entwickeln und anbieten zu können (Szenario 2).
(3) Dritte begehren Zugang zu großen Datensätzen, etwa um KI-Anwendungen zu entwickeln (Szenario 3).

In Szenario 1 kann das Wettbewerbsrecht ein geeignetes Instrument sein, um dateninduzierten Lock-in-Effekten entgegenzuwirken, wenn diese einen Marktverschluss zu bewirken drohen. Voraussetzung ist, dass der Gefahr eines Marktverschlusses nicht bereits durch andere Datenportabilitäts- bzw. Datenzugangsrechte – etwa aus Artikel 20 DSGVO, Artikel 6 Nr. 9 und 10 DMA oder Artikel 4 und 5 DA – effektiv entgegenwirkt wird. Wettbewerbsrechtlich begründete Datenportabilitäts- bzw. Datenzugangsansprüche können etwa aus der Anwendung einer auf die Besonderheiten von Daten und digitalen Ökosystemen angepassten „Aftermarket"-Doktrin folgen. Wo Datenportabilität bzw. Datenzugang systemische Bedeutung für die Funktionsweise eines Wertschöpfungsnetzes erlangen, ist allerdings häufig eine sektorspezifische Ausformung der Datenportabilitäts- bzw. Zugangsrechte vorzugswürdig.

Im Kontext von Szenario 2 kann das Wettbewerbsrecht zum Tragen kommen, wenn ein marktbeherrschendes Unternehmen oder ein Unternehmen mit relativer Marktmacht den Zugang zu aggregierten Daten verweigert, die für den Wettbewerb auf einem nachgelagerten oder komplementären Markt erforderlich sind. Szenario 3-Konstellationen sind mit Hilfe des Wettbewerbsrechts hingegen schwer zu erfassen: In diesen Fällen gilt es nicht, eine potenzielle Marktabschottung durch den Marktbeherrscher zu unterbinden. Vielmehr würde marktbeherrschenden Unternehmen hier eine besondere Verantwortung für die Förderung dezentraler Innovation auferlegt. Dies mag in bestimmten Fällen legitim sein, überschreitet allerdings die Regelungsziele des Wettbewerbsrechts.

Die wettbewerbsrechtliche Diskussion hat sich bislang häufig auf Szenario 2-Konstellationen konzentriert. Viele halten hier die „Essential Facilities"-Doktrin (EFD) für den einschlägigen Analyserahmen. In Anbetracht der Schwierigkeiten bei der Anwendung der EFD-Kriterien auf den Zugang zu Daten wird diskutiert, ob diese Kriterien im Lichte der Besonderheiten der Datenwirtschaft angepasst werden müssen. Bislang gibt es allerdings kaum Rechtsprechung oder behördliche Fallpraxis zur missbräuchlichen Verweigerung des Zugangs zu Daten.

3. DMA/§ 19a GWB

Der DMA adressiert in erster Linie den Datenzugang in Szenario 1-Konstellationen: Während Artikel 6 Nr. 9 DMA ein Recht auf Datenportabilität für Endnutzer mit Hinblick auf Daten begründet, die durch ihre Tätigkeit im Rahmen des jeweiligen zentralen Plattformdienstes

bereitgestellt oder erzeugt werden, führt Artikel 6 Nr. 10 DMA ein vergleichbares Zugangsrecht für gewerbliche Nutzer zu Daten ein, die von ihnen oder ihren Endnutzern bereitgestellt oder erzeugt werden. Auch § 19a GWB betrifft ausschließlich Datenportabilitätsszenarien: Nach § 19a Abs. 2 S. 1 Nr. 5 GWB kann das Bundeskartellamt den Normadressaten Datenportabilitätspflichten auferlegen, wenn die Verweigerung der Datenportabilität den Wettbewerb behindern würde.

Im Rahmen der sich abzeichnenden „Gatekeeper-Regulierungen" geht nur der DMA – und dieser nur in einer der dort aufgezählten Verhaltenspflichten – über eine Datenportabilitätspflicht hinaus: Artikel 6 Nr. 11 DMA verpflichtet Anbieter von Online-Suchmaschinen mit Gatekeeper-Status, dritten Unternehmen, die selbst Online-Suchmaschinen betreiben, Zugang zu ihren Ranking-, Such-, Klick- und Anzeigedaten zu gewähren, und strebt damit an, die Bestreitbarkeit der Gatekeeper-Position von Suchmaschinenbetreibern zu erhöhen.

4. Fusionskontrolle

Weltweit befassen sich die Wettbewerbsbehörden zunehmend mit datengetriebenen Fusionen. Die Europäische Kommission hat bisher noch keinen Zusammenschluss mit der Begründung untersagt, dass der Zugang zu Daten oder deren Kombination wettbewerbsrechtliche Bedenken aufwirft. In den jüngsten Zusammenschlussentscheidungen (vor allem Google/Fitbit und Meta/Kustomer) hat die Europäische Kommission ein Bündel an Verpflichtungszusagen akzeptiert, um Wettbewerbsbedenken auszuräumen. Diese Verpflichtungszusagen sind ihrer Art nach verhaltensorientiert, da sie den Datenzugang, die Datentrennung und die Interoperabilität vorschreiben. Jedoch war das Bundeskartellamt bislang selten mit datengetriebenen Zusammenschlüssen befasst.

Die Übernahme von Meta/Kustomer hat in jüngster Zeit die Debatte beflügelt, ob es einer Reform der geltenden Fusionskontrollregeln in Deutschland und der EU bedarf. Einige Reformen sind bereits erfolgt: Auf EU-Ebene sind der Leitfaden der Europäischen Kommission zur Anwendung des Verweisungssystems nach Artikel 22 FKVO vom März 2021 und die neue Anzeigepflicht über Fusionen von Gatekeepern gemäß Artikel 14 DMA zu nennen. Der deutsche Gesetzgeber hat im Rahmen der 9. und 10. GWB-Novelle einige Änderungen vorgenommen, die unter anderem die Feststellung von Marktmacht auf digitalen Märkten betreffen. Außerdem wurde eine Meldepflicht ab einem Transaktionswert von 400 Mio. EUR eingeführt, und es wurde ausdrücklich klargestellt, dass der Zugang des Unternehmens zu wettbewerbsrelevanten Daten bei der Beurteilung der Marktstellung eines Unternehmens zu berücksichtigen ist.

V. Reformbedarf und Handlungsoptionen

Auf der Grundlage dieser Bestandsaufnahme eruiert die Studie potenziellen Reformbedarf und erörtert Handlungsoptionen.

1. Data Act-Entwurf

Mit dem Entwurf des Data Act („Datengesetz“) sollen neue gesetzliche Zugangsrechte zu den bei der Nutzung von Produkten generierten Daten geschaffen werden. Sowohl den Produktnutzern als auch den von ihnen autorisierten Dritten soll ein Recht auf Datenzugang zustehen. Diese Zugangsrechte – die nach unserer Systematik dem Datenzugangsszenario 1 (Datenportabilität) zuzuordnen sind – sollen unabhängig von einer marktbeherrschenden Stellung des Dateninhabers oder einer abhängigen Stellung des Produktnutzers bestehen. Der Data Act-Entwurf strebt damit die Schaffung einer rechtlichen Infrastruktur an, die nicht ein klar definiertes Marktversagens adressiert, sondern den Übergang zu einer Datenwirtschaft erleichtern soll. Ein solches Regelungsanliegen ist legitim. Der Gesetzgeber sollte allerdings bedenken, wie wenig wir gegenwärtig über die genauen Bedürfnisse der Marktteilnehmer und die zu erwartenden Friktionen in Datenmärkten wissen. Ein neuer Rechtsrahmen sollte daher in hohem Maße flexibel sein und Raum für Anpassungen an Marktgegebenheiten belassen.

Während wir die grundlegenden Entscheidungen des Data Act-Entwurfs hinsichtlich der Zuweisung von Zugangsrechten begrüßen, enthält der Entwurf gegenwärtig noch eine Reihe von Ungereimtheiten, die beseitigt werden sollten.

Rekalibrierung der Rechte des Dateninhabers und des Produktnutzer/Abdingbarkeit von Zugangsrechten bei fehlendem Machtungleichgewicht:
Die durch den Data Act („Datengesetz“)-Entwurf eingeräumten Rechte von Dateninhabern und Produktnutzern sollten nochmals kritisch überprüft werden. Zwar verdient der generelle Ansatz, die technische Exklusivposition des Dateninhabers als solche nicht anzutasten und dies durch gesetzlich definierte Zugangsrechte für Nutzer und Dritte auszugleichen, Zustimmung. Die Rechte sollten aber besser ausbalanciert werden. Sowohl der Dateninhaber als auch der Produktnutzer sollten mit einem angemessenen, von der Zustimmung der anderen Seite unabhängigen Recht zur Nutzung der Daten ausgestattet werden. Artikel 4 Abs. 6 bedarf insoweit der Überarbeitung. Zudem sollte nochmals kritisch überprüft werden, ob das Zugangsrecht des Produktnutzers in Artikel 4 Abs. 1 zwingend ausgestaltet sein muss oder ob – als alternativer Ansatz – ein beschränkter Verzicht zugelassen werden kann, sofern der Nutzer diesen Verzicht nach einer gewissen Zeit widerrufen kann.

Dritte können nach dem Data Act-Entwurf die generierten Daten nur nutzen, wenn sie diese entweder direkt vom Nutzer oder mit dessen Zustimmung vom Dateninhaber erhalten haben, Artikel 5 Abs. 1. Artikel 6 Abs. 1 und 2 sehen eine Reihe von Pflichten des Dritten vor, die bei einer entsprechenden Datennutzung zu beachten sind. In Anbetracht der unterschiedlichen Größe und wirtschaftlichen Stärke möglicher Dateninhaber, Produktnutzer und Dritter sollte der Gesetzgeber nochmals kritisch prüfen, ob die Regelungen in Artikel 6 Abs. 1 und 2 auch dann zwingender Natur sein sollen, wenn der Nutzer kein Verbraucher oder KMU ist.

Reevaluierung der Wettbewerbsverbotsklauseln in Artikel 4 Abs. 4 and Artikel 6 Abs. 2 lit. e:
Die Wettbewerbsverbote in Artikel 4 Abs. 4 und Artikel 6 Abs. 2 Buchstabe e des Data Act reichen zu weit und sollten überdacht werden

Konkretisierung der Zugangsbedingungen:
Nach Artikel 8 Data Act-Entwurf muss ein Dateninhaber, der nach Artikel 5 Data Act-Entwurf „oder nach anderen Rechtsvorschriften der Union oder nationalen Rechtsvorschriften zur Umsetzung des Unionsrechts“ Dritten gegenüber zur Gewährung des Datenzugangs verpflichtet ist, einen solchen Zugang zu FRAND-Bedingungen anbieten. Da der Dateninhaber als Einziger Zugang zu den Daten gewähren kann, ist eine solche Verpflichtung notwendig, um den Dritten vor unangemessenen oder diskriminierenden Bedingungen zu schützen. Bei der weiteren Ausgestaltung der FRAND-Bedingungen durch die Gerichte kann nicht ohne Weiteres auf Erfahrungen aus anderen Bereichen zurückgegriffen werden.

Der Data Act-Entwurf regelt im Übrigen nicht, wie der Datenzugang gemäß Artikel 4 und 5 technisch herzustellen ist. Der Gesetzgeber sollte entweder die Regelung in Artikel 28, welche technische Vorgaben für den Betrieb von Datenräumen vorsieht, so verallgemeinern, dass sie auch für den Datenzugang angewendet werden kann, oder eine neue Vorschrift zu diesem Zweck in Kapitel 3 integrieren. Eine solche Vorschrift sollte technische Vorgaben dazu enthalten, wie der Zugang und die weitere Nutzung von Daten zu ermöglichen und zu erleichtern sind.

Ausschluss des „sui generis“-Datenbankrechts:
Der Regelungsansatz des Data Act-Entwurfs zu „sui generis“-Datenbankrechten und zu Geschäftsgeheimnissen ist sachgerecht. Allerdings sollte die Formulierung von Artikel 35 überarbeitet und Artikel 8 Abs. 6 gestrichen werden.

Klärung der Anforderungen an eine Anonymisierung personenbezogener Datensätze nach der DSGVO:
Der Data Act-Entwurf enthält keine eigenständige Rechtsgrundlage für die Verarbeitung personenbezogener Daten, so dass damit zu rechnen ist, dass die DSGVO dem Zugang zu Daten nach dem Data Act-Entwurf entgegenstehen kann, soweit die maschinengenerierten Daten einen Personenbezug aufweisen. Ein Ansatzpunkt für die Auflösung des Regelungskonflikts könnte darin liegen, die Anforderungen an die Anonymisierung von Daten zu konkretisieren und Dateninhaber, Produktnutzer und Dritte dazu zu verpflichten, alle vorhandenen und wirtschaftlich zumutbaren Mittel zur Anonymisierung einzusetzen, bevor Daten weitergegeben werden, insbesondere in Konstellationen, in denen die Zustimmung der Betroffenen vorher nicht eingeholt werden kann.

Private Durchsetzung:
Der Data Act-Entwurf schließt eine private Rechtsdurchsetzung nicht aus, schreibt sie aber auch nicht ausdrücklich vor. Der Gesetzgeber sollte klarstellen, dass eine private Rechtsdurchsetzung im Grundsatz möglich ist. Zudem sollte näher bestimmt werden, wer sich mit welchen Ansprüchen an die ordentlichen Gerichte wenden kann.

Reevaluierung:
Der Data Act experimentiert mit einer neuen Zuweisung von Datennutzungsrechten in der Datenökonomie. Seine Auswirkungen auf die relevanten Märkte sollten innerhalb einer eher kurzen Frist evaluiert werden, um ggfs. Anpassungen vorzunehmen.

2. Wettbewerbsrecht

Rechtssicherheit betreffend die kartellrechtlichen Zulässigkeitsgrenzen für Datenkooperationen ist ein wichtiges Ziel. Angesichts der Vielfalt möglicher Konstellationen und eines Mangels an Fallpraxis und einschlägiger Rechtsprechung ist die Formulierung von über den Kommissionsentwurf horizontaler Leitlinien hinausreichenden aussagekräftigen abstrakten Regeln gegenwärtig aber kaum möglich. Auch eine umfassende „Daten-GVO" ist derzeit keine realistische Option. Um gleichwohl Raum für die Erprobung verschiedener Formen von Datenkooperationen zu schaffen, erscheint mit Blick auf Datenkooperationen ein Wechsel von einem „kontradiktorischen" zu einem eher „kooperativen" (oder „partizipatorischen") Ansatz der behördlichen Kartellrechtsdurchsetzung ratsam. In Deutschland verfolgt das Bundeskartellamt bereits einen solchen Ansatz. Mit der Einfügung eines neuen § 32c Abs. 4 GWB, der betroffenen Unternehmen bei erheblichem rechtlichem und wirtschaftlichem Interesse einen Anspruch auf eine Entscheidung des Bundeskartellamts verschafft, dass kein Anlass zum Tätigwerden besteht, hat der deutsche Gesetzgeber diesen Ansatz bekräftigt. Auf europäischer Ebene bieten die Reform der „Bekanntmachung der Kommission über informelle Beratung" und die anstehende Überarbeitung der VO 1/2003 Möglichkeiten, vergleichbare Mechanismen einzuführen.

Was etwaige Pflichten marktbeherrschender bzw. relativ marktmächtiger Unternehmen zur Gewährung von Datenzugang nach Artikel 102 AEUV/§ 19, 20 GWB bzw. nach § 20 Abs. 1a GWB betrifft, ist der Mangel an Fällen und Beschwerden bemerkenswert. Die in dieser Studie herangezogenen empirischen Untersuchungen deuten darauf hin, dass dies nicht auf Defiziten des Wettbewerbsrechts beruht. Mögliche Erklärungen sind vielmehr in dem frühen Stadium der Datenwirtschaft, in Informationsasymmetrien und in dem Umstand zu suchen, dass die Struktur und Formatierung von Datensätzen regelmäßig auf die Verwendungszwecke des jeweiligen Dateninhabers abgestimmt und für andere Zwecke nicht notwendig zielführend ist. Die Formulierung eines Datenzugangsbegehrens wird regelmäßig voraussetzen, dass der Petent weiß, welche Arten von Daten verfügbar sind, und über ausreichende Ressourcen und Fähigkeiten verfügt, mit potenziell großen Datenmengen zu arbeiten. Auch diese Voraussetzungen werden in vielen Fällen fehlen. Die Fokussierung von Unternehmen auf effektive Datenportabilität und damit die Möglichkeit, diejenigen Daten zu nutzen, die im Rahmen der eigenen Tätigkeit generiert wurden, erscheint daher zum gegenwärtigen Zeitpunkt der Marktentwicklung sehr plausibel. Ein Rechtsrahmen zur Gewährleistung effektiver Datenportabilität entwickelt sich jedoch gegenwärtig primär außerhalb des Wettbewerbsrechts, wie der Entwurf des DA (bzgl. Daten, die bei der Nutzung von Produkten anfallen), der DMA (bzgl. Daten, die bei der Nutzung von zentralen Plattformdiensten von Gatekeepern anfallen), § 19a Abs. 2 S. 1 Nr. 5 GWB (bzgl. Daten, die von den Normadressaten nach § 19a Abs. 1 GWB kontrolliert werden) und sektorspezifische Rechtsvorschriften belegen. Im deutschen Wettbewerbsrecht kann § 20 Abs. 1a GWB verbleibende Lücken schließen.

Gleichwohl scheint es sinnvoll, den wettbewerbsrechtlichen Rahmen für den Datenzugang in Szenario 2-Konstellationen zu überdenken. Die EFD stellt hier grundsätzlich einen geeigneten

Rahmen für die Feststellung missbräuchlicher Datenzugangsverweigerungen bereit. In Fällen, in denen der Datenzugang über die Möglichkeit entscheidet, innerhalb eines digitalen Ökosystems zu konkurrieren, das zu einem „bottleneck“ für den Zugang zu Kunden geworden ist, kann jedoch ein anderer Analyserahmen geboten sein. In solchen Fällen sollte das Kriterium der Unerlässlichkeit, das in der EFD zu Recht eng ausgelegt wird, durch eine umfassendere Interessenabwägung ersetzt werden, die der Rolle der Daten für den Wettbewerb in digitalen Ökosystemen oder Wertschöpfungsnetzen Rechnung trägt. Die Verweigerung des Zugangs zu Daten kann insbesondere missbräuchlich sein, wenn ein Ökosystem-Orchestrator sich damit von einer bisher verfolgten Open-Access-Strategie löst, die ihm zu einer beherrschenden Stellung verholfen hat. Weiterreichende Datenzugangsverpflichtungen können Ökosystem-Orchestratoren auferlegt werden, die zu Gatekeepern (Artikel 3 DMA) oder Unternehmen mit überragender marktübergreifender Bedeutung für den Wettbewerb (§ 19a Abs. 1 GWB) geworden sind. Solange ein Dateninhaber hingegen auf dem primären „Ökosystemmarkt“ effektiv durch Wettbewerb diszipliniert wird, sollte das Wettbewerbsrecht in Szenario 2-Konstellationen Datenzugangsansprüche nur zurückhaltend gewähren. In allen genannten Fällen sollte die Interessenabwägung den Unterschied zwischen „provided“, „observed“ und „derived data“ berücksichtigen. Die hier empfohlene Interessenabwägung kann innerhalb des bestehenden wettbewerbsrechtlichen Rahmens durchgeführt werden – eine Änderung des Wettbewerbsrechts ist nicht erforderlich. In Sektoren, in denen der Zugang zu Daten über die Innovations- und Wettbewerbsfähigkeit von komplementären Dienstleistern entscheidet, können sektorspezifische Rechtsvorschriften erforderlich sein, um die Datenzugangsverpflichtung zu konkretisieren und ein geeignetes Datengovernance-System zu etablieren.

3. DMA/§ 19a GWB

Die Effektivität der Datenportabilitäts- und Datenzugangsverpflichtungen der Artikel 6 Nr. 9 und Artikel 6 Nr. 10 DMA wird großteils von ihrer Implementierung abhängen. Der DMA verpflichtet Gatekeeper, die Möglichkeit zur Datenportierung in das Design von zentralen Plattformdiensten zu integrieren („compliance by design“). Keine der genannten Normen legt jedoch fest, in welchem Format und über welche Schnittstelle die Datenportabilität oder der Datenzugang herzustellen sind.

Grundlegende Entscheidungen über die Spezifikationen und Bedingungen der Datenportabilität oder des Datenzugangs können nicht allein den Gatekeepern überlassen werden, und sie sollten auch nicht allein von der Europäischen Kommission festgelegt werden. Vielmehr sollte die Europäische Kommission sicherstellen, dass sie in einem offenen Verfahren unter Einbeziehung aller relevanten Akteure und unter Berücksichtigung der Ziele des DMA entwickelt werden. Werden die Datenportabilitäts- und Datenzugangsverpflichtungen des DMA wirksam umgesetzt, so können sie offenere und innovativere Komplementärmärkte fördern (Artikel 6 Nr. 9 DMA), und gewerblichen Nutzern helfen, die von ihren Endnutzern generierten Daten besser zu nutzen (Artikel 6 Nr. 10 DMA). Der Beitrag dieser Bestimmungen zur Steigerung der Bestreitbarkeit der Gatekeeper in der Bereitstellung zentraler Plattformdienste ist demgegenüber im Zweifel eher gering. Endnutzer (Artikel 6 Nr. 9 DMA) und gewerbliche Nutzer (Artikel 6 Nr. 10 DMA) können nur Zugang zu den Daten erhalten, die

aufgrund ihrer eigenen Tätigkeit erzeugt wurden. Nur der Gatekeeper wird Zugang zum gesamten Datenbestand haben. In Anbetracht der Größen- und Verbundvorteile bei der Datenanalyse kann dies ein großer Wettbewerbsvorteil sein. Die Verpflichtung zum Datenteilen nach Artikel 6 Nr. 11 DMA geht deutlich über die vorgenannten Datenportabilitätspflichten hinaus und zielt darauf ab, die Bestreitbarkeit der Machtposition von Google auf dem Suchmaschinenmarkt zu erhöhen. Es ist zu vermuten, dass nur die größten Wettbewerber von Google von diesem Datenzugangsanspruch Gebrauch machen werden. Anders als Art. 6 Nr. 9 und Nr. 10 DMA zielt Art. 6 Nr. 11 DMA nicht darauf ab, den datenbasierten Wettbewerb auf komplementären Märkten zu fördern. Hier wäre auch eine weiterreichende Zielsetzung denkbar gewesen.

§ 19a Abs. 2 S. 1 Nr. 5 GWB ermächtigt das Bundeskartellamt, bestimmten Normadressaten Datenportabilitätsverpflichtungen aufzuerlegen, wenn andernfalls der Wettbewerb behindert würde, bleibt aber insofern hinter dem DMA zurück, als dass das Bundeskartellamt eine mögliche Wettbewerbsbehinderung konkret darlegen muss, während der DMA darauf abzielt, eine übergreifende Datenportabilitätsinfrastruktur für alle Gatekeeper und Kern-Plattformdienste zu etablieren. Einen eigenständigen Anwendungsbereich neben dem DMA kann § 19a Abs. 2 S. 1 Nr. 5 GWB mit Blick auf Dienste der Normadressaten erlangen, die keine zentralen Plattformdienste eines Gatekeepers sind. Ebenso wenig wie der DMA sieht § 19a Abs. 2 GWB Datenzugangsverpflichtungen in Szenario 2-Konstellationen vor. Eine Erweiterung des § 19a Abs. 2-Katalogs kann sich mittelfristig als sinnvoll erweisen. Hier sollte aber die Marktentwicklung abgewartet werden: Wie bereits erörtert, fehlen bislang einschlägige Fälle und Beschwerden.

4. Fusionskontrolle

Die Anwendung der Fusionskontrolle in Fällen, die datengetriebene Geschäftsmodelle betreffen, ist Gegenstand einer laufenden Reformdebatte. Diese hängt mit dem allgemeinen Diskurs über den Umgang mit Fusionen in digitalen Märkten zusammen, aber auch mit der Debatte über „Killer-Akquisitionen“. Der derzeitige Ansatz der Europäischen Kommission, sich auf nationale Verweisungen an die Europäische Kommission gemäß Artikel 22 FKVO zu verlassen, erscheint fragwürdig und unzureichend. Auch die zukünftige Wirkung von Artikel 14 DMA sollte nicht überschätzt werden. Eine Herabsetzung des Anmeldeschwellenwerts in Deutschland gem. § 35 Abs. 1a Nr. 3 GWB (von 400 Mio. EUR auf z.B. 200 Mio. EUR) könnte immerhin die Zahl der Fälle erhöhen, die unter die deutsche Fusionskontrolle fallen und daher potenziell an die EU-Kommission verwiesen werden könnten. Wir halten dies für eine Option, die der Gesetzgeber prüfen sollte.

Generell sollte der Gesetzgeber in Erwägung ziehen, die derzeitigen Fusionskontrollregelungen und ihre Durchsetzung zu aktualisieren und zu stärken, insbesondere im Hinblick auf datengetriebene Märkte und digitale Ökosysteme. Eine solche regulatorische Neuausrichtung erfordert weitere, gezieltere Untersuchungen und Konsultationen. Insbesondere sollte der deutsche Gesetzgeber den besonderen Auswirkungen datenbezogener Zusammenschlüsse auf den Wettbewerb Rechnung tragen, indem er die materiellen Regeln der Fusionskontrolle modifiziert, und zwar im Hinblick auf Vorhaben von Unternehmen von überragender

Bedeutung für den marktübergreifenden Wettbewerb nach § 19a Absatz 1 GWB. Dies bedeutet insbesondere, dass bei der Fusionskontrolle die Auswirkungen des Zusammenschlusses auf das gesamte „Ökosystem“ berücksichtigt werden müssen, um eine allzu segmentierte, ausschließlich auf Einzelmärkte fokussierte Analyse zu vermeiden.

Entsprechende Reformen sollten auch für die EU-Fusionskontrolle in Erwägung gezogen werden. Das betrifft insbesondere auch die derzeitige Praxis der Europäischen Kommission, Verpflichtungszusagen zum Datenzugang, zur Datentrennung und zur Interoperabilität zu akzeptieren. Wir halten es für ratsam, solche verhaltensbezogenen Pflichten bei datenbezogenen Fusionen unter Beteiligung marktstarker Technologieunternehmen nicht zu akzeptieren. Eine künftige Reform der europäischen Fusionskontrolle sollte für solche Fälle eine klare Beschränkung auf strukturelle Abhilfemaßnahmen vorsehen. Die Bundesregierung sollte sich für eine Reform der europäischen Fusionskontrolle einsetzen, die die materiell-rechtlichen Prüfungskriterien ebenso in den Blick nimmt wie die Anmeldeschwellen und das Verhältnis zu den nationalen Fusionskontrollregimen. Überdies ist eine Aktualisierung der EU-Fusionskontrollleitlinien unter besonderer Berücksichtigung von Bedingungen und Auswirkungen des Wettbewerbs auf datengetriebenen Märkten geboten.

5. Datenintermediäre

Datenintermediäre sind Organisationseinheiten, die den Zugang zu Daten und deren gemeinsame Nutzung durch Dateninhaber und Datennutzer ermöglichen, kontrollieren oder erleichtern. In datengetriebenen Märkten können ihnen mehrere Funktionen zukommen, wie etwa die Senkung von Transaktionskosten oder der Abbau von Informationsasymmetrien. Sie können sich damit positiv auf die Wettbewerbsfähigkeit und Innovationskraft solcher Märkte auswirken. In der Praxis wird bereits mit verschiedenen Modellen von Datenintermediären experimentiert. Die Entwicklung steht jedoch erst am Anfang.

Der kürzlich verabschiedete EU-Daten-Governance-Rechtsakt (DGA) bietet einen umfassenden Rechtsrahmen für „Datenvermittlungsdienste“ (DIS), die eine Untergruppe aller Datenintermediäre darstellen. Der DGA schreibt verbindliche Regelungen vor. Danach müssen DIS ihre Dienste sowohl amtlich registrieren, um sie in der EU rechtmäßig anbieten zu können, als auch verschiedene Anforderungen einhalten. Der DGA zielt darauf ab, die Entwicklung von DIS und die Entstehung von entsprechenden Märkten zu fördern. Dies wäre in der Tat wünschenswert. Offen bleibt allerdings, ob sich der DGA insoweit als ein wirksames Regulierungsinstrument erweist. Bislang sind noch keine tatsächlichen Auswirkungen zu beobachten, nicht zuletzt, weil die Regeln für DIS erst ab September 2025 anwendbar sein werden. Derzeit überprüfen die Branchenakteure ihre Geschäftsstrategien und -modelle. Gleichzeitig herrscht große Rechtsunsicherheit in Bezug auf den Anwendungsbereich (z.B. inwieweit GAIA-X-basierte Datenvermittlungsmodelle abgedeckt sind) und auf die gestellten Anforderungen/Verpflichtungen, die einer weiteren Auslegung und Anwendung durch Behörden und Gerichte bedürfen. Dies trägt dazu bei, dass die regulatorischen Auswirkungen des DGA im Wesentlichen unvorhersehbar sind.

Erstrebenswert wäre ein allgemeiner Rechtsrahmen, der die Entwicklung von Datenintermediären erleichtert. Eine kohärente Integration von Datenintermediären in die Rechtsordnungen der EU und der Mitgliedstaaten berührt allerdings gleich mehrere rechtliche Regelungen: Die Datenschutzvorschriften sollten so ausgestaltet werden, dass Datenintermediäre wirksam in die Marktordnung für den Datenaustausch integriert werden können. Bei der Integration von Datenintermediäre in das Vertragsrecht und die FRAND-Grundsätze gibt es Verbesserungspotenzial. Z.B. könnte der EU-Gesetzgeber erwägen, Artikel 8 Abs. 1 des Data Act auch auf DIS gemäß Artikel 12 lit. f DGA zu erstrecken. Der Data Act lässt Datenintermediäre unberücksichtigt und sollte aber klarstellen, inwiefern Daten über Datenintermediäre mit Dritten geteilt werden können. In Bezug auf das Wettbewerbsrecht können Datenintermediäre zu einer effizienteren Datenwertschöpfung beitragen, indem sie die gemeinsame Nutzung von Daten ermöglichen und fördern, aber diese auch verhindern, um die Einhaltung des Wettbewerbsrechts zu gewährleisten. So sollte die Fusionskontrolle Datenintermediäre als ein Instrument zur Stärkung der strukturellen Wirkung von Verpflichtungszusagen anerkennen, sofern sie verhindern, dass Daten zusammengeführt oder für Zwecke verwendet werden, welche die Datenmacht und -konzentration erhöhen würden. Mit Blick auf Artikel 101 AEUV können Datenintermediäre sowohl Normadressaten als auch Compliance-Einrichtungen sein. In beiderlei Hinsicht könnten Leitlinien Rechtssicherheit für sich entwickelnde Geschäftsmodelle schaffen. Sektor-spezifische Rechtsvorschriften können Datenintermediäre strengeren Regeln unterwerfen. Solch einschneidende Markteingriffe sind aber nur gerechtfertigt, wenn es deutliche Hinweise auf Marktversagen oder besondere Gründe des öffentlichen Interesses gibt.

VI. Handlungsempfehlungen

Querschnittsfragen

Im Lichte der wachsenden Bedeutung von Daten für Wettbewerb und Innovation haben die Unternehmen begonnen, deren Potenzial auf vielfältige Weise auszuloten und zu entwickeln. Oft nutzen sie „ihre“ Datensätze hierfür exklusiv, mitunter werden Datenkooperationen abgeschlossen oder Daten mit anderen Unternehmen geteilt. Grundsätzlich steht es den Unternehmen frei, ihre eigene Strategie für die Erprobung und Entwicklung neuer Datenverwendungsmöglichkeiten zu wählen.

Im Gegensatz zu den USA, hat die EU es sich zum Ziel gesetzt, die Entwicklung der Datenwirtschaft proaktiv durch Bereitstellung eines innovativen Rechtsrahmens zu fördern. Das Anliegen, in einem dynamischen Umfeld Rechtssicherheit zu schaffen, ist grundsätzlich zu begrüßen. Die EU muss jedoch darauf achten, (1) die Kohärenz zwischen ihren verschiedenen Rechtsprojekten zu gewährleisten, sowohl in Bezug auf die jeweils verwendeten Begrifflichkeiten als auch mit Blick auf die grundsätzlichen Regelungsansätze, und (2) Flexibilität zu gewährleisten, um ein Experimentieren mit den neuen Möglichkeiten der Datenwirtschaft und ggfs. schnelle Anpassungen des Regelrahmens an neue Erkenntnisse oder veränderte Umstände zu ermöglichen.

Der entstehende Rechtsrahmen erkennt implizit an, dass die tatsächlichen Dateninhaber „ihre" Daten innerhalb der u.a. durch die DSGVO, das Recht der Geschäftsgeheimnisse und die Wettbewerbsregeln für den Informationsaustausch gezogenen Grenzen wirtschaftlich nutzen dürfen. Bei Daten, die durch die Nutzung eines Produkts oder einer Dienstleistung erzeugt werden, zeichnet sich ein Grundsatz ab, dass Produkt- oder Dienstenutzer ein Recht auf Portierung und Verwendung der durch sie „ko-generierten" Nutzungsdaten haben sollen, einschließlich des Rechts, die Daten mit Dritten zu teilen. Für Daten, die bei der Nutzung einer Maschine erzeugt werden, wird dieser Grundsatz im Data Act-Entwurf in breiter Form anerkannt. Für personenbezogene Daten ist er in Artikel 20 der DSGVO zu erkennen. Für Daten, die durch die Nutzung eines Dienstes erzeugt werden, ist der Grundsatz in Artikel 6 Nr. 9 und 10 DMA verankert – allerdings nur im Verhältnis zu Gatekeepern. § 19a Abs. 2 Nr. 5 GWB ermächtigt das Bundeskartellamt, Unternehmen mit überragender marktübergreifender Bedeutung für den Wettbewerb Datenportabilitätsverpflichtungen aufzuerlegen. Zu klären bleibt, warum das Recht auf Datenportabilität im Anwendungsbereich des Data Act-Entwurfs breit ausgestaltet ist, in der DSGVO mit Blick auf personenbezogene Daten ebenfalls weit anerkannt, aber schwach ausgestaltet wird, und bei Daten, die durch die Nutzung von Diensten entstehen, hingegen nur in Abhängigkeit von einer spezifischen Machtposition anerkannt wird (siehe DMA).

Daten sind ein in hohem Maße heterogenes Gut. Die weit verbreitete Analogie mit Rohöl ist insoweit irreführend. Der im Entstehen begriffene Rechtsrahmen erkennt die Heterogenität von Daten implizit an und verfolgt für den Datenzugang dementsprechend einen differenzierten Ansatz. Es besteht weitgehende Einigkeit darüber, dass der Zugang zu „beobachteten" Daten auf breiterer Front zu gewähren ist als der Zugang zu „abgeleiteten" Daten.

Für die Umsetzung des Datenzugangs gilt es, ungeachtet aller Unterschiede allgemeine Grundsätze zu entwickeln, welche vertrags-, immaterialgüter- und wettbewerbsrechtliche Gesichtspunkte zusammenführen.

So muss, wann immer Datenzugang angeordnet wird, die mangelnde Information des Nicht-Dateninhabers über vorhandene Datensätze, deren Struktur und Format berücksichtigt werden. Die P2B-VO enthält bereits einige Informationspflichten. Aus dem Data Act-Entwurf und aus dem Vertragsrecht können sich weitere Informationspflichten ergeben. Der Versuch, diese Informationspflichten zu konsolidieren und auf allgemeine Grundsätze zurückzuführen, liegt nahe.

Außerdem müssen standardisierte Vertragsbedingungen für den Datenzugang entwickelt werden, die unabhängig davon Anwendung finden können, ob die Daten freiwillig oder aufgrund einer gesetzlichen Datenzugangsverpflichtung weitergegeben werden. Neben standardisierten Vertragsbedingungen werden allgemeine Grundsätze für die Grenzen des Datenzugriffs benötigt, wie sie sich aus der DSGVO, dem Recht der Geschäftsgeheimnisse oder dem Wettbewerbsrecht zum Informationsaustausch ergeben können. In all diesen Bereichen sollte „praktische Konkordanz" das Ziel sein: Der Datenzugang soll ermöglicht werden, gleichzeitig aber ein technischer und rechtlicher Rahmen geschaffen werden, der anderen Schutzzielen angemessen Rechnung trägt.

Wo Datenzugangsverpflichtungen bestehen, muss auch deren effektive Implementierung mitgedacht werden. Es gilt, übergreifende Prinzipien für die rechtliche, technische und institutionelle Ausgestaltung des Datenzugangs zu entwickeln. Unter anderem muss ein Datenzugang zu FRAND-Bedingungen gewährleistet werden. Die Bedeutung von FRAND kann im Kontext des Datenzugangs aber etwas anderes bedeuten als beim Zugang zu SEP. Weitergehend wird eine Standardisierung von Datenformaten und Schnittstellen erforderlich sein, um Datenportabilität, Dateninteroperabilität und Datenzugang zu einem funktionierenden Bestandteil der Datenwirtschaft werden zu lassen. Datenzugang kann auf unterschiedliche Weise gewährt werden – mitunter in Form eines in situ-Zugangs; in anderen Situationen wird eine tatsächliche Portierung der Daten geboten sein. Es werden verschiedene Data Governance-Regime entwickelt werden müssen. Hierbei wird auch der möglichen Rolle von Datenmittlern Rechnung zu tragen sein.

Aus wettbewerbsrechtlicher Sicht wird es von entscheidender Bedeutung sein, praktikable Data-Governance-Regelungen zu entwickeln, die überall dort effektiven Datenzugang gewährleisten, wo er Voraussetzung für wirksamen Wettbewerb ist. Die weitere Debatte über Datenzugang in Ökosystemen und datengetriebenen Märkten muss daher von der Entwicklung gut funktionierender Data-Governance-Regime begleitet werden.

Konkret unterbreiten wir die folgenden Empfehlungen:

Die Rolle des Staates

1. Obwohl das Anliegen, mehr Vertrauen in die digitale Wirtschaft zu schaffen, ein wichtiges Politikziel ist, und ein rechtlicher Rahmen geschaffen werden soll, der datenbezogene Handlungsbefugnisse regelt und klärt, sind die zahlreichen von der Europäischen Kommission eingeleiteten Regulierungsinitiativen für die betroffenen Unternehmen und Branchen eine Herausforderung. Der Markt für die gemeinsame Nutzung von Daten befindet sich erst in der einer frühen Phase. Bei der Einleitung weiterer Initiativen ist daher zur Vorsicht zu raten. Etwaige weitere Initiativen müssen ferner eng mit dem derzeitigen Rechtsrahmen abgestimmt werden, um weitere Unsicherheit zu vermeiden. Insbesondere ist eine einheitliche Terminologie zu empfehlen. Darüber hinaus sollten die Regulierungsinitiativen ein gewisses Maß an Reflexivität und Agilität aufweisen, d.h. ursprüngliche Maßnahmen sollten angepasst oder zurückgezogen werden, wenn sich die Zielmärkte in eine andere als die ursprüngliche unterstellte Richtung entwickeln. In diesem Zusammenhang könnten Instrumente wie Reallabore vor allem in sektorspezifischen Kontexten als Entdeckungsverfahren eingesetzt werden, bevor ein horizontaler Rechtsrahmen geschaffen wird.

Vertragsrecht

2. Die aktuellen europäischen Gesetzesinitiativen (Data Act, DMA) dürften die Dynamik in der unternehmensübergreifenden Datennutzung in Deutschland und Europa steigern. Gesetzliche Regelungen zur Ausgestaltung von Datenzugangs- und -nutzungsverträgen sind grundsätzlich wünschenswert, sollten aber die Erfahrungen der sich gerade erst entwickelnden Vertragspraxis zugrunde legen und dieser Entwicklung nicht vorgreifen. Die im Entwurf eines Data Act

vorgeschlagene Entwicklung von Modellverträgen unter Beteiligung der Europäischen Kommission kann die Herausbildung einer solchen Vertragspraxis unterstützen. Zwingende Regeln sollten nur beim Vorliegen eines Marktversagens in Betracht kommen. Der europäische und der deutsche Gesetzgeber sollten in Betracht ziehen, weitere Informationspflichten einzuführen, welche die von Artikel 3 Data Act und Artikel 9 P2B-Verordnung nicht erfassten Fallgestaltungen regeln, insbesondere für den Fall ko-generierter Daten aus der Nutzung von Dienstleistungen.

Data Act-Entwurf

Wir empfehlen der Bundesregierung, den Vorschlag für einen Data Act im Grundsatz zu unterstützen. Folgende Punkte bedürfen jedoch einer Anpassung:

3. Die zwingende Natur des Datenzugangsrechts des Produktnutzers gem. Artikel 4(1) Data Act-Entwurf sollte im Hinblick auf die innovationsfördernde Zielsetzung des Gesetzes überdacht werden. Eine Alternative wäre es, den Produktnutzern dort, wo Machtasymmetrien fehlen, einen vertraglichen Verzicht auf ihr Zugangsrecht zu erlauben, solange der Produktnutzer das Recht behält, diesen Verzicht nach einiger Zeit zu widerrufen.

4. Die Wettbewerbsverbote in Artikel 4 Abs. 4 und Artikel 6 Abs. 2 lit. e des Data Act-Entwurfs reichen zu weit und sollten überdacht werden.

5. Artikel 4(6) des Data Act-Entwurf, der die Nutzung der Daten durch den Dateninhaber von einer vertraglichen Vereinbarung mit dem Produktnutzer abhängig macht, ist neu zu fassen. Grundsätzlich sollten sowohl dem Dateninhaber als auch dem Produktnutzer je eigenständig ausübbare Nutzungsrechte an den Daten zustehen.

6. Die technische Ausgestaltung des Datenzugriffs muss konkretisiert werden.

7. Der Data Act-Entwurf sollte klarstellen, dass eine private Durchsetzung durch den Produktnutzer und Dritte zulässig ist.

Wettbewerbsrecht

8. Für eine Änderung der §§ 19, 20 GWB im Hinblick auf Datenzugang besteht gegenwärtig kein Anlass. Vielmehr sollte der Gesetzgeber die Entwicklung der Fallpraxis und Rechtsprechung abwarten und diese einer gründlichen Ex-post-Evaluation unterziehen („evidenzbasiertes Kartellrecht“).

9. Mehr Rechtssicherheit für Datenkooperationen im Rahmen der Artikel 101 AEUV/§ 1 GWB ist wünschenswert. Gleichwohl empfehlen wir, mit der Einführung einer „Daten-GVO“ zu warten, bis sich auf der Grundlage einer einschlägigen Fallpraxis robuste Grundprinzipien herausschälen. Ein besseres Verständnis dafür, welche Arten von Vereinbarungen Kollusionsrisken mit sich bringen, welche Daten-Governance-Regelungen diesen wirksam entgegenwirken können etc., lässt sich nur durch einschlägige Präzedenzfälle gewinnen.

10. Mehr Rechtssicherheit für Unternehmen lässt sich bis dahin durch informelle Beratungsmechanismen gewährleisten. Während dies auf deutscher Ebene im Rahmen des §

32c GWB gut funktioniert, schützt eine § 32c GWB-Entscheidung nicht vor einem späteren Verbot der Kooperation durch die Europäische Kommission. Auch auf europäischer Ebene gilt es daher, die informelle Beratung im Falle innovativer Datenkooperationen zu stärken. Der Entwurf der Europäischen Kommission für eine überarbeitete Mitteilung zur informellen Beratung ist ein Schritt in diese Richtung, schöpft das Potenzial einer stärker kooperativ angelegten Durchsetzung in diesem Bereich aber nicht aus. Es sollte ein Regelrahmen entwickelt werden, der neue Kooperationsformen schnell und flexibel begleitet und neben der juristischen und ökonomischen, auch die informationstechnische Perspektive miteinbezieht.

Fusionskontrolle

11. Der deutsche Gesetzgeber sollte erwägen, die Schwelle für die Anmeldepflicht des § 35 Abs. 1a Nr. 3 GWB von 400 Mio. EUR auf z.B. 200 Mio. EUR abzusenken, um die Anzahl der Transaktionen zu erhöhen, die unter die deutsche Fusionskontrolle fallen und daher möglicherweise nach Artikel 22 FKVO an die Europäische Kommission verwiesen werden können.

12. Der deutsche Gesetzgeber sollte das derzeitige Fusionskontrollsystem im Hinblick auf datengetriebene Märkte und digitale Ökosysteme aktualisieren und stärken. Eine solche regulatorische Neukalibrierung würde weitere, gezieltere Analysen und Konsultationen erfordern. Zu prüfen wäre insbesondere eine Modifikation der materiell-rechtlichen Regeln der Fusionskontrolle im Hinblick auf Vorhaben, an den Unternehmen mit überragender marktübergreifender Bedeutung für Wettbewerb nach § 19a Absatz 1 GWB beteiligt sind. In solchen Fällen sind die Auswirkungen eines Zusammenschlusses auf das gesamte „Ökosystem" zu prüfen. Zu erwägen ist, ob eine Beschränkung wirksamen Wettbewerbs bereits dann anzunehmen ist, wenn ein angemeldetes Vorhaben einem Unternehmen nach § 19a Abs. 1 GWB den Erwerb von mehr oder neuen Daten ermöglicht oder die Datenerhebung effizienter gestaltet. Eine differenziertere Vermutung könnte insbesondere bei Akquisitionen greifen, die komplementäre Dienstleistungen/Produkte betreffen. Entsprechend den geänderten materiell-rechtlichen Anforderungen müsste auch die Beweislast angepasst werden und einem differenzierteren Ansatz folgen.

13. Die Bundesregierung sollte sich auf europäischer Ebene für eine Reform der FKVO einsetzen, die sowohl die materiell-rechtlichen Prüfungskriterien als auch das Verhältnis zu den nationalen Vorschriften und Anmeldeschwellen betrifft. Die derzeitige Praxis der Europäische Kommission, Verpflichtungen zum Datenzugang, zur Datentrennung und zur Interoperabilität zu akzeptieren, sollte kritisch hinterfragt werden. Jedenfalls bei datenbezogenen Fusionen, an denen marktstarke Unternehmen beteiligt sind, sollten nur strukturelle Abhilfemaßnahmen zulässig sein.

DMA/§ 19a GWB

14. Die Effektivität der Datenzugangsverpflichtungen (und insbesondere der Datenportabilitätsverpflichtungen) des DMA bei der Förderung datengetriebener Innovationen und des Wettbewerbs auf komplementären Märkten wird von ihrer wirksamen Implementierung abhängen. Die Europäische Kommission bzw. die europäischen Normungsorganisationen sind gehalten, einen offenen und partizipativen Standardisierungsprozess für die Entwicklung von Datenformaten und offenen Schnittstellen sicherzustellen, der alle relevanten Interessengruppen

einschließt. Wichtig ist es ferner, die Funktionsfähigkeit und die Auswirkungen der Standards zu überwachen und sicherzustellen, dass sie flexibel angepasst werden können. Auch in diesem Zusammenhang ist ein „partizipatives“ Durchsetzungsregime zu empfehlen.

15. § 19a Abs. 2 S. 1 Nr. 5 GWB kann neben dem DMA eine Rolle spielen, wenn es um die Portabilität von Daten bei der Nutzung von Diensten geht, die keine zentralen Plattformdienste i.S.d. DMA sind (oder wenn § 19a GWB Normadressaten benennt, die keine Gatekeeper im Sinne des DMA sind). Für diese Fälle sind Verfahren zur Konkretisierung der Anforderungen an die Datenportabilität zu entwickeln. Als Vorbild kann das Verfahren nach § 32b GWB dienen.

16. Weder der DMA noch § 19a Abs. 2 GWB sehen die Auferlegung von Datenzugangsverpflichtungen in Szenario 2-Konstellationen vor. Wir schlagen vor, die Möglichkeit der Auferlegung solcher Verpflichtungen mittelfristig zu prüfen. Eine „one size fits all“-Lösung ist hier allerdings nicht angebracht.

Datenintermediäre

17. Die Auswirkungen des DGA sind in hohem Maße unvorhersehbar. Im Hinblick auf die künftige Evaluierung und Überprüfung des DGA durch die Europäische Kommission sollte die Bundesregierung in den kommenden Jahren Erkenntnisse über die Marktentwicklung sammeln, um Vorschläge für notwendige Änderungen der Verordnung zu unterbreiten.

18. Der allgemeine Rechtsrahmen sollte Datenintermediäre kohärent in die Rechtsakte der EU und der Mitgliedstaaten einbinden, um ihre weitere Entwicklung zu erleichtern. Zu diesem Zweck sollten der EU-Gesetzgeber, die nationalen Gesetzgeber und die Wettbewerbsbehörden Folgendes in Erwägung ziehen: Gestaltung von Datenschutzvorschriften zur wirksamen Integration von Datenintermediären in die Marktordnung für den Datenaustausch; bessere Abstimmung von Datenintermediären mit dem Vertragsrecht und den FRAND-Grundsätzen, z. B. durch Ausweitung von Artikel 8 Abs. 1 DA auf DIS gemäß Artikel 12 lit. f DGA; Bezugnahme auf Datenintermediäre und Klärung ihrer Rolle im Rahmen des DA; Berücksichtigung von Datenintermediären als Instrument zur Stärkung der strukturellen Wirkung von Abhilfemaßnahmen in der Fusionskontrolle zur Vermeidung von Daten- und Marktkonzentration; Berücksichtigung der konstruktiven Rolle von Datenintermediären in den Horizontal-Leitlinien im Hinblick auf Artikel 101 AEUV. Strengere sektorspezifische Vorschriften für Datenintermediäre sind nur dann in Erwägung zu ziehen, wenn eindeutige Beweise für ein Marktversagen vorliegen oder dies im öffentlichen Interesse eindeutig gerechtfertigt ist.

Table of contents

A. Research assignment

The Bundesministerium für Wirtschaft und Klimaschutz (BMWK) has commissioned a study on the legal framework for access to data in Germany and the EU from a legal, economic and policy angle, with a special focus on the well-functioning of competition.

The role of data and data access for the data economy – including for competition in the data economy – has already been the subject of various studies.[1] It is well established that competition law – as a 'horizontal' legal framework that may require, or at times limit, data access – interacts with an ever tighter web of other rules and regulations that affect data access in complex ways. Some of them – such as the General Data protection Regulation (GDPR), contract and intellectual property (IP) laws – are of horizontal application. The horizontal legal framework is complemented by a growing number of sector-specific data access rules.[2]

In its 'European Data Strategy',[3] the European Commission has set out the goal to better capture the benefits of the evolving data economy in the years to come. It proposes to create a comprehensive legal framework that aims to increase the use of and demand for data and data-enabled products and services throughout the Single Market, while simultaneously protecting fundamental rights, safety and cybersecurity and ensuring compliance with the GDPR. Promoting and protecting competition in digital markets – including by way of a stronger consideration of access to data – is another important aspect of the evolving framework, as is the goal to enable market actors, including start-ups and small and medium-sized enterprises (SMEs), to access data to enhance their opportunities to innovate. In order to implement this agenda, the EU is currently engaged in a number of legislative projects. Some of them are meant to add another horizontal layer to the existing set of rules. Others are tailored to specific sectors. Among the ongoing legislative policy initiatives are:

- The so-called Digital Markets Act (DMA) which will subject gatekeepers to special obligations. Agreement in the trilogue proceeding was reached in March 2022. The DMA is expected to be passed by the European Parliament this year and to enter into force in 2023.
- The Data Governance Act (DGA) regulates data intermediation services and will apply from 24 September 2023.[4]

[1] See, for example, Schallbruch/Schweitzer/Wambach, Ein neuer Wettbewerbsrahmen für die Digitalwirtschaft, Bericht der Kommission Wettbewerbsrecht 4.0, 2019; Schweitzer/Haucap/Kerber/Welker, Modernisierung der Missbrauchsaufsicht für marktbeherrschende Unternehmen, 2018; ZEW, Datenmärkte in der digitalisierten Wirtschaft: Funktionsdefizite und Regulierungsbedarf, 2017; Crémer/de Montjoye/Schweitzer, Competition Policy for the digital era, Final report, 2019; Feasey/de Streel, Data Sharing for Digital Markets Contestability, CERRE Report September 2020; Krämer/Schnurr/BroughtonMicova, The role of data for digital markets contestability, CERRE Report September 2020.

[2] For a holistic analysis see German Federal Ministry of Justice and Consumer Protection/Max Planck Institute for Innovation and Competition, Data Access, Consumer Interests and Public Welfare, 2021.

[3] COM(2020) 66 final.

[4] OJ 2022 L 152, 1.

- A Draft Data Act[5] which proposes to create novel rights of access to and use of data for data co-generators. The European Commission has published its proposal for a Data Act on 23 February 2022. The debate is ongoing.
- Simultaneously, the European Commission is pro-actively pursuing a number of Common European Data Space initiatives.[6]

Access to data has also been an issue at the national level. The 'GWB-Digitalisierungsgesetz' (GWB-Law on Digitization), which entered into force in 2021, has provided for a better consideration of access to data in competition law proceedings in various ways. Firstly, a new § 19a GWB empowers the Bundeskartellamt to impose data-related remedies upon designated undertakings of paramount cross-market significance for competition across markets. Secondly, § 19(2) No. 4 GWB now specifies that the 'Essential Facilities Doctrine' (EFD) can also be applied to data where access to data is objectively necessary to access and compete on a related market. Lastly, § 20(1a) GWB sets out that a dependency from another undertaking within the meaning of § 20(1) GWB – which triggers the prohibition to unduly obstruct or discriminate against other undertakings under § 19(1) with § 19(2) No. 1 GWB – may also result from a dependency on access to data which is held by another undertaking. A right to access to data may result.

This wave of legislative (and policy) initiatives at the EU and the national level raises several questions in need of further analysis. In addition, the German Bundestag has requested the Federal Government to report on the new GWB provisions on data access after a period of four years and to assess whether the different interests implicated have been adequately considered, to inquire into the effects of data access on the innovative strength of the German economy and to review whether due regard has been made to issues of data protection, IP protection and protection of trade secrets in a practicable manner.

Against this background, the BMWK has asked the consortium to report on the state of law and the state of the debate on access to data and to outline options for action. Firstly, the study should consider under which conditions and to what extent data access mandates are an appropriate instrument to protect competition. This question can be asked with regard to the prohibition of abuses of dominance, the DMA and § 19a GWB as well as § 20(1a) GWB, but also within the framework of merger control. In addition, legislative action might (or might not) be needed that reaches beyond competition law – legislation of a horizontal kind, such as the Draft Data Act, or rather of a sector-specific kind.

Secondly, the study should discuss the limits for data access and data sharing regimes or other forms of data cooperation under competition law. Any mandatory data access regime can create tensions: it may interfere with IP rights, trade secrets and possibly with the GDPR; and depending on its scope, it may create novel risks for competition and possibly innovation that must enter the balance.

[5] COM(2022) 68 final.

[6] COM SWD(2022) 45 final.

Thirdly, where data access is mandated, the need and possible form of a 'data governance' regime to implement rights to access data effectively should be considered. Contract law will be decisive for the implementation of data access rights, and there may be a need – or at least place – for data intermediaries that should be considered.

Fourthly, the BMWK also asks whether the newly created right of an undertaking engaged in a cooperation of significant legal and economic interest under § 32c(4) GWB – namely the right to have the Bundeskartellamt decide on whether there is no cause for action – is sufficient to eliminate any relevant disincentives to such cooperations, or whether further legislation or guidelines should be passed. *Inter alia*, a review of standard terms based on contract law principles may be advisable.

Finally, the legislative developments with regard to data access in other important jurisdictions, particularly in the U.S., and the implementation of such legislation should be considered.

B. The structure of our report

Our study starts with an overview of the policies that currently accompany the unfolding of the data economy at the European and German level, with a side glance at the ongoing policy debates in the U.S. (part C). Both the European and the German legislator have decided to take a pro-active stance vis-à-vis the ongoing transformation, striving to both boost and guide the evolution of the data economy by providing a legislative framework. The European and German economy should be able to capture the benefits of the 'data revolution', in particular to tap the potential for innovation and growth, but to do so within the framework of EU rules and values.

The pro-active policies to promote the unfolding of a data economy raise fundamental questions regarding the role of the state vis-à-vis the market in times of economic transformation. Part D will briefly revisit this debate. In addition, it will set out the categorizations and terminology we will use in the report and summarise the existing empirical evidence on the state of the data economy in Europe and Germany, with a focus on the role that data access and data sharing agreements play both throughout the economy and in specific sectors. An understanding of the hurdles for data sharing and data markets to gain momentum is key for any legislative intervention. Based on this stocktaking exercise, we will sketch different options for the EU and Germany to define their role regarding the development of the data economy, and their approach towards mandatory data access requirements more specifically. In principle – and radically simplifying the continuum of options – two different approaches can be distinguished.[7] On the one hand, 'access to data' obligations may be considered as a tool to remedy well-defined market failures, such as a data-related abuse of monopoly power. On the other hand, the legislator may find that the role of data as a relevant input into innovation along the supply chain – from the development of products and services to their production, distribution and commercialisation – and, consequently, their economic and competitive value are changing so dramatically that a more pro-active and 'infrastructural' approach is needed. This would address or avoid an inefficient underuse of data and deliberately accelerate the transformation towards a data-driven economy. In that case, a new definition or (re-)allocation of rights to data access may be needed. The latter approach appears to underlie the Draft Data Act.

Against this conceptual background, part E sets out the legislative framework as it currently exists. Given the different stances that a jurisdiction may adopt vis-à-vis the emerging data economy, this study does not focus on data-related competition law and 'ancillary' regulatory law alone. Rather, it takes a more holistic approach. In particular, our analysis extends to the data rights and data access debates in IP and contract law and strives to identify possible weaknesses or deficiencies of the existing legal framework in addressing the existing hurdles to a more active data sharing as they have emerged from our empirical survey in part D.

[7] We leave aside relevant public interest justifications for data access regulation in this study – like systems safety requirements etc.

In part F, we then turn to a discussion of the resulting need for legislative reform. We will first discuss the Draft Data Act, striving to lay bare its underlying logic, asking whether it will likely contribute, or can be made to contribute, to a well-functioning data economy. We will then focus on possible reforms in the realm of competition law, including merger control. Finally, we will look at the role that data intermediaries may possibly play in promoting data access and data sharing.

Part G will conclude and summarise the results of the study in the form of concrete recommendations.

When discussing data access, it is essential to visualise specific scenarios in which data access may be relevant. Given the myriad types of data and data use as well as goals of data access, such scenarios can never claim to be complete, i.e. to cover the full range of data access settings as they exist in the real world. Nonetheless, the following reference scenarios for data access have shown to be useful in the past,[8] and we refer to them throughout our study:[9]

- (1) Firstly, market participants who have had part in the generation of individual level data – e.g. machine usage or behavioural data – may request access to these data and the possibility to use them, or to let third parties make use of them. We call this the 'data access by data co-generators' or 'data portability'-scenario.
- (2) Secondly, third parties who offer complementary services within the framework of a data driven value creation network or digital ecosystem may request access to large sets of bundled individual level or aggregate data to develop and improve their complementary services.
- (3) Thirdly, third parties may request access to holders of large, unique datasets that are needed to develop and train algorithms – in particular, artificial intelligence (AI) algorithms – for uses unrelated to the fields of activity of the data controller.

These scenarios will help us to answer the central question under which conditions and to what extent data access requirements are appropriate. In brief, we propose that the EU may be called for to improve the legal infrastructure for data markets by better defining the initial rights of access to data of data co-generators and those third parties that derive their right of access from data co-generators. When it comes to scenarios 2 and 3, we propose that the right way to think about data access is a traditional market failure approach. The most prominent market failure that may justify mandated data access is the abuse of power. While competition law has traditionally focused on market power, the cross-market relevance of many types of data suggests that it will need to focus more on 'ecosystem power' in the future, as is already done in § 19a GWB, and to some extent in the DMA. However, there may be a need to expand an ecosystem-driven type of analysis beyond the reach of § 19a GWB and the DMA. Also, a focus on digital and data-driven ecosystems may justify sector-specific regulation at times.

[8] Crémer/de Montjoye/Schweitzer, Competition policy for the digital era, Final report, 2019, p. 73 et seq.; Schweitzer/Haucap/Kerber/Welker, Modernisierung der Missbrauchsaufsicht für marktbeherrschende Unternehmen, 2018, p. 258 et seq.

[9] For a more comprehensive account of these scenarios, see part E(III)(2)(b)(aa)(1).

C. Data access and data sharing in the data economy: EU and German policy agendas – and a side glance at the U.S.

I. European data strategies

As the digital transformation of the economy and society is underway, there is broad agreement that data is at the centre of this transformation.[10] Data is generated in ever increasing amounts. In B2C relations, it allows for the development of more personalised products and services, as well as for targeted marketing. Businesses can make use of data to, *inter alia*, optimise their production processes and logistics, to engage in data-driven innovation, including an integration of AI. Digital platforms rely on data to fulfil their match-making function. In many, if not most areas, access to data is becoming a precondition – or at least a prominent factor – for innovating and competing effectively.

The European and the German legislator are determined to seize the new opportunities. Simultaneously, both are conscious of the risks that accompany the evolution of the data economy – ranging from risks to privacy, safety and cybersecurity to a far-reaching re-distribution of rents, to novel risks of market and gatekeeper power and a dissemination of technologies that may be used for manipulative purposes, potentially on a broad scale.[11] In both jurisdictions, the legislator is striving to pinpoint the problems that come with the fast deployment of novel technologies and business models and to identify strategies to deal with them.

1. The evolution of the European Commission's thinking on the data economy

For almost a decade now, the new role of data and the need to adapt the legal framework to "tap the full potential of the digital economy […]"[12] figures prominently on the EU's agenda. From the start, the European Commission was determined to build a 'thriving data-driven economy'.[13] Together with an enabling infrastructure and the development of common standards for technology and data interoperability, the private sharing of datasets has been found to be an important part of this endeavour.

With its Digital Single Market Strategy of 2015, the European Commission declared the 'free flow of data' to be one of the three pillars of an effort to realise the growth potential of the European digital economy. Restrictions on the free movement of data for reasons other than

[10] COM(2020) 66 final.

[11] See Zuboff, The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power, 2019.

[12] EUCO 169/13 (2013), para. 2.

[13] COM(2014) 442 final.

protection of personal data were to be removed, and issues such as ownership, interoperability, usability and access to data were to be addressed.[14]

The focus on removing obstacles to the free flow of data remained unchanged in 2017 when the European Commission published its Communication on 'Building a European Data Economy'. Unjustified restrictions imposed by public authorities and legal uncertainty in data sharing were considered key hurdles to be addressed at this point.[15] In order to remove administrative barriers to a free data circulation, Regulation (EU) 2018/1807 on the free flow of non-personal data[16] was passed. The incentives of market actors to engage in data sharing practices were to be increased by enhancing legal certainty through non-legislative instruments.[17]

In 2018, the European Commission launched its 'European data space initiative'.[18] Originally, the European Commission apparently envisioned one single European data space. With its 'European Strategy for Data', the European Commission turned to the idea of setting up nine sectoral 'European data spaces' in 'strategic sectors' where data shall be made available on a voluntarily basis and be reused against remuneration or for free.[19] These sectoral data spaces should be complemented by the establishment of an Open Science Cloud.[20] Additional data spaces have followed, such that the number has meanwhile grown to twelve. The list now includes:

- An Industrial (manufacturing) data space[21]
- A Green Deal data space[22]
- A Mobility data space[23]
- A Health data space[24]

[14] COM(2015) 192 final, 15; See also COM(2017) 228 final.

[15] COM(2017) 9 final.

[16] OJ 2018 L 303, 59 ensures that non-personal data can be stored, processed and transferred anywhere in the EU. This regulation also addresses the problem of 'vendor lock-in' at the level of providers of data processing services, by introducing self-regulatory codes of conduct to facilitate switching data between cloud services.

[17] COM SWD(2017) 2 final, 30 et seq.

[18] COM(2018) 232 final.

[19] COM SWD(2022) 45 final, 2-4. See also COM(2020) 66 final, 30 et seq.

[20] COM(2020) 66 final, 10 and 22.

[21] COM SWD(2022) 45 final, 12 et seq.; see also COM(2021) 350 final.

[22] COM SWD(2022) 45 final, 13-17. In the context of the GreenData4All initiative, the Commission will assess the modernization of and the interaction between the INSPIRE Directive, OJ 2007 L 108, 1, and the Directive on public access to environmental information, OJ 2003 L 41, 26. Furthermore, the creation of the Green Deal data space will be driven by the following strategies and action plans: COM(2021) 572 final; COM(2021) 400 final; COM(2020) 98 final; COM(2021) 82 final; COM(2020) 381 final.

[23] COM SWD(2022) 45 final, 17-20; See also in this context Digital Europe Programme, Work Programme for 2021-2022, Annex, p. 47-49; COM(2020) 789 final; COM(2020) 579 final; COM C(2021) 5763 final; for further information see also https://mobility-dataspace.eu/ (last visited 4.7.2022).

[24] COM SWD(2022) 45 final, 20-23; COM(2020) 690 final; for further information see also https://ec.europa.eu/health/ehealth-digital-health-and-care/european-health-data-space_en (last visited 4.7.2022).

- A Financial data space[25]
- An Energy data space[26]
- An Agricultural data space[27]
- Data spaces for Public Administration[28]
- A Skills data space[29]
- An Open Science Cloud[30]
- A data space for media[31]
- A data space for cultural heritage[32]

Each data space shall deploy data sharing, processing and storage tools and services, provide for a transparent and fair data governance structure, ensure the interoperability of data and thereby promote the free flow of data among market participants.

The European Commission's Common European data spaces initiative thereby pursues an agenda that is significantly more ambitious than the concept of 'data spaces' as it is known from the data science literature, where a full integration of datasets or homogeneity in their schematics and semantics is not necessarily pursued[33] and where labour-intensive data integration of datasets is performed only when needed.[34] In contrast, Common European data spaces shall "overcome legal and technical barriers to data sharing", reduce *ex ante* transaction costs and *ex post* contractual risks, overcome coordination problems, act as commitment

[25] COM SWD(2022) 45 final, 23 et seq.; COM(2020) 591 final; main components: (i) digital access to publicly disclosed financial and sustainability related information, COM(2020) 590 final; (ii) easier reporting and sharing of supervisory data among EU and national supervisory authorities, COM(2021) 798 final; (iii) business-to-business and business-to-consumer data sharing and reuse in the EU financial sector (open finance), COM(2021) 720 final.

[26] COM SWD(2022) 45 final, 24-26; COM(2020) 299 final.

[27] COM SWD(2022) 45 final, 26-28. For further information see https://digital-strategy.ec.europa.eu/en/events/information-session-common-european-agricultural-data-space (last visited 4.7.2022).

[28] Consisting of (i) public administrations legal data space, (ii) Public Procurement Data Space, and (iii) Public administrations security data space for innovation, COM SWD(2022) 45 final, 28-32.

[29] COM SWD(2022) 45 final, 32 et seq.

[30] COM SWD(2022) 45 final, 34-36. For further information see https://ec.europa.eu/info/research-and-innovation/strategy/strategy-2020-2024/our-digital-future/open-science/european-open-science-cloud-eosc_en (last visited 4.7.2022).

[31] COM SWD(2022) 45 final, 36-38.

[32] COM SWD(2022) 45 final, 38 et seq.; COM C(2021) 7953 final; COM C(2021) 7914 final.

[33] See for the difference between schematics and semantics Hassan/Curry in Curry, Real-time Linked Dataspaces, 2020, p. 152: 'At the schema level, this includes the definition of concepts, entities, and their relationships, as well as specific attributes of entities. While basic semantics can be specified in the form of simple vocabularies and constraints, a more detailed semantic representation may require formal ontologies.'

[34] Until then, datasets remain only loosely integrated – see http://dataspaces.info/principles-and-practices/#page-content (last visited 4.7.2022). Similar GAIA-X: 'In general, the term "data space" refers to a type of data relationship between trusted partners, each of whom apply the same high standards and rules to the storage and sharing of their data. It is of key importance that the data is not stored centrally but at source and are therefore only shared (via semantic interoperability) when necessary […]', https://www.gaia-x.eu/what-is-gaia-x/data-spaces (last visited 4.7.2022).

devices,[35] "enhance the availability, quality and interoperability of data" and ultimately lead to a fast emergence of well-functioning European internal market for data. In order to achieve these goals, Common European data spaces, supported by European funding, shall establish a secure infrastructure to pool, access, share, process and use data in specific sectors and provide the necessary data sharing and processing tools. Furthermore, they shall address issues of trust by way of common rules and by establishing data governance mechanisms that safeguard European rules and values.[36] The availability, quality and interoperability of data shall thereby be significantly enhanced.[37] Essentially, the Common European data spaces are based on a self-regulatory approach, but in a number of sectors covered, self-regulation is complemented by legal rules (co-regulatory approach).

Six design principles shall apply horizontally to all data spaces:[38]

- Data control
- Governance
- Respect of EU rules and values
- Technical data infrastructure
- Interconnection and interoperability
- Openness

Although the European Commission is promoting data spaces in strategic sectors, the ultimate aim in the long run is that "the different data spaces will be interconnected so that they progressively lead to a genuine European space in which data is broadly shared and used, while fully respecting the rights of individual persons and businesses over data."[39] The European Common data spaces-project – which the European Commission continues to promote pro-actively[40] – is ultimately driven by the ambition to establish a European infrastructure for emerging data markets.

Simultaneously, the European Commission published its 'Guidance on sharing private sector data in the European data economy'[41] which provides a 'how to' guide focused on data sharing models, legal aspects, and technical issues and set out a number of, albeit non-binding, key principles for data sharing that should help create a level playing field for B2B data sharing, namely transparency, shared value creation, respect for each other's commercial interests, ensure undistorted competition, and the minimisation of data lock-in.

[35] Martens et al. JRC121336 (2020), 6.

[36] COM SWD(2022) 45 final, 2 et seq.

[37] Id., 2; COM(2020) 66 final, 16.

[38] COM SWD(2022) 45 final, 3 et seq.

[39] Id., 2.

[40] Ibid.

[41] COM SWD(2018) 125 final, 3, 5 et seq.

Despite these public policy impulses, private data sharing and pooling initiatives have gained traction only slowly.[42] Against this background and accompanied by growing concerns about the 'gatekeeper' positions of the largest digital platforms (i.e. GAFA), the debate on voluntary, but also on mandatory data sharing has gained momentum. In its 2020 'European Strategy for Data', the European Commission has laid out its agenda for the creation of the EU data economy in the next ten years.[43] The European Commission's general premise is that, despite some progress, not enough data is available for innovative re-use. It identifies power imbalances in relation to data access and use, data interoperability issues that prevent the combination of different sources within and between sectors and a missing data governance framework as possible reasons for this scarcity.[44] A 'comprehensive approach' is proposed to incentivise data sharing and increase the availability, use of and demand for data and data-enabled products and services, including an easy access to an almost infinite amount of high-quality industrial data.[45] Currently, the European Commission is in the process of working off this agenda.

A first priority for operationalising the European Commission's vision was the creation of a cross-sectoral "enabling legislative framework for the governance of common European data spaces".[46] A proposal for a 'Data Governance Act'[47] was introduced in November 2020, which, among other things, establishes a notification and supervisory framework for provision of so called 'data sharing services' (e.g. data intermediation services, cf. Article 9), and a framework for voluntary registration of entities which collect and process data made available for altruistic purposes (Article 1(1)). The DGA entered into force on 23 June 2022 and will apply from 24 September 2023.

On 23 February 2022, the European Commission has published its proposal for a 'Data Act' ('Draft Data Act')[48], which strives to establish data access, portability and usage rights for data co-generators.[49] The need for interoperability standards is explicitly recognised in the Draft Data Act (see Article 28).

To resolve these interoperability issues, the European Commission included this topic in its current annual a 'Rolling Plan for ICT Standardisation'. The application of shared compatible formats and protocols for gathering and processing data from different sources shall ensure that data become interoperable across sectors and vertically within supply chains.[50]

---

[42] Arnaut et al., Study on data sharing between companies in Europe, Final report, 2018, https://op.europa.eu/de/publication-detail/-/publication/8b8776ff-4834-11e8-be1d-01aa75ed71a1/language-en (last visited 4.7.2022), p. 44 et seq. (not representative); COM SWD(2022) 35 final, 4 et seq.

[43] COM(2020) 66 final.

[44] Id., 6 et seq.

[45] Id., 1, 4 et seq.

[46] Id., 12 et seq.

[47] COM(2020) 767 final.

[48] COM(2022) 68 final.

[49] See further below, part F(I).

[50] See https://joinup.ec.europa.eu/collection/rolling-plan-ict-standardisation/rolling-plan-2022 (last visited 4.7.2022).

In its Data Strategy, the European Commission also announced that it would consider *ex ante* regulation to address particularly entrenched forms of market power.[51] In December 2020, the European Commission published a proposal for a'Digital Markets Act',[52] which is part of the 'Digital Services Package'[53] and aims at ensuring fairness and contestability in digital markets, where 'gatekeeper' platforms are active. The DMA also foresees particular data sharing, portability, and interoperability obligations as well as data access restrictions for such gatekeepers (cf. Article 5 No. 2, Article 6 No. 2, 9, 10, 11 and Article 7).[54] The Digital Markets Act is scheduled to be put for final vote in the European Parliament in July 2022 before being formally adopted by the European Council. It will enter into force 20 days after publication in the EU Official Journal and will start to apply six months thereafter in 2023.

The European Commission's agenda for increasing data access is without prejudice to its commitment to the legislative limitations to data access: in sharing data, undertakings have to comply, *inter alia*, with the GDPR,[55] with the Cybersecurity Act[56] and with the Trade Secrets Directive.[57]

2. The German Data Strategy

Data access has also been heavily debated in Germany.

Data access as a competition law remedy was a core issue in the study 'Modernisierung der Missbrauchsaufsicht für marktbeherrschende Unternehmen' commissioned by the BMWK in preparation of the 10th amendment to the GWB. The authors of the study considered that the criteria for determining whether a denial of access to data by a dominant undertaking constitutes an abuse may somewhat differ from the criteria used to determine an abusive denial of access to infrastructure and IP rights.[58] This is particularly true if the data is generated as a by-product and without any special investment. Furthermore, a data access right based on § 20(1) GWB was proposed, in particular in the context of value creation networks, when data is controlled exclusively by one participant in the network and this data is necessary for substantial value creation in this network, and if some kind of 'company-specific dependency' exists.[59] Even if markets for such data have not (yet) emerged, a denial of access may result in an anti-competitive exclusion. These propositions fed into the 10th amendment of the GWB, which

[51] COM(2020) 66 final, 14.

[52] COM(2020) 842 final.

[53] https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package (last visited 4.7.2022).

[54] See further below, part E(V).

[55] OJ 2016 L 119, 1.

[56] OJ 2019 L 151, 15.

[57] OJ 2016 L 157, 1.

[58] Schweitzer/Haucap/Kerber/Welker, Modernisierung der Missbrauchsaufsicht für marktbeherrschende Unternehmen, 2018, p. 131-139.

[59] Id., p. 133-156.

specifically deals with data access in two provisions related to the abuse of dominance, which were hotly debated during the drafting process:[60] § 19(2) no. 4 GWB – which codifies the German version of the EFD – was broadened to the effect that a refusal to supply another undertaking with access to data may constitute an abuse of dominant market power if such access is objectively necessary in order to operate on an upstream or downstream market.[61] § 20(1a) GWB provides for a data access right in cases of 'relative market power', i.e., when an undertaking is dependent on accessing data controlled by another undertaking in order to carry out its own activities.[62] In such a case, a refusal to grant access in exchange for an 'adequate compensation' may also constitute abusive conduct prohibited under competition law. Furthermore, specific data-related remedies may now be imposed on undertakings that have found to be of paramount cross-market significance (see § 19a(2), 1st sentence, No. 4 and 5 GWB).[63]

Data access and the legal framework for data cooperations were also discussed in the report of the 'Kommission Wettbewerbsrecht 4.0' – likewise commissioned by the BMWK. Among other things, the final report proposed the adoption of a sector-specific regulation for dominant online platforms. The portability of user and usage data in real time and in an interoperable data format and interoperability with complementary services figured prominently among the rules ultimately proposed.[64] In addition, the authors recommended to further explore the potentials of data intermediaries for promoting competition.[65] The recommendations also included the establishment of a voluntary notification system at the European level for cooperative projects in the digital domain to enhance legal certainty for such cooperations.[66]

---

[60] See Brenner in Bien et al., Die 10. GWB-Novelle, 2021, Ch. 1 paras. 59 et seq. For comments from companies and associations of undertakings see https://www.bmwi.de/Navigation/DE/Service/Stellungnahmen/GWB-Digitalisierungsgesetz/stellungnahmen-gwb-digitalisierungsgesetz.html (last visited 4.7.2022). Large companies with data-based business models feared 'free rider' problems, a dampening of innovation incentives (see for example the comments of BDI, at 3; Bitkom, at 21 et seq.; Amazon, at 32 et seq.; Google, at 20) and a data usage contrary to the original purpose (comment of Bitkom, at 24). By contrast, SMEs appeared largely supportive of the reform (see comment of ZGV, at 2). All comments expressed the need for clearer and more certain rules as well as the need for further sector-specific regulation – either to limit (comment of BDI, at 9) or to expand data access (comment of ZGV, at 8 et seq.).

[61] 'An abuse exists in particular if a dominant undertaking as a supplier or purchaser of a certain type of goods or commercial services … refuses to supply another undertaking with such a good or commercial service for adequate consideration, in particular to grant it access to data, networks or other infrastructure facilities, and if the supply or the granting of access is objectively necessary in order to operate on an upstream or downstream market and the refusal threatens to eliminate effective competition on that market, unless there is an objective justification for the refusal.'

[62] 'Dependence within the meaning of subsection (1) may also arise from the fact that an undertaking is dependent on accessing data. Refusing to grant access to such data in return for adequate compensation may constitute an unfair impediment pursuant to subsection (1) in conjunction with § 19(1), no. 1. This shall also apply even if such data have not yet been commercially traded.'

[63] For all of this see further below: part E(V)(2).

[64] Schallbruch/Schweitzer/Wambach, Ein neuer Wettbewerbsrahmen für die Digitalwirtschaft, Bericht der Kommission Wettbewerbsrecht 4.0, 2019, p. 38 et seq.

[65] Id., p. 43 et seq.

[66] Id., p. 62 et seq.

The SPD went further. In 2019, it put forward a 'Daten-für-Alle-Gesetz' proposal that would have created a far-reaching data sharing obligations for dominant firms and a corresponding right to access non-personal and completely anonymised data for all market actors, not only for data co-generators (this reaches way beyond what it foreseen in the Draft Data Act).[67]

In January 2021, the German Federal Government published a 'Datenstrategie der Bundesregierung'.[68] Among other things, the strategy foresaw the establishment and promotion of an interoperable decentralised data infrastructure which should consolidate existing infrastructures – a project that has become known as GAIA-X.[69] Increasing legal certainty was another issue that figured high on the German agenda: with regard to personal data, data protection law should be clarified, e.g. by specifying the requirements for an anonymisation of data under the GDPR. With regard to non-personal data, voluntary data sharing should be incentivised. In some data-driven markets, data sharing obligations should be considered, whether under competition law or sectoral regulation.[70] Innovative forms of data cooperation should be encouraged and the role for data intermediaries explored.[71]

A strategy paper 'Daten für den Wandel nutzen' released by Anna Christmann, Dieter Janecek and other members of the German Green Party in August 2021 sets out a partly overlapping agenda.[72] Here, increasing legal certainty under the GDPR, the promotion of data sharing between private actors through data intermediaries and the promotion of data infrastructures and interfaces figure prominently as well. Dominant undertakings shall be obliged to offer data portability and ensure the interoperability of services. In addition, the possibility for breaking up with excessive data power irrespective of an abuse is considered. On the institutional side, the establishment of a 'data institute' (comparable to the UK 'Open Data Institute') is proposed.

With regard to data policies, the SPD, BÜNDNIS 90/DIE GRÜNEN und FDP 'Koalitionsvertrag 2021-2025' declares to support the establishment of data infrastructures (e.g. through instruments as data trustees, data hubs, and data donations), to strive for better access to data, in particular to enable start-ups and SMEs to innovate.[73] Moreover, the coalition aims to strengthen standardised and machine-readable access to self-generated data, and it promotes anonymisation techniques and create legal certainty through standards.[74] Finally, a data institute

[67] SPD, Digitaler Fortschritt durch ein Daten-für-Alle-Gesetz, https://www.spd.de/fileadmin/Dokumente/Sonstiges/Daten_fuer_Alle.pdf (last visited 4.7.2022).

[68] Bundesregierung, Datenstrategie – Innovationsstrategie, 2021. For a table with all planned measures see p. 6.

[69] Id., p. 10-15.

[70] Id., p. 16-24.

[71] Id., p. 33-36.

[72] https://annachristmann.de/daten-fuer-den-wandel-nutzen/ (last visited 4.7.2022).

[73] https://www.spd.de/fileadmin/Dokumente/Koalitionsvertrag/Koalitionsvertrag_2021-2025.pdf (last visited 4.7.2022), p. 14.

[74] Ibid.

should foster data availability and standardisation and establish data trustee models and licenses.[75]

II. The policy debate on data access in the U.S.

1. Overview

While issues of data access and data sharing are discussed in the U.S. as well, the debate differs in significant respects.

The goal to pro-actively create and promote data markets, which drives many European initiatives – e.g. the proposal to create special data access and usage rights (see the Draft Data Act) or the establishment and promotion of special 'data spaces' with public support – is largely absent from the U.S. debates. The ALI/ELI Draft Principles for a Data Economy, which have put forward the idea of an access right for co-generated data, have not generated much attention in the U.S. so far (which may change after their final adoption by the ALI).[76] It seems that with regard to data access, the U.S. relies on the market to produce adequate solutions. The U.S. debates on data focus on one side on the recognition of property or ownership rights for personal data – which so far is a rather academic debate – and on the other side on portability of personal data under privacy laws and in specific sectors such as banking or automotive. Also, it is discussed whether interoperability obligations should be imposed on large digital gatekeeper platforms specifically – whether based on special laws to be passed or on an expanded interpretation of general antitrust laws.

There is some debate on whether to revive the EFD with a view to data access. Given the scepticism with which the EFD is generally received in the U.S., this proposition is not the primary focus of the public debate, however. At least for the near future, it is not a realistic option. Instead, a more pro-active data portability and interoperability regulation is being discussed. Also, several bills have been proposed that would impose data-related obligations on the largest digital platforms. A realistic possibility for the bills to be passed only exists for two of these bills, namely the American Choice and Innovation Online (ACIO) Act and the Open App Markets Act (see further below).

So far, there is little debate on the limits that Section 1 Sherman Act may impose on voluntary data sharing arrangements. Information sharing agreements are subject to a per se prohibition if price information is exchanged and there is evidence of an agreement to fix or stabilise

[75] Ibid.

[76] The project was approved by ALI's membership at the 2021 Annual Meeting but has not yet been officially adopted, see American Law Institute, https://www.ali.org/projects/show/data-economy (last visited 4.7.2022).

prices.[77] However, the applicability of information sharing rules to data sharing agreements or other antitrust limits of data sharing agreements have hardly been discussed in the U.S. so far.[78]

2. U.S. Debates on the allocation of data access and usage rights and data-related contract law

a) Debate on data property or data ownership

In the U.S. academic discourse, property or ownership rights for data are discussed very actively, however with a strong focus on data privacy. Rights against invasion of privacy have traditionally been grounded in tort law principles.[79] A violation of an individual's privacy rights entitles them to seek damages.[80] Different from a violation of the right of ownership or property, for which protection by means of injunctions is available, the common law principles of tort law only provide damages as a remedy. Injunctions must be pleaded on the basis of equity.[81] The weakness of the tort law approach to privacy has already been discussed in the late 1960s when computer technology and collection of personal data were in a very early stage. Westin proposed in 1967 that personal information should be recognised as an object of property rights so that individuals could forbid collection and use of information about data subjects without their consent, hence protecting their privacy.[82] The idea of a strengthening of privacy by property was later prominently put forward by Lessig in his often cited paper 'Privacy as Property' in which he argues that "the norms associated with property talk should be used as a means of reinforcing privacy generally". In his view, "we would better support privacy within American society if we spoke of privacy as a kind of property."[83]

Today, proponents of a property concept of privacy also refer to the function of property rights as – at least partially tradeable – commodity on data markets.[84] According to this line of argument, a property right on personal information would enable the data subject to become

---

[77] The McCarran-Ferguson Act established an antitrust exemption for the insurance industry – see 5 U.S.C. § 1011 et seq. This exemption is currently under critique – see e.g. Mason Malone, *Sharing Is Not Always Caring: Reevaluating the Insurance Industry's Antitrust Exemption and Information Sharing in the Machine-Learning Era*, 58 Hous. L. Rev. 987 (2021).

[78] If the anticompetitive potential of sharing data is appreciated at all, it is in the context of mandated data access as a remedy to an antitrust infringement or as argument against revising the EFD – see Makan Delharim, Speech at University of Haifa (Oct. 17, 2018) (transcript available https://www.justice.gov/opa/speech/assistant-attorney-general-makan-delrahim-delivers-remarks-university-haifa-israel (last visited 4.7.2022)); Jon M. Yun, *The Role of Big Data in Antitrust*, *in* GAI Report on the Digital Economy 241 (Joshua D. Wright & Douglas H. Ginsburg eds., 2020).

[79] See the famous article of Samuel Warren & Louis D. Brandeis, *The Right to Privacy*, 4 Harv. L. Rev. 193, 199-206 (1890).

[80] Lauren Henry Scholz, *Privacy as Quasi-Property*, 101 Iowa L. Rev. 1113, 1116-1123 (2016); Jeffrey Ritter & Anna Mayer, *Regulating Data as Property: A New Construct for Moving Forward*, 16 Duke L. & Tech. Rev. 220, 248 (2018).

[81] Mark A. Lemley & Philip J. Weiser, *Should Property or Liability Rules Govern Information?*, 85 Tex. L. Rev. 783, 786 (2007).

[82] Alan Westin, Privacy and Freedom (1967).

[83] Lawrence Lessig, *Privacy as Property*, 69 Soc. Res. 247 (2002). See also Scholz, *op. cit.*, 1123.

[84] For an early voice see Kenneth C. Laudon, *Markets and Privacy*, 39 Communications of the ACM 92 (1996).

active on the market for personal information and to extract parts of the value created with its data.[85] Such market-oriented arguments have attracted more attention recently in light of the economic success of data driven business models. Several articles have developed more or less detailed proposals of how such a data property right should be conceptualised. According to Schwartz a property right on personal information should be construed as a bundle of interests to be shaped through attention to five areas: inalienabilities, defaults, a right of exit, damages, and institutions.[86] Based on these components he suggests a data privacy right comprising use-transferability restrictions with an opt-in requirement and private rights of enforcement, which are partly inspired by the old German data protection rules.[87] Ritter and Mayer suggest that the ownership of data should be allocated to the party who first controls the data technically. Such an ownership should not derogate from the ability of data subjects to exercise their privacy rights. Once ownership would be attached through digital systems, the rights, privileges, controls, and constraints of data usage were to be enforced through electronic contracting mechanisms, especially blockchain technology.[88] The article is of special interest since it mainly focuses on machine-generated data with the example of vehicle data. Jurcys et al. argue for the recognition of a property right in personal/user-generated data which individuals are able to collect in their personal data clouds or 'digital wallets'. Such user-held data collected in an individual's digital wallet should be protected by a property law type of entitlements.[89]

But the concept of privacy (or in a broader sense data) as property has also been criticised in legal literature. According to Cohen a property concept would rather weaken than strengthen privacy protection: "Recognizing property rights in personally-identified data risks enabling more, not less, trade and producing less, not more, privacy."[90] Cofone in a recent article emphasises that the concept of data ownership would magnify "well-known problems of consent in privacy law: asymmetric information, asymmetric bargaining power, and leaving out inferred data."[91]

So far, the academic debate on the different property approaches to personal (or non-personal) data has not been taken up by U.S. courts and legal practice. Courts continue to apply tort law principles and more recent data privacy legislation.

b) Privacy laws, ALI Principles

[85] See Patricia Mell, *Seeking Shade in a Land of Perpetual Sunlight: Privacy as Property in the Electronic Wilderness*, 11 Berkeley Tech . L. J. 1, 5 (1996); Lessig, op. cit., 261.

[86] Paul M. Schwartz, *Property, Privacy, and Personal Data*, 117 Harv. L. Rev. 2055, 2097 (2004).

[87] Mainly the BDSG.

[88] Ritter & Mayer, *op. cit.*, 260-277.

[89] Paulius Jurcys et al., *Ownership of User-Held Data: Why Property Law Is the Right Approach* (Oct. 1, 2020), https://ssrn.com/abstract=3711017 (last visited 4.7.2022).

[90] Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 Stan. L. Rev. 1373, 1391 (2000).

[91] Ignacio Cofone, *Beyond Data Ownership*, 43 Cardozo Law Review 501 (2021).

The protection of data privacy in the U.S. is regulated in numerous statutes both on federal and state level. The first major statutes on the federal level, the Fair Credit Reporting Act (1970) and the Privacy Act (1974), were later followed by a number more specific statutes, before the federal legislator in 1998 enacted a first major privacy act focussing on internet services, the Children's Online Privacy Protection Act (COPPA).

Of the many enactments on state level, the California Consumer Privacy Act (CCPA) deserves special attention.[92] The CCPA was adopted in 2018 and entered into force in 2020. It is often described as the most ambitious U.S. data privacy legislation and as a U.S. counterpart to the European GDPR. The CCPA is of special importance not only because of the significance of the Californian market for the whole U.S. and the numerous internet companies with headquarters in the State of California but also because of its spill-over effects into other jurisdictions. Technically, the CCPA creates rights for Californian citizens only. However, if companies want to offer uniform services in all U.S. states, it is an obvious choice to provide those services in compliance with the CCPA.[93]

The CCPA goes beyond older U.S. privacy legislation. It contains a right to know about the personal information a business collects about consumers and how it is used and shared (Section 1798.100 Civil Code); this right contains a far-reaching requirement for data portability in lit. d.[94] The CCPA further provides a right to delete personal information collected from consumers (with some exceptions) (Section 1798.105 Civil Code); a right to opt-out of the sale of their personal information (Section 1798.120 Civil Code); and a right to non-discrimination for exercising their CCPA rights, meaning that a business shall not discriminate against a consumer because the consumer exercised any of the consumer's rights under the CCPA (Section 1798.120 Civil Code). In contrast to the GDPR, the CCPA is not based on a principle that the processing of data is lawful only based on the data subject's consent or another specific legal ground. Furthermore, the CCPA provides rather limited remedies for violations of its requirements; civil actions may only be instituted in case of 'personal information security breaches' (Section 1798.150 Civil Code). Apart from this, the enforcement of the CCPA is handed over to a newly established California Privacy Protection Agency (Section 1798.199.10 Civil Code).

---

[92] See from the abundant literature on the CCPA Yunge Li, *The California Consumer Privacy Act of 2018: Toughest U.S. Data Privacy Law with Teeth?*, 32 Loy. Consumer L. Rev. 177 (2019-2020); Nicholas F. Palmieri, *Who Should Regulate Data: An Analysis of the California Consumer Privacy Act and Its Effects on Nationwide Data Protection Laws?*, 11 Hastings Sci. & Tech. L.J. 37 (2020); Sanford Shatz & Susan E. Chylik, *The California Consumer Privacy Act of 2018: A Sea Change in the Protection of California Consumers' Personal Information*, 75 The Business Lawyer 1917 (2020).

[93] Elizabeth Harding et al., *Understanding the scope and impact of the California Consumer Privacy Act of 2018*, 2 J. Data Protection & Privacy 234-253 (2020).

[94] "A business that receives a verifiable consumer request from a consumer to access personal information shall promptly take steps to disclose and deliver, free of charge to the consumer, the personal information required by this section. The information may be delivered by mail or electronically, and if provided electronically, the information shall be in a portable and, to the extent technically feasible, in a readily useable format that allows the consumer to transmit this information to another entity without hindrance. A business may provide personal information to a consumer at any time, but shall not be required to provide personal information to a consumer more than twice in a 12-month period."

In 2020, the American Law Institute published the 'Principles of Law, Data Privacy' which restate the amalgam of the current U.S. data privacy law of different federal and state constitutional laws, statutes and common law principles.[95] Of special interest is the detailed provision on 'Data Portability' in § 9. The ALI Principles are more detailed than the CCPA, but also deviate in certain aspects, e.g. they provide the possibility for the data controller to require a reasonable fee 'when appropriate'. Also, the provisions on enforcement deserve special attention. § 14 provides a list with a variety of enforcement mechanisms including enforcement by public authorities and civil proceedings. The availability of these remedies depends on a case-by-case decision for which the factors to be considered are listed. The 'Reporter's Notes' explain that data privacy laws notably differ in the availability of private rights of actions for individuals. However, even if a given data privacy law does not foresee such private rights of action, its material standards can still play a role for the analysis of common law actions based on tort or unjust enrichment, where a standard of care has to be assessed.[96]

c) No property right for non-personal data, but trade secret protection

For non-personal data, U.S. law does not recognise any specific property or other exclusive right.[97] Whereas the reluctance to recognise a property-kind of right has at least been partially compensated in case of personal data by a growing number of privacy laws, no such substitute for property has been developed for non-personal data so far. Yet, it is apparent that tech companies in the U.S. de facto regard data as their asset and trade it even though the doctrinal basis to justify ownership of data may still be unstable.

Sets of non-personal (or personal) data are usually not protected by intellectual property rights. Creative databases may be protected by copyright if the selection or arrangement of the elements is original, see sections 102(a), 103(a) U.S. Copyright Act. But this will only cover a small share of the datasets in question. Much of the structured and unstructured 'big data' collected and stored by businesses is not selected or arranged in a specific manner but retained in so called 'data lakes'. Different from the EU, U.S. copyright law has not implemented a 'sui generis' right for non-original databases.

Trade secret protection is of far greater practical importance in the U.S. since it applies to both structured and unstructured datasets.[98] Trade secret protection in the U.S. is available under federal and state law, including common law grounds. Many of the state laws have been adopted on the basis of the Uniform Trade Secret Act (USTA) of 1985. In 2016 the Federal Defend Trade Secrets Act (DTSA) was passed to provide federal jurisdiction for civil causes of action for misappropriation of trade secrets. The definitions of both instruments cover all kinds of

[95] Principles of the Law: Data Privacy (American Law Institute ed., 2020).

[96] Id., 119-126.

[97] Bret A. Hrivnak, *United States*, *in* Law of Raw Data 397 (Jan Bernd Nordemann & Christian Czychowski eds., 2021).

[98] Hrivnak, *op. cit.*

information that derive economic value from not being generally known and that is subject to reasonable efforts taken by the owner to keep such information secret. It is obvious that holders of datasets usually take measures to keep their data secret, including limiting access to employees, having parties with access signing confidentiality agreements, maintain technical barriers etc. Protection of trade secrets in the U.S. is not without limits. The USTA protects trade secrets only against misappropriation by 'improper' means which does not encompass discovery by independent invention or discovery by 'reverse engineering'.[99] Still, the USTA does not provide a right of access to datasets that are protected as trade secrets. A party seeking access would therefore have no legal ground to force the data holder to disclose data or grant access.

Given the technical possibility of data holders to exclude others from accessing their datasets and the legal protection of many of those datasets as trade secrets, it is up to the data holder to decide whether other parties get permission to access such data. Typically, the basis for such a permission is a license contract which in the U.S. is subject to the principle of freedom of contract. Such license agreements on datasets will either be based on trade secrets – and provide safeguards for the secrecy of the date – or on a merely contractual specification of the covered data and on technical protection measures.[100]

d) No general access right to datasets, few sector-specific rules

U.S. law traditionally puts much weight on the private parties' freedom to advance their own interests through contracts. Under the principle of freedom of contracts, parties are free to choose whether they want to conclude a contract, with whom they want to conclude a contract and what the specific conditions should be. These principles also apply with regard to datasets collected and stored by private entities. As of today, the European discussions on general access rights to data or access rights to co-generated data has not reached the other side of the Atlantic. This may change once the Data Act has been enacted. One may also expect that the ALI/ELI Draft for Principles for a Data Economy, once they are adopted, will push the idea of an access right to co-generated data forward.[101] But for the time being, neither the academic nor the broader economic and policy discourse on data seems to address general access rights.

To this date, the U.S. law also follows a different approach with regard to sector-specific access regimes. Whereas in Europe, 'Open Banking' was essentially driven by the Payment Services Directive (EU) 2015/2366 (PSD2),[102] the U.S. regulators so far left it mainly to market forces to develop new business models for the banking sector. Such business models rely on the consumer's permission to access their bank accounts or other sensitive financial information and on practices such as 'screen scraping'. When the Biden administration ordered the

[99] National Conference of Commissioners on Uniform State Laws, Uniform Trade Secret Act with 1985 Amendments, Comment on Section 1.

[100] Hrivnak, *op. cit.*

[101] See Principle 20, ALI-ELI Principles for a Data Economy.

[102] See part E(III)(2)(b)(aa)(2).

Consumer Financial Protection Bureau (CFPB) to issue further regulations for such data transfers to other banks and fintech services in July 2021, this initiative was mainly driven by concerns over the security of the banking sector and consumer data.[103] The situations in the U.S. and in the EU also differ with regard to vehicle data. In the EU access to vehicle data has been regulated since 2007 by Regulation 715/2007 (EU) for repair data and on-board diagnostics with the aim to ensure fair competition on the repair and maintenance aftermarket. The U.S. approach so far relies on self-regulation. In 2014, manufactures and aftermarket associations came to a 'Memorandum of Understanding' for the U.S. market according to which vehicle owners and technicians are supposed to have the same access to information, tools, and software that car companies make available to licensed dealers.[104] However, given the growing complexity and greater importance of information technology (and driver's data) for electric and other recent vehicles, independent repair shops appear to be increasingly locked out from the aftermarket. Against this backdrop, a proposal for a 'Right to Equitable and Professional Auto Industry Repair (REPAIR) Act' has been introduced to the House of Representatives in February 2022,[105] but its prospects of success are still unclear.

3. Antitrust policy debate in the U.S.

Beyond such sectoral initiatives, antitrust law, and more particularly Section 2 Sherman Act and Section 5 FTC Act, might provide a legal basis for mandating access to data, data portability or data interoperability for that matter. The EFD, which would feature access to data as the pertinent remedy, continues to be highly controversial however (a). A requirement to ensure data portability is considered a candidate for regulation that would complement antitrust law (b). Data interoperability might be a viable antitrust remedy to anti-competitive exclusion in some cases (c). There is little debate on whether the state should pro-actively promote data standardisation. A market-based evolution of standards appears to be favoured. Generally, the U.S. debate on data-related rules of conduct based on antitrust law – such as the antitrust debate more broadly – is characterised by a marked divide. While some argue for a shift in antitrust policy towards a significantly more pro-active approach, and while proponents of this view occupy important political positions[106] and receive substantial public attention, the arguably dominant view continues to support a more restrictive interpretation of the antitrust rules. As it is likely that U.S. courts would follow this interpretation, no huge swings are to be expected in the realm of U.S. antitrust law in the near and medium term. If at all, some special legislation

---

[103] Evan Weinberger, *Did Biden Open Up Banking? The President's CFPB Order Explained*, Bloomberg Law (July 12, 2021), https://news.bloomberglaw.com/banking-law/did-biden-open-up-banking-the-presidents-cfpb-order-explained (last visited 4.7.2022).

[104] See Memorandum of Understanding (Jan. 15, 2014), https://www.autocare.org/docs/default-source/government-affairs/r2r-mou-and-agreement-signed.pdf?sfvrsn=40570f58_4 (last visited 4.7.2022).

[105] Press Release, Robby L. Rush, Rush Introduces REPAIR Act to Ensure Equal Access to Auto Repair Data for Independent Repair Shops and Preserve Consumer Choice (Feb. 3, 2022), https://rush.house.gov/media-center/press-releases/rush-introduces-repair-act-ensure-equal-access-auto-repair-data (last visited 4.7.2022).

[106] See, in particular, Lina Khan – Chairwoman of the FTC; Tim Wu – member of the National Economic Council and special assistant to the president for technology and competition policy; Jonathan Kanter – Assistant Attorney General of the Department of Justice.

on the obligations of the largest digital platforms may be forthcoming (see 4.) – albeit significantly more limited than the DMA or § 19a GWB.

a) Mandating data access under U.S. antitrust law: should the 'Essential Facilities Doctrine' be revived?

While the possibility to mandate dominant firms – and in particular dominant platforms – to grant competitors access to their data has been heavily debated in the EU competition law community (see below, part E(III)(2)(b)), the parallel debate under U.S. antitrust law is much more reserved. The noticeable caution in the U.S. debate is arguably linked to a dearth of cases under Section 2 Sherman Act in which access to data would be the appropriate or preferred remedy and to a predominantly sceptical view of the EFD in U.S. antitrust law in general. Although the EFD was imported to EU competition law from the U.S. – its conceptual basis is generally traced back to the U.S. Supreme Court's decision *United States v. Terminal Railroad Association*[107] – the EFD has never been formally recognised in the U.S. Supreme Court's Section 2 Sherman Act jurisprudence. In its *Trinko* decision of 2004,[108] the U.S. Supreme Court has expressed a highly reticent attitude.[109]

However, both the 2019 Stigler Report and the 2020 Majority Staff House Report, issued by the Subcommittee on Antitrust, Commercial and Administrative Law of the Committee on the Judiciary of the U.S. House of Representatives, have recommended revitalizing the EFD. However, these proposals are not primarily linked to possible data access obligations, but rather to an obligation of the major digital platforms to grant access to the platform: the reports find that in several instances the major digital platforms threaten to delist platform users as a leverage to extract greater value or more data. Against this background, the House Report suggests overriding judicial decisions "that have treated unfavourably essential facilities- and refusal to deal-based theories of harm"[110] – in particular *Trinko* and *LinkLine*.[111] Because of their market power, such a platform's threat to deny businesses access to the platform "is the equivalent of depriving a market participant of an essential input". The central role of digital platforms as distribution channel would suggest that the benefits of antitrust intervention might be greater than previously appreciated. Depending on the circumstances, a revived EFD might also justify the imposition of data access obligations. Yet, the Stigler Report acknowledges the difficulty to determine the appropriate terms of data access or trade. Nonetheless, where this

[107] United States v. Terminal R.R. Ass'n, 224 U.S. 383 (1912).

[108] Cf Commc'ns Inc. v. Law Offices of Curtis v. Trinko, LLP, 540 U.S. 398 (2004); Pacific Bell Telephone Co. v. LinkLine Commc'ns, Inc., 555 U.S. 438 (2009).

[109] For a more complete discussion see Mestmäcker/Schweitzer, Europäisches Wettbewerbsrecht, 3rd ed. 2014, § 19 paras. 64 et seq.

[110] Subcommittee on Antitrust, Commercial and Administrative Law of the Committee on the Judiciary, Majority Staff Report and Recommendations (2020), 20 et seq., 397 et seq.

[111] Verizon Commc'ns Inc. v. Law Offices of Curtis v. Trinko, LLP, 540 U.S. 398 (2004); Pacific Bell Telephone Co. v. LinkLine Commc'ns, Inc., 555 U.S. 438 (2009).

determination is left to the dominant platforms, they retain the opportunity to raise rivals' costs and reinforce the platform's dominant position.[112]

While the proposal to revive the EFD with regard to platforms has received some support, and some have argued that it might justify data access obligations in particular,[113] the overwhelming reaction has been sceptical.[114] The House 'Minority Report', authored by Ken Buck, for example, took a cautious stance toward "handing additional regulatory authority to agencies in an attempt to micromanage platforms' access rule".[115] Along similar lines, academic commentators have argued that a duty to provide access to an essential facility would weaken firms' and rivals' incentives to invest and innovate.[116] Courts would have to monitor pricing and terms and conditions – tasks for which they are not well-equipped: what and how much data should be shared? With whom and at what price? How should the data be organised? Who is responsible for the costs? In addition, data sharing could lead to the revelation of competitively sensitive information. Other commentators have claimed that data sharing obligations might be unconstitutional takings of property.[117]

Instead of reviving the EFD, commentators propose to explore different paths: for example, the broader 'refusal to deal' doctrine could be extended to cases in which dominant internet companies prohibit scraping of public data on their platform and show an intent to

---

[112] Stigler Committee on Digital Platforms, Final Report (2019), 96 et seq.

[113] As early as 2014, Abrahamson argued that the classic criticism of the EFD (see above) carries less weight when it comes to data that is essential to competition and that the same elements should apply, i.e. (i) the monopolist must control and deny access to the data, (2) competition must fail without access to the data, (3) the plaintiff must lack means to duplicate the data, (4) the monopolist must be able to share the data, and (5) the essential facility plaintiff must demonstrate the monopolist's power in the market – see Zachary Abrahamson, *Essential Data*, 124 Yale L.J. 867, 869 et seq. (2014). See also Nikolas Guggenberger, *Essential Platforms*, 24 Stan Tech L Rev 237, 305 et seq. (2021) who wants to 'revive, renew and expand' the EFD with a two-tier approach inspired by IP policy and European competition law: At a first stage, regulators and courts must bar discrimination and self-preferencing and create access rights for third parties, and at a second stage, after an amortization period, enforcers must upend platform monopolies entirely by mandating interoperability.

[114] Jon M. Yun, *The Role of Big Data in Antitrust*, *in* GAI Report on the Digital Economy 242 (Joshua D. Wright & Douglas H. Ginsburg eds., 2020).

[115] Ken Buck, *The Third Way* (Oct. 6, 2020) 12 et seq., https://buck.house.gov/sites/buck.house.gov/files/wysiwyg_uploaded/Buck%20Report.pdf (last visited 4.7.2022).

[116] Michael L. Katz, *Mulisided Platforms, Big Data, and a Little Antitrust Policy*, 54 Rev. Ind. Organ. 695, 699 et seq. (2019); Keith N. Hylton, *Digital Platforms and Antitrust*, Law, 98 Neb. L. Rev. 272, 286 (2019); Makan Delharim, Speech at University of Haifa (Oct. 17, 2018) (transcript available https://www.justice.gov/opa/speech/assistant-attorney-general-makan-delrahim-delivers-remarks-university-haifa-israel (last visited 4.7.2022)).

[117] FTC Commissioner Wilson has argued that the application of the EFD constitutes a 'taking' under the Fifth Amendment to the U.S. Constitution, which provides that private property shall not be taken for public use without just compensation – see Christine S. Wilson, Remarks for the U.S. Chamber of Commerce Antitrust Webinar Series: Focus on Conduct (May 6, 2021) 4 et seq. (transcript available https://www.ftc.gov/system/files/documents/public_statements/1589671/chamber_of_commerce_wilson_keynote_final_1.pdf (last visited 4.7.2022)).

monopolise.[118] The *hiQ Labs v LinkedIn* case,[119] in which LinkedIn prevented HiQ Labs to gather and analyse data from public profiles by implementing IP blocks and sending a cease and desist letter, provides a practical example. An effects balancing test could be applied to determine whether a scraping prohibition might lead to foreclosure.[120] Katz has proposed that mandatory sharing may be appropriate if there is some sort of data pooling across platforms while there is no substitute for access to this data collection. In such a setting, the terms of sharing have already been agreed upon by the parties to the pool, and members are already engaging in concerted practice.[121]

b) Data portability, interoperability and standardisation

In the EU, data portability has originally been discussed in the context of privacy laws, but is increasingly considered as a competition policy tool.[122] However, commentators point to the significant practical challenges of ordering data portability within the normal antitrust framework.[123] In a jurisdiction that focuses on private enforcement and that, simultaneously, is very mindful of the institutional limitations of courts when ordering and enforcing quasi-regulatory behavioural obligations, the fact that firms subject to a portability obligation may need to establish new provisioning systems under the supervision of courts is pointed out as a significant hurdle. In addition, the compatibility of data structures would need to be ensured – either through conversion or through standardisation.

The House Report has therefore recommended to consider data portability as a self-standing complement to a vigorous antitrust enforcement that would reduce switching costs for consumers and lower barriers to entry for competitors.[124]

---

[118] Ionnis Drivas, *Liability for Data Scraping Prohibitions under the Refusal to Deal Doctrine: An Incremental Step toward More Robust Sherman Act Enforcement*, 86 U. Chi. L. Rev. 1901 (2019).

[119] hiQ Labs, Inc. v. LinkedIn Corp., 273 F Supp 3d 1099 (ND Cal 2017); confirmed by hiQ Labs, Inc v. LinkedIn Corp, 2019 WL 4251889 (9th Cir). *Authenticom v CDK* provides another example: Authenticom scraped and analyzed public data from car dealers' websites operated by CDK. Initially open to public, CDK decided to close its website, which effectively prevented Authenticom from data gathering and enabled CDK to demand higher prices for its own data analytics services that competed with Authenticom prior to closing the website – see Authenticom, Inc. v CDK Global, LLC, 874 F.3d 1019 (2017).

[120] Drivas, *op. cit.*, 1930 et seq.

[121] Katz, *op. cit.* , 699 et seq. citing emetriq as an example, an initiative of German publishers to pool advertising data, https://www.emetriq.com (last visited 4.7.2022).

[122] See for example Peter Swire, *The Portability and Other Required Transfers Impact Assessment (PORT-IA): Assessing Competition, Privacy, Cybersecurity, and Other Considerations* (Sept. 8, 2020), https://ssrn.com/abstract=3689171 (last visited 4.7.2022), suggesting PORT-IA (Portability and Other Required Transfers Impact Assessment) framework providing structured questions to assess whether mandatory data sharing is likely to be net beneficial. Some point to the reduction of incentives to innovate and privacy or cybersecurity risks, however – see Daniel L. Rubinfeld, *Data Portability*, 2(2) CPI Antitrust Chronicle 16, 17-20 (Nov-2020). See also Peter Swire & John Snyder, *Using the Portability and Other Required Transfers Impact Assessment ("PORT-IA") in Antitrust Law*, 2(2) CPI Antitrust Chronicle 23, 27 (Nov-2020).

[123] Christopher S. Yoo, *Unpacking Data Portability*, 2(2) CPI Antitrust Chronicle 30 (Nov-2020).

[124] Subcommittee on Antitrust, Commercial and Administrative Law of the Committee on the Judiciary, Majority Staff Report and Recommendations (2020), 384 ('Subcommittee staff recommends that Congress consider data

Similarly, the Stigler Report proposed a data porting regulation that would, among other things, give consumers the right to receive their data in a standardised format.[125] A Digital Authority (see below) should be tasked with identifying industries where porting is likely to aid the competitive process and with proposing standards for exchanging data – considering industry desires. In addition, it may be necessary to establish a right to transfer data to a new entrant by authorising it to be transferred directly from the former service provider. In this case, the Digital Authority would need to authorise the entrant to offer his facility to consumers and establish regulation to require the incumbent to transfer the consumer's data.

The recommendations in the House Report and in the Stigler Report were taken up in the proposed ACCESS Act (see below). However, the Senate Judiciary Committee has not voted to advance the ACCESS Act. There is, therefore, no realistic chance for the ACCESS Act or similar legislation to be passed any time soon.

c) Mandating interoperability?

Moving beyond data portability, the case for or against interoperability has become a much-debated issue in the U.S. Mandatory horizontal platform interoperability has been proposed as 'the super tool' of digital platform governance.[126] While this proposal primarily relates to the interoperability of platforms, not of data, data interoperability may then be a necessary annex (aa). Sometimes, data interoperability is also discussed as a self-standing antitrust remedy (bb).

aa) Horizontal platform interoperability

The focus of the interoperability debate has been on horizontal platform interoperability, as prominently advocated by Fiona Scott Morton.[127] Her views are reflected in both the Stigler Report and the House Report. According to both reports, platform interoperability should be considered as a remedy wherever a dominant firm has exploited network effects in an anti-competitive manner – e.g. through 'platform annexation'[128] or anti-competitive serial acquisition strategies. The strength of this remedy is that, with platform interoperability,

---

interoperability and portability to encourage competition by lowering entry barriers for competitors and switching costs for consumers. These reforms would complement vigorous antitrust enforcement by spurring competitive entry') and 386.

[125] Stigler Committee on Digital Platforms, Final Report (2019), 18, 52, 109 et seq.

[126] For the term Fiona M. Scott Morton et al., *Equitable Interoperability: The 'Super Tool' of Digital Platform Governance* (July 13, 2021), https://ssrn.com/abstract=3923602 (last visited 4.7.2022).

[127] Ibid.; Fiona M. Scott Morton & Michael Kades, *Interoperability as a Competition Remedy for Digital Networks* (March 19, 2021), https://ssrn.com/abstract=3808372 (last visited 4.7.2022); Fiona M. Scott Morton & Susan Athey, *Platform Annexation* (Feb. 16, 2021), https://ssrn.com/abstract=3786434 (last visited 4.7.2022); Fiona M. Scott Morton & David C. Dinielli, *Roadmap for an Antitrust Case Against Facebook* (June 2020), https://www.omidyar.com/wp-content/uploads/2020/06/Roadmap-for-an-Antitrust-Case-Against-Facebook.pdf (last visited 4.7.2022), at 2, 17.

[128] See Scott Morton & Athey, *op. cit.*, 1: '[…] whereby a platform annexes mulit-homing tools or other adjacent products in a way that interferes with multi-homing by users, lessening competition.'

positive network effects would not only benefit one platform but the market as a whole.[129] According to Scott Morton, adjudication alone is ill-suited to implement an interoperability remedy, however. But the FTC could issue a default order on interoperability, which could be modified by the adjudicator to suit the situation in the particular case. Mandatory platform interoperability would have some implications for data portability/data interoperability. For example, it would involve not only open but also common Application Program Interfaces[130] and arguably require the adoption of open standards for data and data exchange, to be overseen by a Digital Authority.[131]

While the possibility to mandate platform interoperability receives much attention, some commentators have argued that – depending on the specific circumstances and the precise design of the mandate – interoperability may have ambivalent effects on competition: it may reduce the room for differentiation as well as the room for innovation – and thereby the room for competition between digital platforms.[132] Interoperability may also weaken platforms' incentives to compete through innovation and pricing, since firms no longer compete for positive network externalities.[133] In addition, it is contended that mandating interoperability may entrench incumbents by constraining new functionalities and thereby discouraging 'Schumpeterian competition' for disruptive innovations.[134] Others point to possible frictions with intellectual property rights, privacy and other doctrines, which have to be considered when mandating interoperability.[135] Given these potentially negative side-effects of interoperability, any such regime would need to be carefully designed, and its implementation would require a potentially resource-intense ongoing supervision.

This notwithstanding, the idea of mandating horizontal platform interoperability was taken up in the proposed ACCESS Act (see below). As the Senate Judiciary Committee has not voted to advance the ACCESS Act, this proposition is no longer on the immediate legislative agenda, however.

bb) Data interoperability

Sometimes – but rarely – data interoperability is discussed as such. Herbert Hovenkamp has discussed the advantages that a 'data pooling' requirement may have as an alternative to

[129] See Subcommittee on Antitrust, Commercial and Administrative Law of the Committee on the Judiciary, Majority Staff Report and Recommendations (2020), 385 et seq.: An interoperability requirement would allow competitors to connect to the dominant firm's services and 'break the power of network effects' by allowing newcomers 'to rely on existing network effects at the level of the market, not the level of the company'.

[130] Stigler Committee on Digital Platforms, Final Report (2019), 16.

[131] Stigler Committee on Digital Platforms, Final Report (2019), 113.

[132] Jay Ezrielev & Genaro Marquez, *Interoperability: The Wrong Prescription for Platform Competition*, 3(1) CPI Antitrust Chronicle 8, 10 et seq. (June-2021).

[133] Id., 11 et seq.

[134] Id., 12.

[135] Laura Alexander & Randy Stutz, *Interoperability in Antitrust Law & Competition Policy*, 3(1) CPI Antitrust Chronicle 31 (June-2021).

structural remedies in both Section 1 and 2 Sherman Act cases – in particular, where a dominant platform exerts market power over business partners through practices such as exclusive dealing or MFN agreements.[136] Such a 'data pooling' remedy could "weaken dominant positions while actually improving performance" by increasing the installed base of a platform. Simultaneously, it would not come with the cost increases and reduction of quality that an asset divestment remedy might have.[137] When Hovenkamp speaks of the 'pooling' of data[138] in this context, it means "something similar [to interoperability], although with greater emphasis on the sharing of information […], which may consist of little more than compelled pooling of data in a common format".[139] For example, a pooling remedy for search engines would entail placing search data into a common database equally accessible by all participating search firms to improve search results and thus consumer welfare.[140]

d) Data standardisation

One way to promote data portability and interoperability is through data standardisation, which is the process of converting data into a common format to enable data users to process and analyse it. Data standards may relate, for example, to "the attributes of the data to be collected; to the terminology, structure, and organisation of the dataset; to aspects of data storage (location, etc.); or to its use (including protocols for data portability)".[141] Most commonly used are Application Programming Interfaces (APIs), which are computer protocols defining how software components communicate.

Data standardisation can lead to smoother data flows by removing technical obstacles to data portability and interoperability.[142] Furthermore, data standardisation can potentially incentivise data collection, organisation, and storage, generating ever-increasing amounts of accessible data, leading to the promotion of a competitive and distributed data collection ecosystem.[143] Nevertheless, data standardisation may also come with some negative externalities, such as privacy and cybersecurity risks or disincentives for investment and innovation in the case of a lock-in into an inefficient or inferior standard.[144]

It is generally acknowledged that the development of standards can frequently be left to the market and private standard-setting organisations (SSOs). With regard to data, private collaboration projects such as schema.org or Google Takeout play a significant role.[145]

---

[136] Herbert Hovenkamp, *Antitrust and Platform Monopoly*, 130 Yale L. J. 1952, 2020 et seq. (2021).

[137] Id., 2032.

[138] Id., 2020 et seq., 2032-2038.

[139] Id., 2032 et seq.

[140] Id., 2035.

[141] Michal S. Gal & Daniel L. Rubinfeld, *Data Standardization*, 94 N.Y.U. Law Rev. 737, 749 (2019).

[142] Id., 747 et seq.: metadata uncertainties, obstacles to data transformation, missing data.

[143] Id., 754 et seq., 757 et seq.

[144] Id., 756 et seq.

[145] Rubinfeld, *op. cit.*, 18.

However, it is also recognised that market failures can occur which may necessitate direct or indirect government intervention and potentially facilitation of more open, transparent and collaborative standard-setting.[146] In particular, market failures may exist when (i) large incumbents, who enjoy a data-based comparative advantage and have implemented company-specific standards, have little incentives to engage in collaborative standardisation, but rather engage in anti-competitive behaviour; (ii) markets are fragmented to a degree that no single standard gains critical support and collective action and coordination problems arise;[147] (iii) spill-over effects on data subjects are disregarded and the standards achieved do not reflect the social optimum.

Both the House Report and the Stigler Report do not take a stance on the issue of data standardisation. However, while the House Report is silent on standardisation in general, the Stigler Report recommends giving the Digital Authority the power to impose open (platform) interoperability standards (see above).

e) Institutional aspects

Even those voices in the U.S. debate that favour a more pro-active stance of the state in setting the rules for the emerging data economy tend to be sceptical whether the predominantly adjudicative and frequently private enforcement of U.S. antitrust law will suffice. The Stigler Report has therefore recommended the establishment of a sectoral regulator, a 'Digital Authority', and presents a 'menu' of broadly applicable rules and regulations that should apply to firms with bottleneck power. Such a regulatory scheme could include a 'Data Law' including rules on data portability to enable user mobility by reducing switching costs and facilitate entry, which would be accompanied by the right of users to have their data sent directly to a new service provider authorised by them. This seems to broadly align with the data portability obligations of 'gatekeepers' in the DMA (Article 6 No. 9 DMA). The report suggests that the Digital Authority could propose portability standards, but that they should remain open to options preferred by the industry and to frequently update the standard to reflect new technological developments in the industry.[148] Furthermore, the Digital Authority should pre-emptively prevent "the consolidation of control over users' identities". Digital identities incorporate data on age, sex, (email) address etc. to help companies to identify, tag and track users. The next major shift in digital competition is expected to be "the quest to control the identification market".[149] Accordingly, the Digital Authority should promote open standards in this regard so that new entrants can easily offer their own identity product – the Estonian 'e-Estonia' initiative, which gives citizens a unique digital identifier, could serve as a blueprint.[150] This would allow individuals to 'port their identity to the platforms and providers they wish to

[146] Gal & Rubinfeld, *op. cit.*, 762 et seq.

[147] Carl Shapiro & Hal R.Varian, *The Art of Standards Wars*, 41 California Management Review 8 (1999).

[148] This argument is brought forward by Apple, for example, against common standards for mobile phone chargers.

[149] Stigler Committee on Digital Platforms, Final Report (2019), 54.

[150] With further examples Id., 110 et seq.

use' and thus promote entry of new services and mitigate switching costs of established platforms.

Furthermore, the Digital Authority should promote entry into 'markets of interest' by facilitating the development of open interoperability standards to be used by all competitors.[151] In deciding where such interoperability standards are needed, the importance of the market and the potential harm from market power are of the essence. As a candidate for issuing such interoperability standards, the consumer IoT sector is mentioned, where "devices in the home might be required to adhere to an open standard so that any platform could connect with any device."[152] This suggests that the focus is on vertical interoperability in this context. The authors recognise a risk that such interoperability standards might slow down innovation. Simultaneously, they expect that open standards will "drastically reduce lock-in and market power, leading to greater incentive to innovate on the service itself."[153]

As of now, there are no concrete legislative plans to establish a Digital Authority, however. Rather, it is the FTC that remains competent to regulate the digital sector. The scope of the FTC's rule-making authority under Section 5 FTC Act is controversial.[154]

4. Legislative initiatives regarding data-related gatekeeper regulation

Following up on the aforementioned reports and an intense public debate, six bills have been introduced with bipartisan support in the House of Representatives of U.S. Congress[155] in June and August 2021 that are meant to cover the five largest digital platform operators[156] and to revive competition in the markets dominated by them. Three of these bills address data access, namely the American Choice and Innovation Online (ACIO) Act, the Augmenting Compatibility and Competition by Enabling Service Switching (ACCESS) Act, and the Open

---

[151] Id., 113.

[152] Ibid.

[153] Ibid.

[154] See for example Rohit Chopra & Lina M. Khan, *The Case for "Unfair Methods of Competition" Rulemaking*, 87 Univ Chic Law Rev 357 (2020); Thomas W. Merrill & Kathryn Tongue Watts, *Agency Rules with the Force of Law: The Original Convention*, 116 Harv. L. Rev. 46 (2002); Jay B. Sykes, *The FTC's Competition Rulemaking Authority*, Congressional Research Service (Aug. 12, 2021), https://crsreports.congress.gov/product/pdf/LSB/LSB10635 (last visited 4.7.2022); Tim Wu, *Antitrust via Rulemaking: Competition Catalysts*, 16 Colo. Tech. L.J. 33 (2016).

[155] American Choice and Innovation Online Act, H.R.3816; Platform Competition and Opportunity Act, H.R.3826; Ending Platform Monopolies Act, H.R.3825; Augmenting Compatibility and Competition by Enabling Service Switching (ACCESS) Act, H.R.3849; Merger Filing Fee Modernization Act, H.R.3843. See also the Open App Markets Act, H.R.5017, introduced in August 2021.

[156] To determine whether a platform operator is 'covered' by the Acts, quantitative criteria are applied at the firm level and qualitive criteria are applied at the platform level: According to Section 2(g)(4) ACIO Act a threshold of 500 million U.S.-based monthly active users or 100,000 U.S.-based monthly active business users and 600 billion U.S. Dollars in net annual sales or market capitalization must be met (similar to Article 3 DMA). Based on sales and market capitalization, this only covers the five largest platforms. Section 2(g)(10) ACIO Act defines which platform services are covered. This approach is somewhat similar to Article 2(2) DMA. Important differences remain: advertising services, number-independent communications services, OS or cloud computing services are not explicitly included; yet categories of the U.S. approach appear to be more expansive.

App Markets Act. Of these three bills, the Senate Judiciary Committee has voted to advance the ACIO Act – which focuses on non-discrimination rules, including a prohibition of self-preferencing, and features some data use restrictions and data access rules – in January 2022, and the Open App Markets Act – which stipulates certain rules on data usage for app store operators – in February 2022.[157]

The proposed ACCESS Act would have introduced rules on data portability and interoperability as well as on the standards. However, the Senate Judiciary Committee has not voted to advance the ACCESS Act.

a) Data use restrictions

Both the ACIO Act and the Open App Markets Act propose to constrain powerful platforms in the use of the data generated by platform business users.

Section 2(b)(3) ACIO Act would make it unlawful for a covered platform operator to "use non-public data obtained from or generated on the platform by the activities of a business user or its customers that is generated through an interaction with the business user's products or services to offer or support the offering of the covered platform operator's own products or services". Similarly, Article 3(c) of the Open App Markets Act prohibits any person that owns or controls an App Store for which users in the United States exceed 50,000,000 to "use non-public business information derived from a third-party App for the purpose of competing with that App". These data use restrictions – which are similar to Article 6 No. 2 DMA – are addressed to 'dual role' platforms that act as platform operators but compete on the platform at the same time. By prohibiting the use of the data generated by competing businesses on the platform for advancing their own business activities on the platform, they strive to outlaw an 'unfair' appropriation of business opportunities based on privileged data access and to protect a level playing field for competition on that platform.

Neither the ACIO Act nor the Open App Markets Act propose to impose constraints upon the combination of data sourced from different services, as Article 5 No. 2 DMA and § 19a(2), 1st sentence, No 4 lit. a GWB do.

b) Data access rules

According to Section 2(b)(4) of the proposed ACIO Act, a platform operator covered by this act shall not "restrict or impede a business user from accessing data generated on the platform by the activities of the business user or its customers through an interaction with the business user's products or services, such as contractual or technical restrictions that prevent the

[157] See American Innovation and Choice Online Act, S.2992, Open App Markets Act, S.2710. In addition two of the other four bills were voted to be advanced, namely the Platform Competition and Opportunity Act of 2021, S.3197; and the Merger Filing Fee Modernization Act of 2021, S.228.

portability of such data by the business user to other systems or applications". This provision, which is reminiscent of Article 6 No. 9 and No. 10 DMA, would recognise a right of business users to access and port data generated by their platform activity and offer. No further-reaching right to access to data is recognised.[158]

c) Rules on interoperability

aa) Vertical interoperability

The proposed AICO Act also mirrors some of the DMA's rules on vertical interoperability:

Section 2(b)(1) of the proposed ACIO Act would prohibit to "restrict or impede the capacity of a business user to access or interoperate with the same platform, operating system, hardware and software features that are available to the covered platform operator's own products, services, or lines of business" – and would thereby be comparable to Article 6 No. 7 DMA. It would outlaw a covered dual role platform's self-preferencing when it comes to access to and the vertical interoperability of its own offers with the platform and ancillary services. However, Section 2(b)(1) does not deal with data interoperability as such.

Furthermore, Section 2(b)(4) ACIO Act would make it unlawful to 'restrict or impede a business user, or a business user's customers or users, from interoperating or connecting to any product or service' – and is therefore similar to Article 6 No. 7 DMA. Again, this provision does not deal with data interoperability as such, although it may implicate some degree of data interoperability.

bb) Horizontal interoperability

Further-reaching rules on the horizontal interoperability obligations to be imposed on the largest digital platforms as advocated by Fiona Scott Morton were promoted in the proposed ACCESS Act. In particular, Section 4(a) of the ACCESS Act reads: "A covered platform shall maintain a set of transparent, third-party-accessible interfaces (including application programming interfaces) to facilitate and maintain interoperability with a competing business or a potential competing business that complies with the standards issued pursuant to Section 6(c)". According to Section 6(c)(1) of the ACCESS Act, the FTC should issue standards of interoperability specific to each covered platform with the goal to encourage entry by reducing or eliminating the network effects that limit competition with the covered platform. This would ensure that competing businesses or a potential competing business could interconnect with the covered platform on fair and non-discriminatory terms, and to protect data security and privacy.

---

[158] In particular, there is no equivalent to Article 6 No. 11 DMA, according to which a gatekeeper shall "provide to any third party undertaking providing online search engines, at their request, with access on fair, reasonable and non-discriminatory terms to ranking, query, click and view data in relation to free and paid search generated by end users on its online search engines. Any such query, click and view data that constitutes personal data shall be anonymised."

The proposed ACCESS Act was not voted to go forward, however.

d) Data portability

Apart from rules on horizontal platform interoperability, the proposed ACCESS Act also featured data portability obligations: according to its Section 3(a), covered platforms should "maintain a set of transparent, third-party-accessible interfaces (including application programming interfaces) to enable the secure transfer of data to a user, or with the affirmative consent of a user, to a business user at the direction of a user, in a structured, commonly used, and machine-readable format that complies with the standards issued pursuant to Section 6(c)." A data portability right for platform users would facilitate switching or multi-homing or allow third parties to offer data-based, personalised complementary services to such users. Contrary to its European counterpart in Article 6 No. 9 DMA, Section 3(a) did not contain a requirement that the data feed be real-time and continuous. Despite this significantly more cautious approach, the proposal is no longer scheduled to go forward. What remains is the proposal for introducing a data portability right for business users (see above).

e) Overall assessment

While the legislative agenda to create a special legal framework for the most powerful digital platforms has started out ambitiously, it has been curtailed significantly in the meantime. This is also true with a view to data-related rules of conduct. Even if the ACIO Act and the Open App Markets Act were to be passed, the covered platforms would remain free to combine datasets from different sources. Moreover, data access and data portability would be ensured for business users only, but not for other platform users. Overall, the U.S. debate on the cross-market use of data within the framework of large and powerful data-driven ecosystems is less pronounced than in the EU. To the extent that new rules on data are discussed, the debate is, however, driven by antitrust concerns. The European strive for pro-actively developing rules and institutions for data-sharing is largely absent in the U.S. With regard to the establishment of a well-functioning framework for the emerging data economy, the U.S. relies much more on a market-driven 'bottom up' approach.

D. Data Economy and data sharing: basic concepts and empirical analysis

As shown in part C, the EU and the U.S. pursue very different policies when it comes to promoting the evolution and growth of the data economy. Whereas the U.S. appears to follow a market based, bottom-up approach and appears to be relatively cautious, if not reluctant, to intervene, the EU pursues a much more pro-active policy.

In light of this divergence, we start out with an inquiry into different theories of how the role of the state should be conceptualised in times of fundamental economic transformation (I.). In a second part (II.), we then provide an overview of the state of data cooperations and data sharing in Europe. In doing so, we start by setting out the taxonomy of data, data access and data sharing that we will use throughout the rest of our study. We then continue by summarizing various recent empirical surveys on data markets and data sharing in Europe and Germany, tentatively matching them with the insights we gained from some selected interviews with relevant market actors (III.). On this basis, we explain what we find to be an appropriate role for the European and German legislator in promoting the evolution of the data economy (IV.).

I. The role of the state in times of fundamental economic transformation: market failures, system failures and the transformational role of the state

1. Addressing market failure: traditional market failure analysis

Exploring the need for market intervention from a law and economics perspective traditionally amounts to thorough analysis of possible market failures and to an inquiry whether these can be best fixed by the market itself or are rather in need of public policy intervention. Looking at data-driven markets from this angle, it turns out that they may be affected by all the well-established categories of market failures, namely information asymmetries, market power, externalities and public goods.[159]

As with other intangible goods, data is characterised by a high level of asymmetric information. The data generator will typically have a much better knowledge about the completeness and quality of the data compared to the data user. Consequently, the willingness to pay for the data may be much lower than the price asked for. GSMA refers to data as an ‘experience good’.[160] However, data come with another important feature: the value of data, such as with other intangibles, is not ‘intrinsic’ to the data but varies depending on the uses to which they are put. What ultimately matters is what kind of information can be gleaned from them. It follows that context, format (e.g. whether it is structured or not) and timeliness may matter . For many

[159] Pindyck/Rubinfeld, Microeconomics, 8th ed. 2013, p. 593 et seq.

[160] GSMA, The Data Value Chain, 2018, p. 11, https://www.gsma.com/publicpolicy/wp-content/uploads/2018/06/GSMA_Data_Value_Chain_June_2018.pdf (last visited 4.7.2022).

sectors and uses, data is most useful and valuable when provided in real-time.[161] When it comes to 'big data', the factors that affect the value of data are usefully summarised as the four Vs: Volume, Velocity, Variety and Veracity.[162] Whether data-related information asymmetries or the preconditions for drawing value from data justify public intervention cannot be answered in the abstract: it must be considered in a context-specific manner.

The sharing of data can generate negative externalities, for example privacy and security risks. A number of rules and regulations strive to address these risks in the EU. With regard to the protection of personal data, the GDPR plays a central role. It may however produce market failures of its own.[163]

No less important, the sharing of data can generate positive externalities. Data is non-rivalrous in its use:[164] the use of data by one party does not impede it being used by others. This means that data can be 'used by more than one person (or algorithm) at a time and it is not consumed in the process'.[165] The OECD depicts how data can be re-used for an indefinite number of purposes and by an indefinite number of users.[166] The more data is shared and used, the more value can be derived from it. An important source of value creation is the combination of different datasets. A dataset may have relatively little value on its own, but the insights that can be gained from it, and hence the value, can significantly increase as it is combined with other data. Positive externalities can emerge as a result of 'transfer learning' where an algorithm trained on a high-quality dataset can then be used on another.[167] These positive externalities may not be taken into account by the data producers and holders, however. One may expect that third parties who may benefit from access to data will compensate the data producers or holders within the framework of contractual relationships. However, where these exchanges fail on a systemic basis, a tendency towards underinvestment into the production, but also sharing of data can result. We will turn to the debate on the contractual sharing of data and a possible need for property rights in data later (see below, part E(I)-(II)).

The market failure that has arguably been most intensely debated in the context of sharing of data is market power. Markets in which data are an important competitive input are frequently characterised by strong economies of scale and scope. This is true, in particular, for data that are generated by the use of digital platforms. In these settings, the network effects that characterise platforms translate into economies of scale in the collection of data, which may

[161] A case in point is financial trading where transactions are conducted within milliseconds, reacting to a multitude of data, and where the more dated the data becomes the less useful and valuable it is.

[162] See Gal/Rubinfeld N.Y.U. Law Rev. 2019, 737.

[163] See Gal/Aviv J. Compet. Law Econ. 2020, 349.

[164] GSMA, The Data Value Chain, 2018; Martens et al. JRC121336 (2020).

[165] GSMA, The Data Value Chain, 2018, p. 9.

[166] OECD, Enhancing Access to and Sharing of Data: Reconciling Risks and Benefits for Data Re-use across Societies, 2019.

[167] Gal/Rubinfeld N.Y.U. Law Rev. 2019, 737 (744).

help to further reinforce the competitive position of the platform.[168] However, economies of scale and scope may also exist in other settings, because setting up databases and the necessary infrastructure require significant fixed costs, whereas adding future data and even data sources does not generate significant further costs. In particular, the development of algorithms as a basis of Artificial Intelligence (AI) using data for training purposes needs investments in software development. The efficiency of the algorithms then continuously improves the more training data is available, at near zero marginal cost. Furthermore, the economic value creation of the digital asset is further accelerated by digital asset reusability. In summary, the economics of AI can lead to market dominance.[169] The fact that only a few companies invest massively in the development of data-driven AI tends to further increase concentration and may eventually lead to monopolization of the supply side.

However, data can also come with important economies of scope: the combination of different datasets may significantly increase the value of the data. The fact that data frequently is a multi-purpose input that can be a competitively important asset in different markets may enable digital gatekeeper platforms that control large data troves to quickly enter into new markets and expand by way of data-driven platform envelopment strategies.[170] Likewise, data-driven lock-ins in aftermarket settings may raise market power (or cross-market power) concerns. Therefore, there is a special role for competition law and competition law-based regulation in data-driven markets (for further discussion see: part E(III),(V)).

2. Innovation system failures

Where a traditional market failure analysis will see a cause for public intervention mainly when it comes to correcting market power or cross-market power, it may tend to overlook some of the factors that are needed to successfully innovate. The transformative power of the data economy may require us to focus on how the EU and Germany can enable and promote innovation in data-driven markets such as to make them deploy their full potential, and therefore to use a broader analytical framework to explore possible needs for action.[171] In the 1980s already, innovation economists developed the so-called innovation system approach[172] to analyse market failures related to research and development, but also innovation more broadly. Possibly innovation system failures to be considered in this line of thinking include infrastructural failures, institutional failures, interaction failures and capability and learning failures.

[168] Prüfer/Schottmüller J. Ind. Econ. 2021, 967.

[169] Wagner Evolut Inst Econ Rev 2020**,** 111.

[170] Condorelli/Padilla J. Compet. Law Econ. 2020, 143.

[171] For an analysis of system and transformational failures related to 5G roll-out see Blind/Niebel Technol. Forecast. Soc. Change 2022, 121673.

[172] Freeman, Technology Policy and Economic Performance: Lessons from Japan, 1987; Lundvall, National Systems of Innovation: Towards a Theory of Innovation and Interactive Learning, 1992.

Infrastructural failures occur when physical or other infrastructures are required for future innovation activities. GAIA-X is supposed to address this lack of infrastructure for data integration and sharing in the EU. But the European science and technology infrastructure remains weak because of the lack of educated and skilled personnel, in particular in the field of data science.

In contrast to these infrastructural failures, institutional failures can be addressed by expanding or changing the regulatory framework conditions. 'Hard' institutional failures are associated with insufficient formal institutions, such as gaps in intellectual property rights or data regulations. 'Soft' institutional failures are failures in informal institutions such as social and cultural norms, which can only be indirectly addressed by regulations. They can, however, be rectified by the establishment of voluntary standards.

Interaction failures are a subgroup of system failures that refers to the relationships between the different actors of innovation systems. They are divided into strong and weak network failures. In the case of strong network failures, actors build too strong ties with each other while pulling into wrong directions. For example, firms might be handicapped by a blindness to developments taking place outside their closed network. Weak network failures occur if the actors in the innovation system do not sufficiently learn from one another's knowledge and experience. Others speak of the 'non-complementarity' of actors. Due to a lack of ties, it is difficult to develop a common vision and find compromises in case of conflicting interests. In the case of data sharing, this may partly explain the (non-)interaction between potential data providers and potential data recipients. In such a case, the state may try to promote data sharing – either by establishing attractive incentive structures or by mandating data sharing. However, obligations to share data that are opposed by the vast majority of companies might trigger counter strategies, eventually leading to an inefficient outcome.

Finally, capability and learning failures limit both learning and eventually innovation within innovation systems. Such innovation systems might not be open enough to new scientific and technological developments, and they may lack the ability to switch from an established to new technological trajectories, such as for example, the use of AI in analysing data.

3. Transformational system failures

Weber and Rohracher (2012)[173] have gone one step further and have considered possible failures of transformative change (so-called transformational system failures), including, in particular, directionality failures, demand articulation failures, policy coordination failures and reflexivity failures. Given the extensive restructuring of business models, markets and ultimately economies that accompanies the shift towards a data economy, this approach may usefully systematise relevant preconditions for successful economic change that may justify some sort of state intervention.

[173] Weber/Rohracher Res. Policy 2012, 1037.

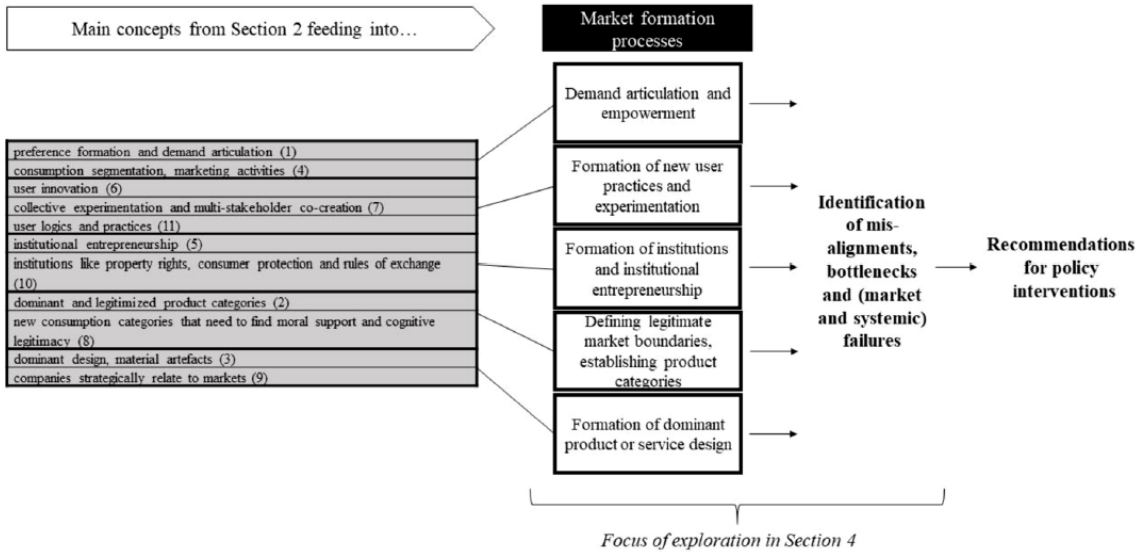
Directionality failures occur when there is no common vision of the transformation among the relevant actors. This may manifest itself through a lack of targeted funding, comprehensive projects and demonstrations, but also a lack of guidance from regulations and/or an undersupply of standards. Demand articulation failures take place when concrete demands from the relevant stakeholders or the economy and society as a whole are missing but would be needed for the formation of new markets. Policy coordination failures occur if there is no or only insufficient policy coordination across industries, but also among policy makers at the regional, national and supranational level and/or between the public sphere and private actors. The lack of coordination can pertain to, *inter alia*, technologies, standards or regulations. Finally, reflexivity failures, i.e. the inability to monitor, to anticipate and to involve actors in processes of self-governance, are very likely to occur in highly uncertain and long-term oriented transformations. To counteract such failures, experimentation, monitoring, learning and adaptation of policies and regulations is required.

Applied to the ongoing economic transformation towards a data economy, the literature on system failures and transformation failures can provide important guidance to policy makers. Due to their emerging character, data-driven markets are prone to both system and transformational failures. The literature usefully highlights the need to understand the demand of stakeholders and how they interact, including the constraints they encounter; the need for a precise analysis if – and if so what – types of rules, institutions and standards are needed when it comes to data sharing; the need for consistency of the legal framework – combined, however, with room for experimentation, regular monitoring and adaptation; and the need for coordination between different policy levels.

Recently, Boon, Edler and Robinson[174] have combined various strands of the literature and developed a conceptual framework meant to advise transformative innovation policy in reaction to fundamental and systemic socio-technical changes. They have identified the following market formation processes, which may take place simultaneously: demand articulation and empowerment; the formation of new user practices and experimentation; the formation of institutions and institutional entrepreneurship; the definition of legitimate market boundaries and establishment of product categories; and the formation of dominant product or service designs. Although the authors, highlight that the five processes do not follow a linear stage model, their cases reveal that the completion of certain processes have an influence on following processes.

[174] Boon/Edler/Robinson Environ. Innov. Soc. Transit. 2022, 152.

Fig. 1: Steps leading to the conceptualization of market formation processes to improve policy.



Source: Boon/Edler/Robinson Environ. Innov. Soc. Transit. 2022, 153.

We find that this framework may help to understand the formation of new, data-driven markets in the emerging data economy and the ways in which the state may be able to contribute to their evolution. The demand articulation links user or customer preferences to the opportunities generated by new technologies and their innovative applications, products or services. It reduces information asymmetries between the supply and the demand side. The supply side pushes marketing activities, the demand side by endorsing innovations based on the new technologies being close to their specific needs.

On the demand side, users and customers start to integrate innovation into their already established practices via experimentation, partly modifying it and even developing follow-up innovations themselves.

In the next phase, stakeholders react to the challenges of new markets by establishing rules and institutions allowing them to further evolve and work efficiently. Such rules and institutions may be developed bottom-up – e.g. by way of private standard-setting and self-regulation. Stakeholders can thus become institutional entrepreneurs, setting up new rules themselves to accommodate the characteristics of the innovative products and services. But they may also involve governmental regulation.

Markets evolve in parallel. The market boundaries, including product categories, are established by single suppliers or the whole supply side in order to align the new markets with the existing markets they already serve. Competitive relationships may shift accordingly.

The final stage of market formation is the formation of dominant designs,[175] mainly based on proprietary de facto standards, which may eventually have a strong influence on the development of markets. But complementary to these proprietary de facto standards, open standards agreed upon by the most relevant companies and further stakeholders, e.g. suppliers and customers, but also governmental representatives, can be also contribute to the formation of dominant designs. In the software area, for example, open source communities set standards, which are eventually as widely implemented as formal standards and can therefore be considered another form of dominant design.[176] Whereas proprietary de facto standards can be used by dominant market players to close interfaces and/or leverage market power, open standards not protected by intellectual proprietary rights or accessible via FRAND conditions may be more conducive to competition.

Regarding the role of the state, the analysis by Boon, Edler and Robinson contributes to the growing body of literature that argues that it is not only market failures in the 'classical' sense that can call for policy interventions, but already misalignments, bottlenecks and frictions in the market formation processes. More particularly, the authors argue that for grand transformations, public policy has to focus on creating and shaping new markets and not only of market fixing[177], and that public policy should start rather early with initiatives to shape new markets. In particular, policy makers should reduce uncertainty for all market actors and relevant stakeholders across all five stages of market formation by creating transparency, supporting directionality, fostering discourse and interaction among all stakeholders and providing regulatory frameworks. Those regulatory frameworks should be both flexible enough to be adjustable to unforeseen changes in the different processes and sufficiently stable for potentially interested producers and consumers.[178]

Given that there may be a role for public policy to play in promoting the up-take of the emerging data economy, we turn next to an analysis of the state of the data economy and data sharing in the EU and in Germany (II.) in order to better understand what type of intervention may be needed (IV.).

II. The state of the data economy in Europe

1. Evolution and growth of the data economy

The generation, collection and use of data has grown exponentially in the 21st century. Simultaneously, we have seen the emergence of entirely new business models. Data-driven business models have given rise to companies that now count as some of the largest in the

[175] Ibid.; Suarez/Utterback Strateg. Manag. J. 1995, 415. Later, Suarez et al. introduced dominant product categories that precede the emergence of dominant designs, Suarez/Grodal/Gotsopoulos Strateg. Manag. J. 2015, 437.

[176] Blind/Boehm JRC117836 (2019).

[177] Robinson/Mazzucato Res. Policy 2019, 936.

[178] Boon/Edler/Robinson Environ. Innov. Soc. Transit. 2022, 152.

world. Data has become central to the rise of new technological areas such as the Internet of Things (IoT) or Artificial Intelligence (AI) and has led to dramatic changes in most sectors including agriculture, mobility, health, energy to name just a few. Various indicators depict that from 2019 to 2025 as a baseline scenario the European data economy will further increase in value.[179] For example, whereas in 2019 data suppliers' revenue was 64 Billion EUR, by 2025 it is projected to be at the very least 99 Billion EUR. It is also interesting to compare the value of data markets[180] in different regions of the world: although the EU's data-related markets are more valuable than those in other countries and regions, they are still far smaller than the U.S. data markets.

The volume of data is expected to further increase in the future. In particular, industrial data will significantly increase. Simultaneously, data processing and data storage technologies continue to change – e.g. from IoT devices to edge computing. This is expected to lead to new opportunities for individuals, society, businesses and governments.[181]

2. The data value chain, actors in data-driven markets and taxonomies of data

In order to take advantage of the opportunities of the emerging data economy, an increase in data access and sharing is found to be of the essence. Before summarizing the relevant surveys on the extent to which data sharing currently takes place, we take a look at the structure of the data value chain, the different interests of different actors in data-driven markets, and the heterogeneity of data.

a) The data value chain and the varying degrees of exclusivity of data

The data value chain[182] (see Fig. 2) depicts how data gains value. The following steps can be distinguished: 'data generation', 'data collection', 'data analytics' and 'data exchange'.[183] When discussing data access, we will have to consider, among other things, at which step of the value chain access shall be granted.

[179] European Commission, EDM Monitoring Tool, 2020.

[180] For a definition of data markets see European Commission, Final Study Report of the Updated European Data Market Study, 2020: a market where digital data is exchanged as products or services derived from raw data as well as the value of the overall data economy (including the economic impacts generated by the data market). See also Simon et al., TRUSTS Trusted Secure Data Sharing Space, 2021: a digital system where data is traded as an exchangeable economic good. It connects data providers and data buyers and facilitates data exchange and financial transactions. It has mechanisms to enforce laws, rules, and regulations to coordinate transactions, so that the trust of data marketplace users can be enhanced. Key actors that provide data marketplace functionalities include data marketplace owners, operators, and third-party providers (TPPs). Other actors to support data marketplaces are infrastructure providers and independent data brokers.

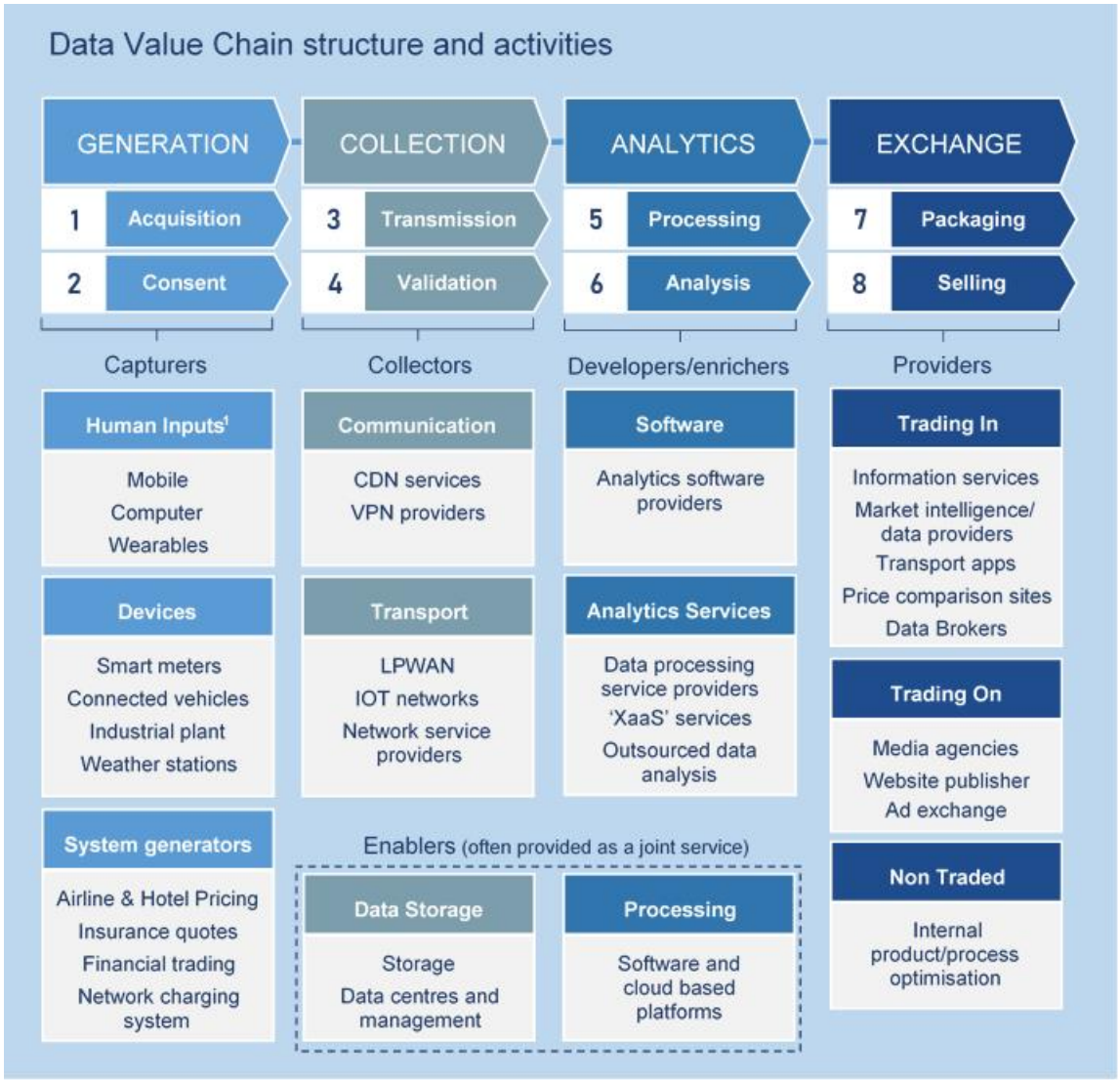
[181] COM(2020) 66 final.

[182] See Peitz/Schweitzer NJW 2018, 275.

[183] GSMA, The Data Value Chain, 2018.

Data also differ along many other dimensions, including their exclusivity: whereas some data are collected by a variety of firms in parallel (e.g. geolocation via a smartphone app), other data are more exclusive or expensive to obtain. This may be due to an exclusivity of data access points, temporal advantages of data access where the 'freshness' of data matters or the control of collection-inducing products and services, or legal and behavioural limitations on collection.[184]

Fig. 2 Data Value chain



Source: GSMA (2018)

b) Different interests of different actors in data-driven markets

[184] Gal/Rubinfeld N.Y.U. Law Rev. 2019, 737, (747).

Data access and data sharing comes with different benefits and risks for the different actors and stakeholders involved.[185] The most important actors are data holders (who may – depending on the circumstances and their business model – benefit from sharing data, selling data analytics or from using data exclusively), data co-generators (who have also participated in the generation of the data, but do not control it, data co-generators will typically benefit from having access to the data – for further discussion see below), data subjects (where personal data is involved), data users (who may be able to engage in innovative product and service development based on data), and data intermediaries (who may facilitate the access to and sharing of data).

c) Data taxonomies

Data exists in a variety of forms. It can be structured or unstructured, it can contain personal or non-personal information, and it can be collected by various different means for different purposes in different domains. All these factors may become relevant for the emerging legal framework.

The OECD provides the following categorization of data with a view to systematizing and informing the governance of data sharing and access: (i) 'Personal data', with varying degrees of identifiability, (ii) 'The domain of the data', (iii) 'The manner data originates', (iv) 'The ways in which data is accessed and controlled'.[186] We address the first three aspects here and deal with the ways in which data is accessed and controlled more in depth in e).

aa) Personal data vs non-personal data – degrees of identifiability

Where a dataset contains personal data, the GDPR sets out the rules based on which the data can be accessed or shared. Given the constraints that the GDPR imposes on any processing of data, a clear distinction between personal and non-personal data is of the essence. So far, the line is difficult to draw. A broad literature has emerged that shows how seemingly anonymised data, when combined with other data points, may allow for the identification of persons again[187] (on this see part E(I)(4)).

The ISO/IEC 19941 standard for interoperability and portability in cloud computing outlines five levels of data identifiability. Starting with the most identifiable one and progressively becoming less so, the five levels are: 'identified data', then 'pseudonymised data', 'unlinked pseudonymised data', 'anonymised data' and 'aggregated data'. On a technological level, the

---

[185] See Thuermer/Walker/Simperl, Data Sharing Toolkit, 2019, https://eprints.soton.ac.uk/436050/1/7770_Final_Data_Sharing_Toolkit_Web.pdf (last visited 4.7.2022).

[186] OECD, Enhancing Access to and Sharing of Data: Reconciling Risks and Benefits for Data Re-use across Societies, 2019.

[187] OECD, Enhancing Access to and Sharing of Data: Reconciling Risks and Benefits for Data Re-use across Societies, 2019. See also Article 29 Data Protection Working Party, Opinion 05/2014 on Anonymisation Techniques, 0829/14/EN WP216, 8-10; Klar/Kühling in Kühling/Buchner, DS-GVO BDSG, 3rd ed. 2020, Article 4 No. 1, paras. 31-34; Roßnagel ZD 2021, 188; Hansen in Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Article 4 No. 5 paras. 50-57.

ISO/IEC 19941 helps to discern the extent to which data can be traced back to individuals and subsequently, to decide on an appropriate level of data openness as well as on legal and technical parameters regarding data sharing and access.

What is ultimately needed for a data economy to flourish is a *legal* clarification of when data can be considered fully anonymised, i.e. a legal test that provides some degree of legal certainty regarding the conditions under which data access and data sharing are no longer constrained by the GDPR. We return to this point under part E(I)(4).

bb) Data domains: private and public-sector data

The most common data domain differentiation is between private and public-sector data. This distinction influences the extent to which data can be shared and accessed. In particular, policies have aimed to open up public information for private re-use early on.[188] According to the 'open data' paradigm, data that public sector bodies collect, create and hold for fulfilling public tasks should normally be made available to everyone for re-use, if possible, for free and without restrictions. The underlying rationale is that data that the state generates (often with taxpayers' money) should be widely disseminated to maximise the degree of (private) innovation based on such data and to increase social welfare.[189] General 'horizontal' rules on the re-use of public sector information[190] are complemented by sector specific rules which provide access to specific public sector data.[191]

By contrast, the default for privately held data is private control.[192] Such private sector data partly consists of personal, partly of non-personal data (see above). Consequently, the OECD differentiates between three data domains: 'the personal domain' (where individuals can be identified, i.e. the data is personal within the meaning of the GDPR), 'the private domain' (proprietary data that are protected by Intellectual Property Rights (IPRs), including copyright and trade secrets, or other (e.g. contractual) access and control rights, and for which there typically exists an interest in excluding others) and 'the public domain' (no IPRs) where access and re-use is free.[193] These domains are not fully separate, however, but rather overlap at times. However, each domain is subject to a different regulatory environment. Overlaps may then complicate the finding of a data governance framework that works for all stakeholders.

---

[188] See Directive 2003/98/EC on the re-use of public sector information, OJ 2003 L 345, 90 [repealed by Directive (EU) 2019/1024 on open data and the re-use of public sector information, OJ 2019 L 172, 56]; OECD Recommendation of the Council for Enhanced Access and More Effective Use of Public Sector Information, 2008.

[189] On the conceptual foundations see Richter, Information als Infrastruktur, 2021, p. 38–42.

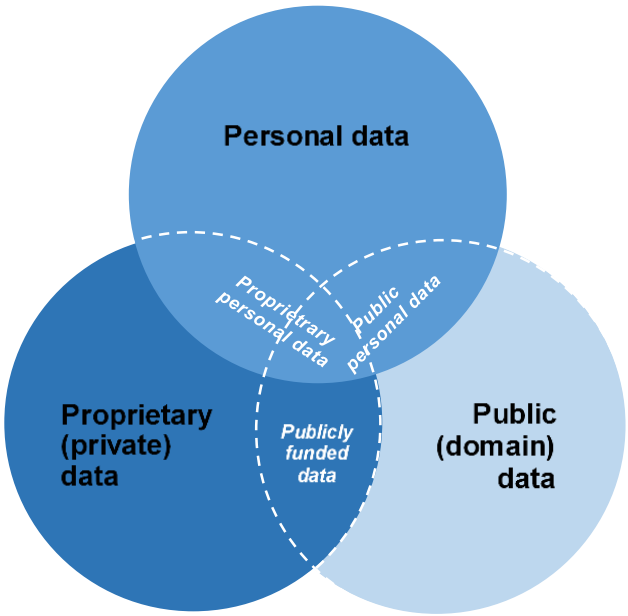
[190] OJ 2019 L 172, 56.

[191] OJ 2007 L 108, 1.

[192] Schweitzer/Welker in German Federal Ministry of Justice and Consumer Protection/Max Planck Institute for Innovation and Competition, Data Access, Consumer Interests and Public Welfare, 2021, p. 109.

[193] OECD, Enhancing Access to and Sharing of Data: Reconciling Risks and Benefits for Data Re-use across Societies, 2019.

Fig. 3 Domains of data: personal, private and public



Source: OECD (2019)

cc) How data originates and how it is processed

Abrams has distinguished four ways of how data is collected (see Table 1): data may be provided, observed, derived and inferred.[194] Data is 'provided' if it is intentionally shared by the user of a product or service (e.g. by posting on social media or entering credit card information). The term 'observed data' is used when user activities are passively captured and recorded (e.g. location data or click data). Finally, new data may be created through data analytics, where, for example, observed data is transformed into 'derived/inferred' data (e.g. credit scores).

This distinction has become important for policy debates on data rights and data access in many ways. For example, many argue that legal mandates to make data portable or accessible should typically be limited to provided or observed data. Also, the sharing of derived and inferred data – even if voluntary – may at times be anti-competitive (see below). At times, competition authorities have referred to related distinctions. In its Google/Alphabet decision under § 19a GWB, the Bundeskartellamt has distinguished between provided data and observed data (location data).[195] The European Commission distinguished in its Google/Fitbit merger decision

[194] Abrams, The Origins of Personal Data and its Implications for Governance (21.3.2014), https://ssrn.com/abstract=2510927 (last visited 4.7.2022).

[195] Bundeskartellamt 30.12.2021, B7-61/21 – *Google/Alphabet*, paras. 152 et seq.

according to the data source, namely if the data is generated manually (meaning human), by the device (e.g. via sensor) or by inference.[196]

The European legislator has not (yet) formally adopted the distinction between provided, observed, derived and inferred data. Nonetheless, it sometimes refers to the distinction in the recitals to legislative proposals. According to Recital 59 of the DMA, for example, the portability right of Article 6 No. 9 DMA applies to "the data they [business users and end users] *provided* or that was *generated through their activity* on the relevant core platform services of the gatekeeper" (emphasis added). The data sharing obligation of Article 6 No. 10 DMA towards business users applies to data 'provided' and 'generated' from the use of a core platform service by a business user or its end users (see Recital 60).[197]

The Draft Data Act refers to machine-generated data, namely data generated by the use of a 'product'[198] or a 'related service',[199] i.e. data collected by sensors, cameras, microphones, gyroscopes, radar, lidar and similar modules, and relating to the functioning of the product and its components, how it is used and on the environment in which it operates (Recital 4), and hence primarily to usage data obtained in the context of the 'Internet of Things' (Recital 14). De facto, the data access rights under Articles 4 and 5 of the Draft Data Act therefore relate to both actively provided and passively observed data, as made clear in Recital 31. By contrast, derived or inferred data, where lawfully held, are outside the scope of the proposed Data Act (Recital 14).

Sometimes, a distinction is made between 'raw' and 'processed' data.[200] In economic literature, the term 'raw data' is often used for data before it is processed into meaningful information.[201] The European Commission's draft Horizontal Guidelines introduce another subdivision however: they distinguish between 'raw data', i.e. data in need of processing to be useful, 'pre-processed data', i.e. data that is prepared and validated, and 'data that has been manipulated in order to produce meaningful information' (para. 145).[202] At first glance, this distinction corresponds to the stages of the data value chain (see above). 'Pre-processed' data would then seem to describe a step in data mining and analysis that transforms raw data into a format that

[196] European Commission 17.12.2020, M.9660 – *Google/Fitbit*, para. 415.

[197] Interestingly, the Commission's original proposal included 'inferred data', too – see Recital 55 of COM(2020) 842 final.

[198] See Article 2(2) of the Draft Data Act.

[199] See Article 2(3) of the Draft Data Act.

[200] See, for example, Kerber J. Compet. Law Econ. 2019, 381 (393): 'Another big problem is that the in-vehicle data are themselves very heterogeneous, which implies that the optimal data governance solutions might be different for different types of data. This refers not only to the important distinction between personal and nonpersonal data (compliance with GDPR) but also to the distinction between raw and processed/aggregated data, data about technical functions of the (components of the) car or about traffic, road and weather conditions, and so forth.'

[201] See, for example, Muschalle et al., Pricing approaches for data markets, mimeo 2012.

[202] Furthermore, the draft Horizontal Guidelines include 'any other type of information, including non- digital information', COM(2022) 1159 final, para. 407.

can be understood and analysed by machines.[203] Under this premise, annotated or structured data would probably be regarded as pre-processed data. The product-related machine-generated data covered by the Draft Data Act would seem to qualify as either 'raw data' or 'pre-processed data'. Where exactly the line between 'raw' and 'pre-processed' data should be drawn remains unclear, however.

Ultimately, the purpose of the distinction will be determinative. In the draft Horizontal Guidelines, the goal is to determine whether competitively sensitive information is being exchanged (para. 428, see further below, part E(III)(1)(a)) – but the category of 'pre-processed data' is then mixed up with the category of aggregated data: under the heading 'aggregated/individualised information and data', the European Commission assumes that the exchange of raw data may be less commercially sensitive than the exchange of 'data that was already processed into meaningful information'. Furthermore, 'raw data may be less commercially sensitive than aggregated data'. Whether the European Commission understands data aggregation as a form of data pre-processing remains unclear.[204] If we try to link the distinction between 'raw' data, 'pre-processed' data and 'data that has been manipulated to produce meaningful information' to the OECD classification, the latter category would seem to qualify as 'derived data', whereas 'raw' and 'pre-processed data' might be either provided and observed data.

Table 1 Origins of data

Category	Sub-Category	Example	Level of Individual Awareness

Provided	Initiated	○ Applications
		○ Registrations
		○ Public records
		  ○ Filings
		  ○ Licenses
		○ Credit card purchases
			High

	Transactional	○ Bills paid
		○ Inquiries responded to
		○ Public records
		  ○ Health
		  ○ Schools
		  ○ Courts
		○ Surveys
			High

	Posted	○ Speeches in public settings ○ Social network postings ○ Photo services ○ Video sites	High

[203] This process may include, but is not limited to, converting text, symbols, and characters to numeric values, data imputation, and data cleansing.

[204] This would be consistent with the distinction of Kerber in the case of in-vehicle data between, *inter alia*, 'raw and processed/aggregated data', J. Compet. Law Econ. 2019, 381 (393).

Observed	Engaged	○ Cookies on a website ○ Loyalty card ○ Enabled location sensors on personal devices	Medium
	Not Anticipated	○ Data from sensor technology on my Car ○ Time paused over a pixel on the screen of a tablet	Low
	Passive	○ Facial images from CCTV ○ Obscured web technologies ○ Wi-Fi readers in buildings that establish location	Low
Derived	Computational	○ Credit ratios ○ Average purchase per visit	Medium to Low
	Notational	o Classification based on common attributes of buyers	Medium to Low
Inferred	Statistical	○ Credit score ○ Response score ○ Fraud scores	Low
	Advanced Analytical	○ Risk of developing a disease based multi-factor analysis ○ College success score based on multi-variable big data analysis at age 9	Low

Source: Abrams (2014)

Another important distinction relates to *how* data is processed: data can be used non-anonymously or anonymously on an individual level (i.e. bundled) basis, or it can be transformed and processed as an aggregate.[205] Individual level data refers to data used to provide a service to the individual, e.g. recommendations to a music app user based on the songs she has previously listened to. The Draft Data Act would seem to cover individual-level and bundled individual level data when it allocates rights to individual private or business users of a product or related service (Articles 1(1)(a), 4 lit. f.). Data is used anonymously on an individual level when the goal is not to directly serve an individual who generated the data in the first place but rather to train machine-learning algorithms or AI systems. Aggregated data refers to more standardised data that has been irreversibly aggregated, e.g. sales data, where access to individual-level data is not necessary.

d) Types of data sharing

Different types of data sharing have evolved that differ along technical, economical, organisational and legal dimensions. These types include ‘data pools and data spaces’, ‘data

[205] See Crémer/de Montjoye/Schweitzer, Competition Policy for the digital era, Final report, 2019, p. 8, 25 et seq.

markets and data exchanges', 'mandatory data sharing', 'open data', 'data commons', 'data cooperatives' and 'data trusts' (see also Table 2).

Table 2 Types of data sharing[206]

	Who shares with whom?	What data is shared, and how?	Who benefits?	Practical examples
Data pools & data spaces	Typically companies, research institutions or public authorities. Individual citizens are generally not directly involved.	In principle, a very broad range of data can be shared. The manner in which data is shared is not predetermined.	The actors involved benefit directly from pooling their data. Third parties may benefit indirectly, depending on the design.	The European Commission plans to create data spaces to support the development of new products and services.
Data markets & data exchanges	Companies share with one another in data markets. In data exchanges, individual users offer their data for sale.	Data sharing takes place via a supply-demand mechanism.	Market participants and operators benefit financially.	On the Universal Basic Data Income online platform, users can sell the data they generate online.
Mandatory data sharing	Companies operating in data-driven markets that hold a dominant market position are required to make I portion of their data available to others.	Exactly what data are to be shared, and how, has yet to be defined.	Data sharing primarily benefits companies without large quantities of data that need data to develop digital products and services.	Authors are not aware of any instances in which a general and comprehensive data-sharing obligation has been implemented.
Open data	Mostly used by government bodies that share data with the public.	Data on areas such as the environment, traffic or energy are made available through inline portals. Personal data and other sensitive	A potentially large number of users can benefit, as can the data providers, via feedback on erroneous datasets.	The GovData portal makes administrative data from Germany's federal, state and municipal governments

[206] Pawelke, Daten teilen, aber wie? Ein Panorama der Datenteilungsmodelle, 2020, p. 8.

		information are excluded.		publicly available.
Data commons	No fixed standard regarding what data is collected, and with whom it is shared. Similarly, there are no fixed mechanisms or decision-making bodies. Rather, decisions are meant to be made and actions taken in the interest of the community.	The data commons model is in principle applicable to different kinds of data, but is generally discussed in the context of user-generated data. It emphasises the need for collective decision-making processes, as individual decisions have an impact on third parties.	Data sharing is primarily meant to benefit the community, although the community can be defined in different ways.	The goal of the DECODE project is to test data-commons models that give citizens the opportunity to decide how the data they produce can be used by third parties.
Data cooperatives	Members of data cooperative share data among themselves, and depending on the design, potentially with external parties as well, in some cases against payment.	No fixed standard regarding what data are to be shared. However, the model generally involves data generated by the individual members.	Members of individual cooperatives benefit by pooling their data, which among other advantages, gives the collective a better negotiating position vis-a-vis external parties.	In the MIDATA data cooperative, members pool their health data in order to make it available for disease research.
Data trusts	Individual actors transfer governance over their data, or decisions regarding data access and usage rights, to one or more trusts.	If and how data trusts will share data generated by their members with other actors varies from trust to trust.	Individual users are freed from dealing with data sharing and usage question by letting data trusts handle data control. They can choose the data trust that best fits their preferences.	The Open Data Institute has tested data trusts for purposes such as combatting illegal wildlife trafficking and the reduction of food waste.

Some sectors are considered to be particularly prone to be driven by data in the future (such as automotive, agriculture, mobility, or health). In these areas, undertakings have started to experiment with data sharing and governance models. The European Commission supports these efforts with its 'Common European data spaces' initiative (more on this: see part C(I)(1)).

Data sharing and governance becomes an important issue also where value-adding networks or digital ecosystems emerge. Frequently, they evolve around large digital platforms and the services they provide, around physical objects or products in the area of IoT and around cloud services. Given that these services and products and the value they provide to consumers are heavily data driven, data access and data sharing is key. In particular, the degree of data access and data sharing determines who can enter complementary or aftermarkets and who can innovate on which basis. Again, some initiatives can be identified that strive to organise data sharing in these (and other) settings – for example GAIA-X – a prominent European project that strives to create an open, trustworthy, secure data-sharing ecosystem in line with European values and rules. More precisely, it aims to define policy rules and standards for a decentralised and federated ecosystem and to establish "mechanisms for the transparent, self-determined sharing and processing of data across different parties [...]" in this environment.[207] Contrary to Amazon Web Services (AWS) or Microsoft Azure, GAIA-X is not a hyperscaler but rather, a federated infrastructure building upon and connecting already existing European infrastructures.

Legally, a number of legislative initiatives strive to impose data portability and/or data sharing requirements in such settings and under different conditions (see part E(V) (on § 19a GWB and the DMA) and part F(I) (on the Draft Data Act)). These legislative initiatives show that there frequently is a remarkable reluctance to share data in these settings so far.

Data sharing of a different kind may be involved when it comes to the development and experimenting with Artificial Intelligence (AI) for a multitude of purposes that may well fall outside the activity of a value-adding network or ecosystem. Generally, data access for AI development currently takes place in the absence of a regulatory framework. The focus of the European Commission's recent AI Act proposal[208] of the European Commission rather is on the governance of AI systems.

In all areas where data access and data sharing – whether voluntary or mandated – becomes an issue, the question of data governance is raised, and in particular whether data intermediaries shall be involved. While data intermediaries are beginning to operate in some areas (such as MIDATA or test runs of the Open Data Institute), they continue to play a minor role in practice so far. The EU strives to promote these models through the DGA by establishing a governance framework for data sharing providers (further on this, see below, part F(IV)(4)). Articles 10 et seq. of the DGA require these providers to, *inter alia*, remain neutral and, in the case of offering

[207] GAIA-X, Policy Rules and Architecture of Standards, 2020, p. 4.

[208] COM(2021) 206 final.

services to natural persons, to assume fiduciary duties towards the individuals using them. Where the European legislator mandates data access, it typically does not specify the type of data sharing mechanism to be chosen, however.

e) How data is shared: technical governance and standardisation

Sectoral or cross-sectoral data sharing does not only raise legal issues, however. First of all, a technical architecture has to be developed for the sharing of data – irrespective of whether data access and data sharing are organised on a voluntary basis or whether data access is mandated. In doing so, questions regarding data formats and the design of the interfaces through which data is shared are bound to arise. Furthermore, standards may need to be developed to provide trust in the quality of data and to allow for the tracing its provenance.[209]

aa) The ways in which data access is provided and controlled

Data sharing may occur in a variety of different scenarios: data may simply be passed on to a third party. But it may also be in the interest of the parties to a data sharing transaction or legally necessary, to limit and control the use of data by that third party. Consequently, the ways in which data access is provided and can be controlled is essential.

The OECD outlines how data are most commonly shared and accessed either via 'downloads', 'Application Programming Interfaces (APIs)', or 'data sandboxes'.[210]

Via downloads, data can be accessed online. This is the method most often used for sharing and accessing data from open data platforms.[211] The major issue with downloads is that of interoperability between platforms. Issues of interoperability might even persist, where data are stored and formatted in a machine-readable way. Another issue is related to cybersecurity and privacy where once the data has been downloaded, it leaves the data holder's sphere of control.

APIs allow for more streamlined access and interoperability of data.[212] Furthermore, APIs also allow data holders to maintain more control over the data, with the ability to limit or specify the parameters of the data sharing and access.

Data sandboxes provide data holders with the greatest degree of control. The OECD describes them as "any isolated environment, through which data are accessed and analysed, and analytical results are only exported, if at all, when they are non-sensitive". In this setting, the

[209] See BDVA, Towards a European Data Sharing Space: enabling data exchange and unlocking AI potential, 2019.

[210] OECD, Enhancing Access to and Sharing of Data: Reconciling Risks and Benefits for Data Re-use across Societies, 2019.

[211] Ibid.; Ubaldi, Open government data: Towards an empirical analysis of open government data initiative, 2013.

[212] Borgogno/Colangelo Comput. Law Secur. Rev. 2019, 105314.

data is not freely accessible online. Rather, access often requires a physical presence to where the data is kept.

bb) Data standardisation

The technical infrastructure is the basis for any form of data access and data sharing. It can create – or help tackle – economic as well as legal barriers. For example, the technical infrastructure can allow data holders to control access to their data or can provide de-identification methods to comply with the GDPR. At the core of data sharing is interoperability, i.e. the ability of products or systems to work with other products or systems. It can be realised by the use of common standards. Standardisation within this framework is associated with standards in the data value chain such as the "attributes of the data to be collected; to the terminology, structure, and organisation of the dataset; to aspects of data storage (location, etc.); or to its use (including protocols for data portability)".[213] The most prominent example of standards for data sharing and access are APIs, which are the computer protocols that set the framework of communication between IT segments. More specifically "APIs ease the flow of data by describing the kinds of data that can be retrieved, how to retrieve it, and the format in which data will be shared".[214]

Gal and Rubinfeld depict three main technical obstacles to data use which standardisation would solve.[215] The first is 'metadata uncertainties' and refers to the data about the data or its attributes (e.g. data semantics or data accuracy). When there is a lack of metadata, it compromises the ability of others to use the data. The second is 'obstacles to data transformation' where there are issues of combining datasets. The third is 'missing data' and can be the most problematic and difficult to rectify. Overall, some of the major technical issues are related to interoperability and developing an appropriate architecture of standards.

Before looking at the variety of standards related to data interoperability, it is useful to have a brief outline of the various standard setting organisations (SSOs). At the international level the most prominent examples are the International Organization for Standardisation (ISO), the International Electrotechnical Commission (IEC), the International Telecommunication Union (ITU) or the World Wide Web Consortium (W3C). There are also regional SSOs where the most relevant ones for data sharing and access in the EU are the European Committee for Standardisation (CEN), the European Committee for Electrotechnical Standardisation (CENELEC) and the European Telecommunications Standards Institute (ETSI). Furthermore, there are national standardisation organisations – such as the Deutsche Institut für Normung (DIN) in Germany. Traditionally, SSOs and the subsequent standards are industry driven and thus the adherence to a standard is often voluntary. Some standardisation activities are mandated, however. In the EU, the European Commission can request or mandate standards

[213] Gal/Rubinfeld N.Y.U. Law Rev. 2019, 737 (749).

[214] Id., 750.

[215] Gal/Rubinfeld N.Y.U. Law Rev. 2019, 737.

from the European Standardisation Organizations (ESOs) namely CEN, CENELEC and ETSI, under EU Regulation No 1025/2012.[216] The use of these standards still remains voluntary unless particular reference to a standard is made in a piece of EU legislation. Where no standard is legally referenced, some standards may still be developed to ensure compliance with special acts of legislation, such that organisations can utilise the standard to facilitate and provide certification for legal compliance.

Frequently, a lack of data-related standards is deplored. Based on the analysis of strategic dependencies in the updated Industrial Strategy as well as stakeholder input through the industrial alliances, an urgent need for the development of standards has been identified, inter alia, with regard to data standards enhancing data interoperability, data sharing and data re-use in support of the Common European Data Spaces.[217]

However, relevant standards already exist but are not used. An example is the ISO/IEC 19941 standard for interoperability and portability in cloud computing. While this standard exists since 2017, an analysis of all German companies' websites – using a web scraping methodology – reveals that only one company refers to this standard. Similarly, despite the existence of the W3C family of provenance standards, the BDVA states that there is currently weak 'provenance support'.[218]

Other relevant data-related standards at the international level include, for example, the ISO 2700 series for information security management, which are used to comply with certain segments of the GDPR.[219] Also, significant standards are developed by the W3C. Data formats include XML, JSON and CSV which are often used to port data. Other important standards include the Resource Description Framework (RDF) – for data interchange on the web; the Web Ontology Language (OWL) – for semantic interoperability; and standards to query for information, SPARQL and XQuery. There is also the PROV family of specification particularly, the Provenance Data Model (PROV-DM) which allows for the sharing of provenance information. At the EU level, CEN/CENELEC have engaged in a variety of standardisation activities related to interoperability. Searching through their standards database with the term 'interoperability', legal framework being 'Directives' and standards classification 'ICS' results in 383 standards. Of those, 346 have already been published, 11 are under drafting, 4 are in the preliminary stage, 21 under approval/enquiry and 1 is approved. What is also particularly interesting is that the standard DIN SPEC 27070 'Requirements and reference architecture of a security gateway for the exchange of industry data and services' has been developed and is being used by intermediary platforms or data spaces 'GAIA-X' and International Data Spaces (IDS).[220]

[216] OJ 2012 L 316, 12.

[217] COM(2022) 31 final.

[218] See BDVA, Towards a European Data Sharing Space: enabling data exchange and unlocking AI potential, 2019, p. 10.

[219] Pandit et al. 2020.

[220] See GAIA-X, Policy Rules and Architecture of Standards, 2020.

The existing standards may not suffice, however. In the EU, the need for data standards has been included in the new European standardisation strategy.[221] However, the fact that a relevant number of standards exist but are not utilised provides reason to inquire whether there are other barriers to data sharing – whether economic, organisational or of a different kind.

III. Empirical analysis on data sharing in the EU and Germany

Based on the categorizations established above, we now summarise the most important empirical findings on the state of data access and data sharing in the EU and – more thoroughly – in Germany. For the EU, we focus on the European Commission's Impact Assessment Report annexed to the Draft Data Act of 2022[222] and on the studies conducted in the context of this impact assessment (1.).[223] Since these reports and studies are not able to provide representative and consistent results, we have conducted several analyses to try to generate a more balanced view for Germany based on different approaches (2.).

1. Evidence of the under-use of data in the EU

According to the Impact Assessment Report accompanying the publication of the Draft Data Act[224] and a number of studies conducted in its context, the economic potential of data is currently severely under-exploited throughout the EU.

In its Impact Assessment Report, the European Commission finds that only around half of the economic potential of non-personal industrial data along the value chain and even only one third of the potential of exploiting data across sectors has been realised.[225] According to another study, less than 10% of the companies are deriving value from data. In addition, the data usage is focused on a few experimental use cases.[226]

Simultaneously, around three quarters of the firms responding to the consultation of the Data Strategy complain about problems in getting access to the data required from other companies.[227] Voluntary B2B and B2G data-sharing agreements have not been effective in

[221] COM(2022) 31 final.

[222] COM SWD(2022) 35 final.

[223] For example, European Commission, SME panel consultation B2B data sharing - Final Report, 2019; European Commission, Industrial ecosystems survey, Main findings, 2019; European Commission High-Level Expert Group on B2G, website. European Commission, Study to support an Impact Assessment on enhancing the use of data in Europe, 2022 [study prepared by Deloitte]; European Commission, Outcome of the online consultation on the Data Act, 2022.

[224] COM SWD(2022) 35 final.

[225] Id., 8. See also Deloitte, Realising the economic potential of machine-generated, non-personal data in the EU, Report for Vodafone Group, 2018, p. 30.

[226] See Bisson et al., Breaking away: The secrets to scaling analytics, 2018.

[227] European Commission, Outcome of the online consultation on the European strategy for data, 2020.

solving this problem.[228] In particular, SMEs report that in practice, these data sharing agreements did not help them to access data from other companies.[229] A more recent survey by the European Commission focusing on EU industrial ecosystems confirmed that serious barriers continue to exist with regard to the availability and use of data.[230] Another study related to the impact assessment of the Data Act confirmed this observation.[231]

Despite the existence of some sectoral legislation and codes of conduct, e.g. on agricultural data sharing, most cases of data access and use are eventually voluntary. However, around two thirds of companies replying to the online consultation had problems in getting access to other companies' data based on bilateral contract negotiations.[232] More than half of the companies experienced general refusals in getting access to data. Still almost half of them report an abuse of imbalances of bargaining power in the specifications of the contracts. And still over 40% complain about unfair high prices. These results are confirmed by other studies.[233] In particular, when companies try to make use of data in their provision of products and services including the installation and repair of machinery, they are frequently confronted with contractual limitations.[234]

This evidence is corroborated by the European Commission's public consultation on a Data Act[235] – which does not provide representative numbers, however: only slightly more than three hundred organisations responded to the Data Act consultation, which is a small and biased sample both in numbers and distribution.[236] Therefore, the two thirds of all respondents and the more than 90% of representatives of companies claiming to share data with other companies by either providing own or accessing other companies' data should not be regarded as reflecting the reality, as revealed in the above mentioned studies accompanying the publication of the Draft Data Act. Therefore, we will not report percentages related to the results of the Data Act consultation, but only qualitative results.

According to the consultation, data is shared mainly on a voluntary basis, and only to a very small degree on a mandatory basis. Where data is shared, it is used to develop new products

[228] COM(2018) 232 final; COM SWD(2018) 125 final.

[229] European Commission, SME panel consultation B2B data sharing - Final Report, 2019.

[230] European Commission, Industrial ecosystems survey, Main findings, 2020; European Commission High-Level Expert Group on B2G website.

[231] European Commission, Study to support an Impact Assessment on enhancing the use of data in Europe, 2022 [study prepared by Deloitte].

[232] European Commission, Outcome of the online consultation on the Data Act, 2022.

[233] European Commission, Industrial ecosystem survey, Main findings, 2022.

[234] European Commission, Study on emerging issues of data ownership, interoperability, (re-)usability and access to data, and liability, 2018 [study prepared by Deloitte].

[235] European Commission, Public Consultation on the Data Act: Summary report, 2021, https://digital-strategy.ec.europa.eu/en/public-consultation-data-act-summary-report (last visited 4.7.2022).

[236] A similar study on EU study data sharing companies by everis presents results based on slightly more than 100 companies – see European Commission, Study on data sharing between companies in Europe: final report, 2018. Therefore, they are not reported.

and service, to increase the efficiency of supply chains, to train AI based algorithms and to perform predictive maintenance.

The obstacles related to data sharing that were mentioned in the consultation were mostly of a technical nature, e.g. a lack of formats and standards; but in addition, legal hurdles were pointed out, e.g. legal uncertainty regarding the legality of data sharing under competition law, uncertainty regarding the legal basis for data sharing under the GDPR and uncertainty on the existence of 'sui generis' IP protection under the Database Directive. Finally, very high prices are mentioned as a problem.

The following measures are mentioned as potentially helpful to improve data sharing: the development of model contracts could be helpful in particular for SMEs. A fairness test under contract law could help avoid unfair conditions and ensure fair horizontal data access modalities. In the context of co-generated IoT related data, clear access rights for the users of IoT objects were perceived as a way forward. Smart contracts were mentioned as a potentially effective tool to technically realise continuous data access and use, but also to help realise data portability. Data portability was perceived to depend on standards, clear rules and viable identification/authentication methods.

2. Empirical evidence on the state of data access and sharing in Germany

Since the consultation and the studies conducted in the context of the impact assessment of the Draft Data Act, are not able to provide representative and consistent results, we have conducted several analyses to try to generate a more balanced view for Germany based on different approaches. First, we analysed companies' description in large company data bases (a). Second, we present the relevant results of three studies among German companies[237] based on around one thousand controlled observations (b). This stands in contrast to the uncontrolled answers to public consultation or the around one hundred responses to the surveys performed in the context of the impact assessment. Third, we conducted in-depth interviews with industry experts to reveal further details about the actual data sharing activities, perceived problems and suggested solutions (c). These three approaches allow us eventually to come to a sound evidence base of the data sharing activities of German companies.

a) Companies with a focus on data sharing – insights from company databases

In order to get a more reliable picture of the state of data access and sharing in Germany, we used two large databases – the Orbis database and Crunchbase – for companies which indicate that their business activities include 'data sharing'.

[237] IEDS, Anreizsysteme und Ökonomie des Data Sharings: Handlungsfelder des unternehmensübergreifenden Datenaustausches und Status quo der deutschen Wirtschaft, 2022; IW, Datenwirtschaft in Deutschland - Wo stehen die Unternehmen in der Datennutzung und was sind ihre größten Hemmnisse?, 2021; EFI, Jahresgutachten 2022 with reference to ZEW, Konjunkturumfrage Informationswirtschaft 3. Quartal 2021.

First, for more than 70% of the more than 380 million companies in the Orbis database, trade descriptions of around one page are available. However, only 38 companies contain 'data sharing' in their description based on a search in March 2022. Among these companies, only two companies are located in Germany, which are eventually not involved in data sharing.

Therefore, we applied the search strategy also at Crunchbase, which contains more than 2 million startups. Here, we identify in total 243 companies by the end of March 2022, which include 'data sharing' in their description. Eight of these companies, which represent slightly less than 5%, have their headquarters in Germany. Again, only two companies, i.e. Caruso and qDatum, are really are active in data sharing, the others are mostly providing consultancy around data sharing.

b) German studies

In this part, we summarise the most relevant results of three larger scale studies on the state of data sharing which focus on German companies and organisations, in particular studies conducted by the 'Incentives and Economics of Data Sharing' (IEDS) project, the 'Institut der deutschen Wirtschaft' (IW), and the 'Leibniz-Zentrum für Europäische Wirtschaftsforschung' (ZEW).[238]

aa) Incentives and economics of data sharing

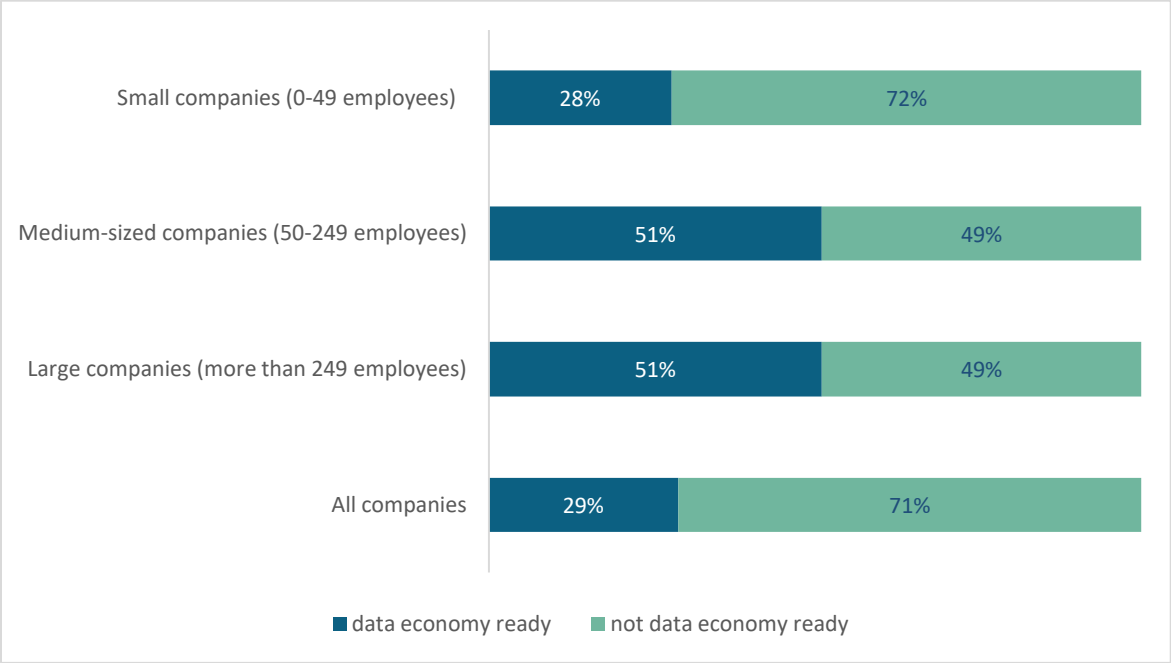
Within the IEDS project[239], a representative survey of more than one thousand companies from industry and industry-related service providers has been conducted in 2021 to examine the extent to which companies in Germany are able to manage data efficiently. In addition to their own data economy readiness, the survey asks to what extent joint data management with other companies plays a role. Finally, the companies are also asked about their cloud usage behaviour.

In particular, the proportion of companies has been identified that meet the requirements for participation in the data economy and, under certain circumstances, also have an internal data management, but so far do not share data with other companies. Furthermore, obstacles to data sharing have been identified in this way.

[238] IEDS, Anreizsysteme und Ökonomie des Data Sharings: Handlungsfelder des unternehmensübergreifenden Datenaustausches und Status quo der deutschen Wirtschaft, 2022; IW, Datenwirtschaft in Deutschland - Wo stehen die Unternehmen in der Datennutzung und was sind ihre größten Hemmnisse?; EFI, Jahresgutachten 2022 with reference to ZEW, Konjunkturumfrage Informationswirtschaft 3. Quartal 2021.

[239] In the following we present a reduced and modified version of selected sections of the English translation of IEDS, Anreizsysteme und Ökonomie des Data Sharings: Handlungsfelder des unternehmensübergreifenden Datenaustausches und Status quo der deutschen Wirtschaft, 2022.

Fig. 4: Data economy readiness (n= 1002)

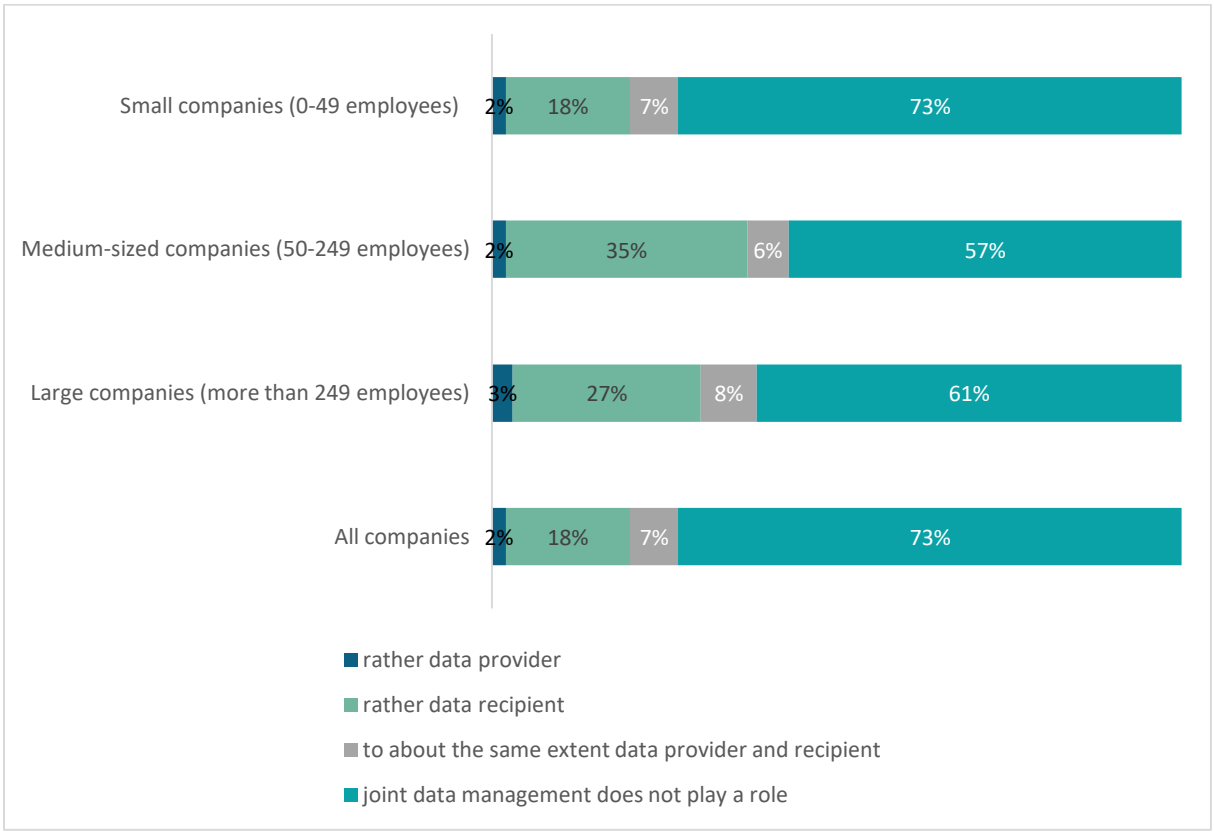


Source: IEDS, 2022, p. 21

In a second step, the companies were asked whether data sharing plays a role for them and whether they are data providers or data recipients (see Fig. 5).

In contrast to the results of the consultations and surveys conducted related to the impact assessment of the Data Act, data sharing does not play a role for almost two thirds of all companies. Less than 20% of the companies are more likely to be data recipients, only 2% are more likely to be data providers, and 7% are data providers and data recipients to roughly the same extent. In summary, only a very small minority of companies in the German industry and related services provide data.

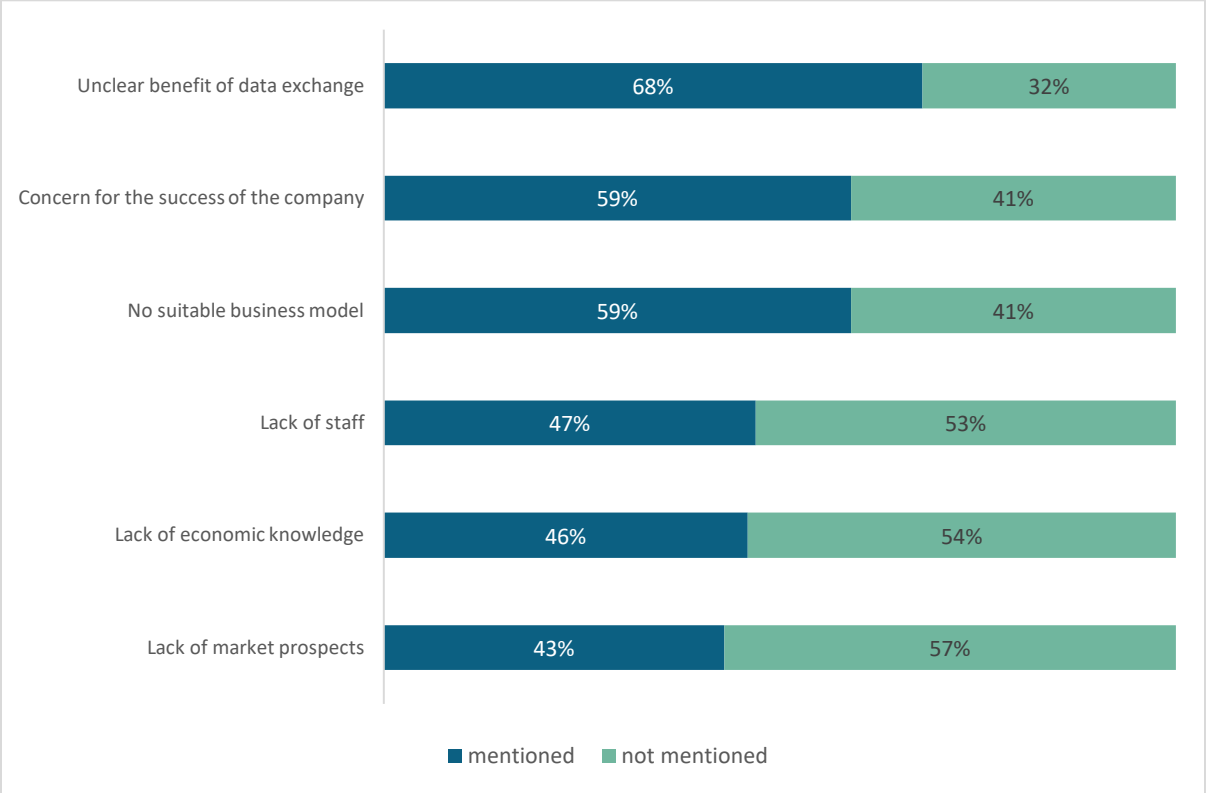
Fig. 5: Data sharing n= 987



Source: IEDS, 2022, p. 22

In summary, a large proportion of all companies see themselves more as recipients of data provided by third parties. Only 2% are data providers. The passing on of their own data plays a very minor role among the companies surveyed. This indicates that there are barriers to data sharing, which are presumably more likely to be present in data sharing than in the use of data from third parties. A smaller subsample of around 200 companies mentions the following economic barriers in connection with data sharing (Fig. 6).

Fig. 6: Economic barriers to data sharing n=219



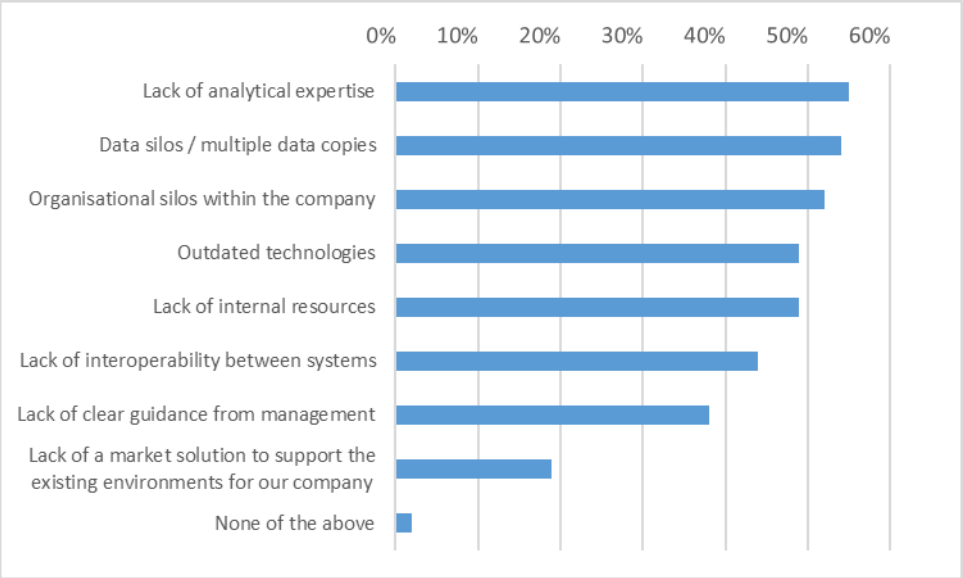
Source: IEDS, 2022, p. 23

Almost 70% of all companies that experience economic obstacles perceive the unclear benefits of data exchange as an economic barrier. Almost 60% of the companies mention concerns about the success of their own business or the lack of a suitable business model. Other economic obstacles are a lack of staff (47%), of economic knowledge (46%) and of market prospects (43%).

Complementary to the obstacles named in the survey performed within the IEDS project, the Harvard Business Review presented already in 2019 a list of reasons, which prevent the maximisation of the strategic value of data.[240] In addition to the lack of expertise, data silos are mentioned by more than half of the respondents. Furthermore, outdated technologies, lack of resources, missing interoperability, lack of guidance from the management and of market solutions are named.

[240] Harvard Business Review Analytic Services, Critical success factors to achieve a better enterprise data strategy in a multi-cloud environment, Pulse Survey 2019, https://hbr.org/resources/pdfs/comm/cloudera/CriticalSuccessFactors.pdf (last visited 4.7.2022), p. 11.

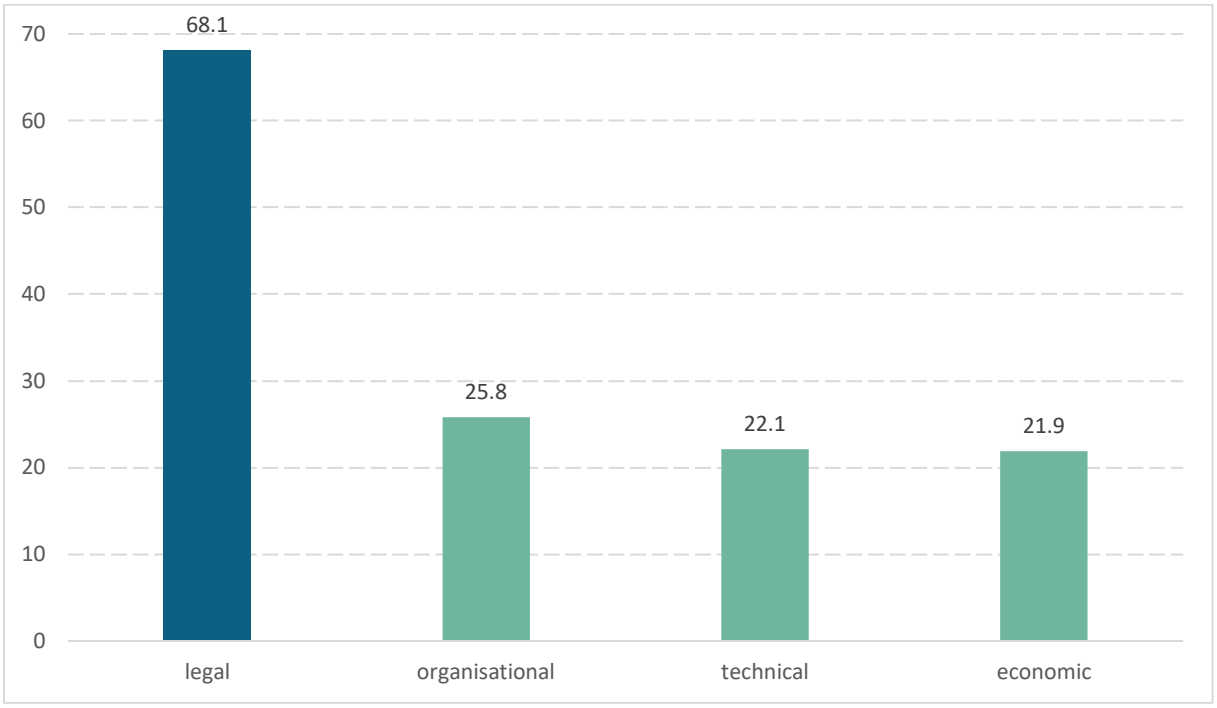
Fig. 7: Obstacles to maximising the strategic value of data[241]



The IEDS survey then examines the economic, legal, technical and organisational barriers to data sharing more in detail and finds that, in contrast to the above mentioned results of the consultation related to the Data Act, legal obstacles, in particular, hinder the willingness to share data. Almost 70% of the companies surveyed perceive legal barriers, while organisational, technical and economic barriers are only relevant for one fifth to one fourth of the companies.

[241] Harvard Business Review Analytic Services, Critical success factors to achieve a better enterprise data strategy in a multi-cloud environment, Pulse Survey 2019, https://hbr.org/resources/pdfs/comm/cloudera/CriticalSuccessFactors.pdf (last visited 4.7.2022).

Fig. 8: Barriers to data sharing n=1002

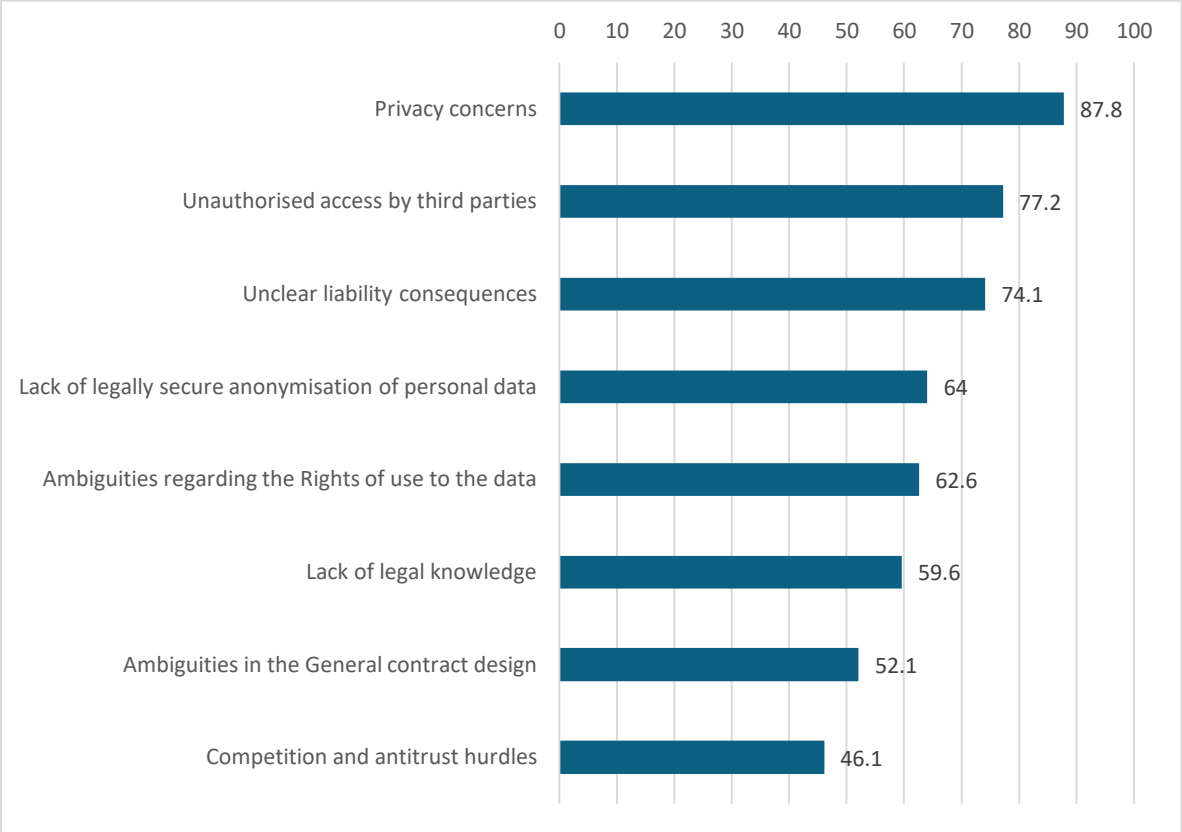


Source: IEDS, 2022, p. 52

The particular importance of legal barriers to data sharing calls for a further analysis of the different areas of law. Fig. 9 shows that for almost 90% of the companies surveyed, data protection concerns, in particular, limit their willingness to share data. A closer look shows that there are significant differences between small, medium-sized and large companies. Since small companies have limited legal expertise, the potential barriers are higher from their perspective.

Furthermore, unauthorised access by third parties is an obstacle for more than three quarters of the companies, followed by unclear liability consequences by almost three quarters, lack of legally secure anonymisation of personal data, lack of clarity regarding the rights to use the data, lack of legal knowledge as well as lack of clarity in the general drafting of contracts. For almost half of the companies, competition law related hurdles pose a problem.

Fig. 9: The importance of different legal barriers to data sharing n=723



Source: IEDS, 2022, p. 53

Consequently, there are not only legal uncertainties with regard to personal data, but also with regard to non-personal data, pertaining, in particular, questions of liability and contractual issues relating to the rights of use.

bb) Data use and obstacles

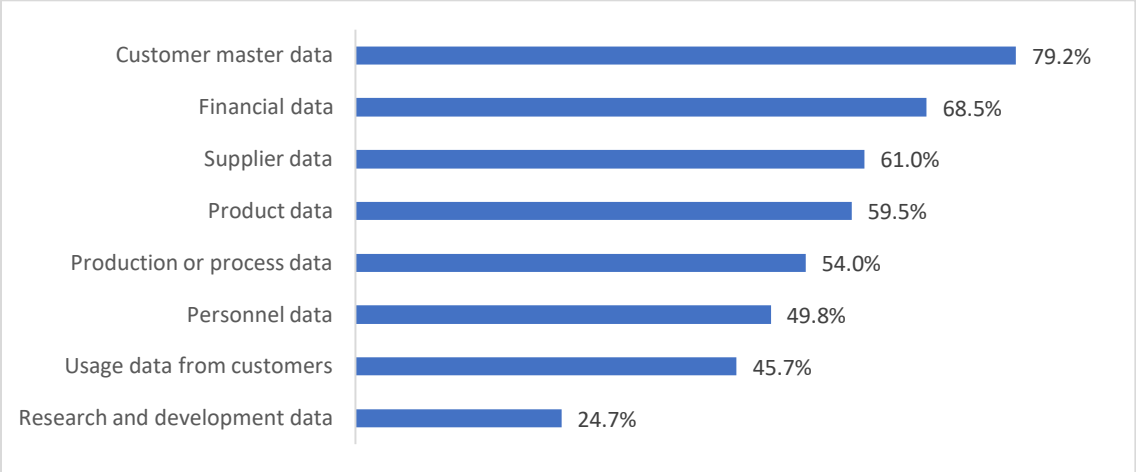
In the context of the project 'Datenwirtschaft in Deutschland – Wo stehen die Unternehmen in der Datennutzung und was sind ihre größten Hemmnisse?', around 500 companies in Germany from the industry and business-related service provider group were interviewed in a telephone survey on the topic of data economy in 2020.[242] The sample enables the analysis of further subgroups, e.g. the three employee size classes and the industry groups. The available survey results were extrapolated to the population of German companies on a number-weighted basis.

In a first part, the companies were asked about data storage in the survey. The companies surveyed store the master data of their customers most frequently (see Fig. 10). Almost four out of five companies state that they store this mainly or completely in digital form. In second and

[242] In the following we present a reduced and modified version of selected sections of the English translation of the results of IW, Datenwirtschaft in Deutschland - Wo stehen die Unternehmen in der Datennutzung und was sind ihre größten Hemmnisse?, 2021, https://bdi.eu/publikation/news/datenwirtschaft-in-deutschland/ (last visited 4.7.2022).

third place come the digital storage of financial and supplier data, which are stored digitally by more than two thirds and six out of ten of the companies, respectively. Likewise, product and production and process data are predominantly stored digitally by more than half of the companies surveyed. In contrast, slightly less than half of the companies state that they digitally store personnel or usage data. Not even a quarter of the companies store research and development data digitally.[243] Overall, it shows that while the majority of companies store data of one type or another, many companies still store customer master data alone or even no data at all.

Fig. 10: Storing data in digital form, n = 467

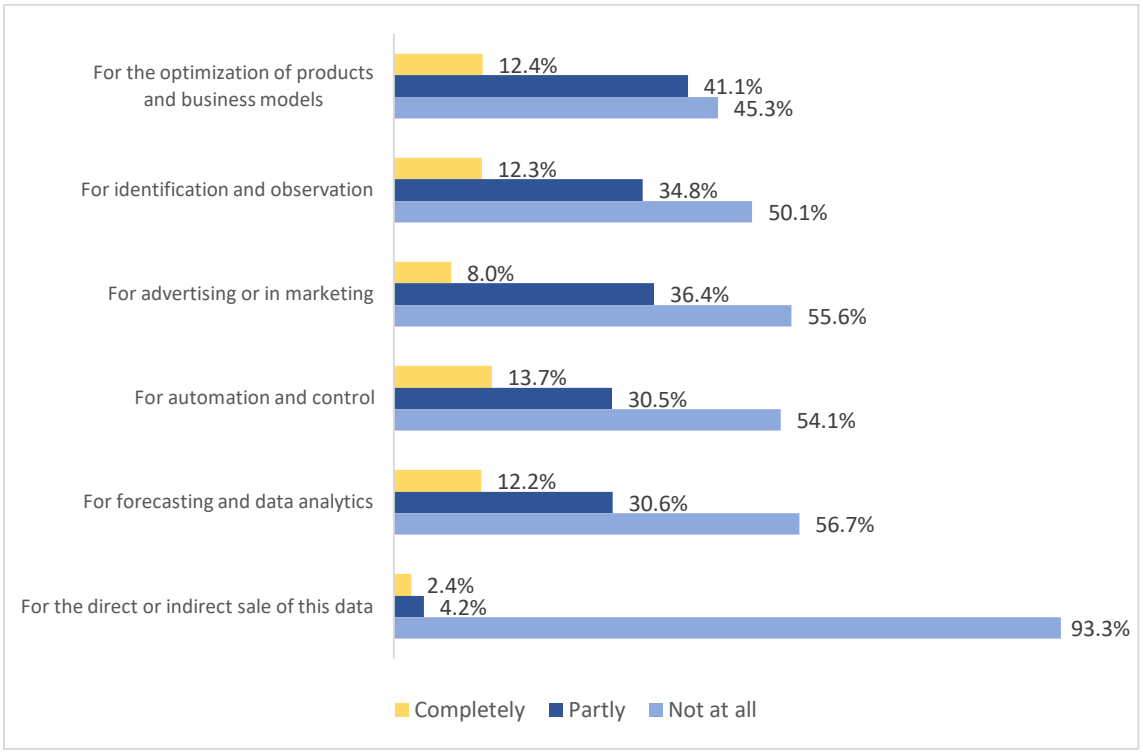


Source: IW-/IWC-Unternehmensbefragung Datenökonomie, 2020,
IW (2020): Datenwirtschaft in Deutschland - Wo stehen die Unternehmen in der Datennutzung und was sind ihre größten Hemmnisse?, p. 16.

When asked, in a second step, about the purposes of data use (see Fig. 11), the companies indicated six different purposes. The most frequently mentioned purpose is the optimisation of products and business models. With less than 5% agreement, monetisation through the sale of data plays hardly any role.

[243] The report does not specify how these data are stored instead.

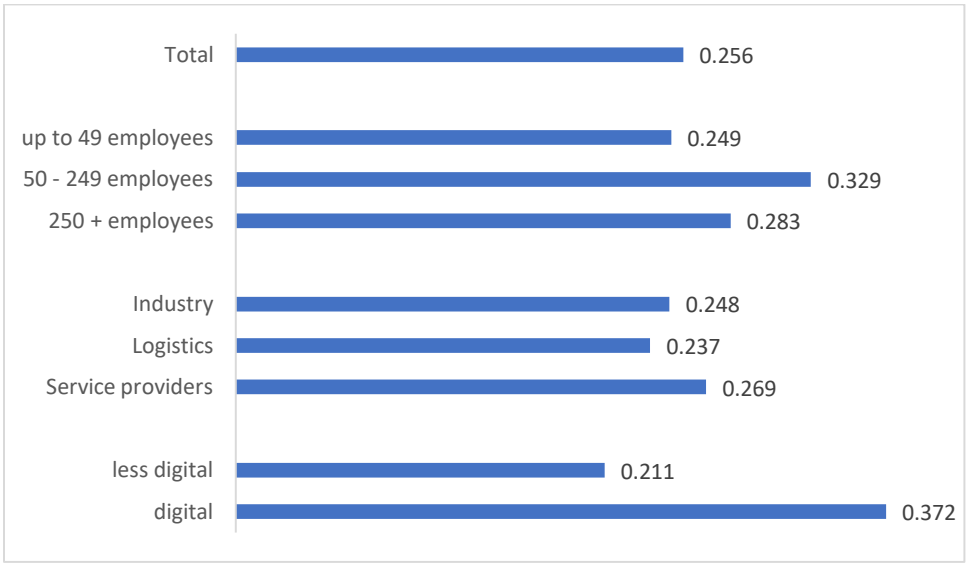
Fig. 11: Purposes of data use in the company, n = 467



Source: IW-/IWC-Unternehmensbefragung Datenökonomie, 2020,
IW (2020): Datenwirtschaft in Deutschland - Wo stehen die Unternehmen in der Datennutzung und was sind ihre größten Hemmnisse?, p. 20.

In the introductory question on data sharing, one quarter of the companies surveyed stated which data – for example, product data and customer and usage data – they need from external sources because they cannot generate them internally (see Fig. 12).

Fig. 12: Need for data from external sources, n = 467

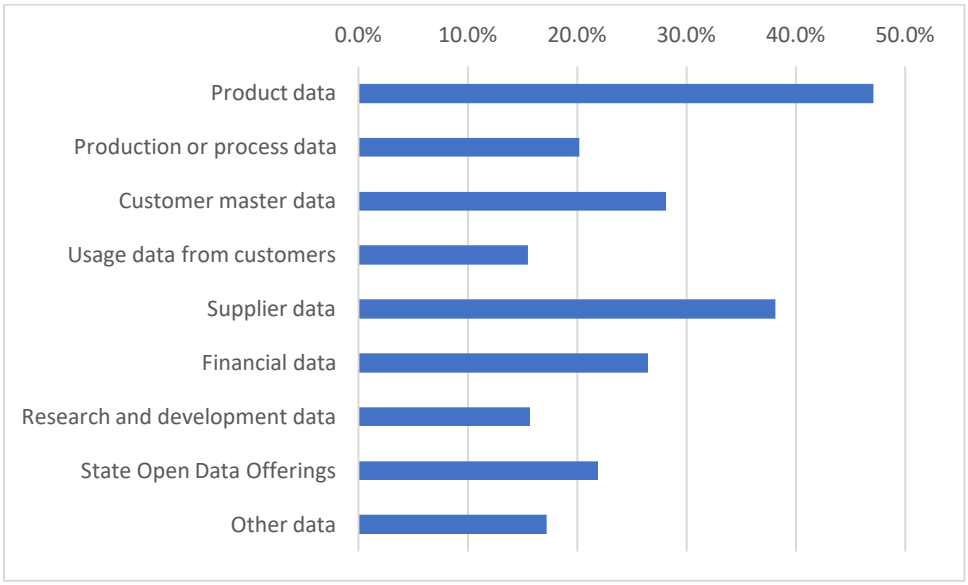


Source: IW-/IWC-Unternehmensbefragung Datenökonomie, 2020,

IW (2020): Datenwirtschaft in Deutschland - Wo stehen die Unternehmen in der Datennutzung und was sind ihre größten Hemmnisse?, p. 24.

In the overall sample, product data is most frequently obtained from external sources, namely by almost every second company (see Fig. 13). This is followed by supplier data, named by almost 40% and master data named by almost 30% of the companies surveyed. Less important for the survey participants is customer usage data – possibly because this is difficult to obtain – as well as research and development data. The latter could be due to the fact that the majority of companies do not conduct any continuous research and development (R&D).

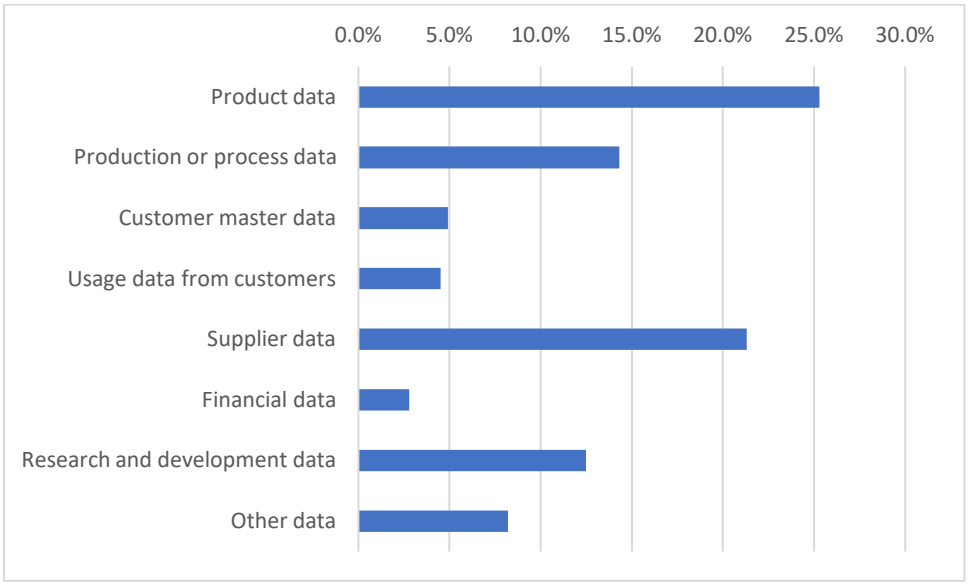
Fig. 13: Type of data needed from external sources, n = 467



Source: IW-/IWC-Unternehmensbefragung Datenökonomie, 2020,
IW (2020): Datenwirtschaft in Deutschland - Wo stehen die Unternehmen in der Datennutzung und was sind ihre größten Hemmnisse?, p. 25.

In addition to their need for external data, the companies were also asked which of these data types they would generally be willing to share with other companies. Only slightly more than 10% of the companies are willing to share their own data. With approval rates of one quarter or less, product and supplier data are in the top two places (see Fig. 14). In the case of product data, the large companies in particular show a clear deviation from the response behaviour of the overall sample. Not even 10% of the companies in this group are open to sharing product data in principle. The picture is different for production and process data. Here, more than one quarter of the large companies state that they are prepared to share data in principle. In summary, it can be observed that the companies would like to receive the data of others, if at all, while the willingness to hand over the types of data originating from their own company is on average slightly above 10%. Under no circumstances is the vast majority of more than 95% of the companies willing to share financial or usage data, but also customer data.

Fig. 14: Type of data ready to be shared, n = 467



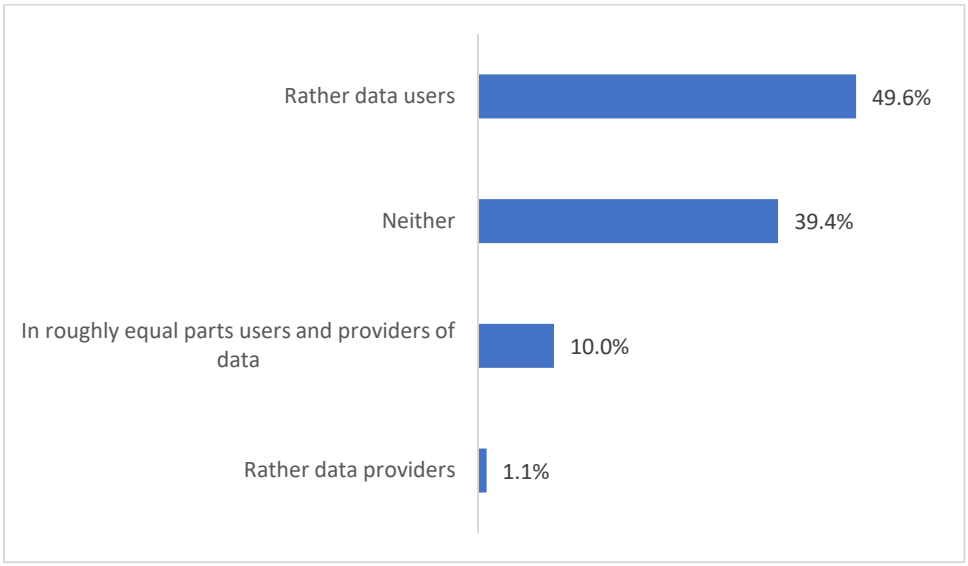
Source: IW-/IWC-Unternehmensbefragung Datenökonomie, 2020,
IW (2020): Datenwirtschaft in Deutschland - Wo stehen die Unternehmen in der Datennutzung und was sind ihre größten Hemmnisse?, p. 26.

The willingness to share data is closely related to the value that companies place on internal and external data. For this purpose, the importance of internal and external data for the companies was asked. Specifically, they were asked to indicate on a scale from very low to very high how important the two types of data are for their company's business model. Internal data is clearly more important for the companies than external data, i.e. almost 70% of the companies state that internal data is of high to very high importance for their own company's business model. For external data, the proportion is significantly lower at just over 40%.

The question of whether the companies are more likely to be data users or data providers shows a consistent result (see Fig. 15). With the exception of the less digital companies and industry, which most frequently state that they are neither data providers nor data users, all companies are more likely to be data users. Among all companies in the sample, just less than half indicate that they fall into this category.

Every tenth company acts in roughly equal parts as a provider and a consumer of data, while pure data providers are not really existing. In second place, on the other hand, is the statement 'neither', with a total of just under 40% of the companies agreeing. It is also striking that hardly any companies state that they offer data to other companies and institutions as part of their own business model: in total, only just over 1% of the companies state that this applies to them.

Fig. 15: Share of data users and providers, n = 463

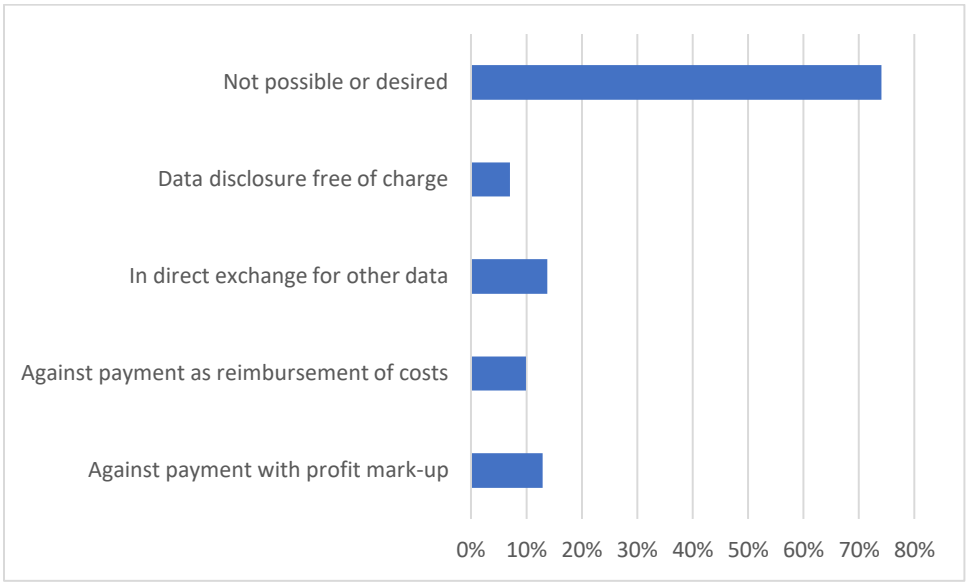


Source: IW-/IWC-Unternehmensbefragung Datenökonomie, 2020,
IW (2020): Datenwirtschaft in Deutschland - Wo stehen die Unternehmen in der Datennutzung und was sind ihre größten Hemmnisse?, p. 29.

Based on these findings, the question follows under which conditions it would at least be worth considering for the companies to make their own data available to other companies (see Fig. 16). The companies are confronted with various scenarios in the context of data transfer and asked to indicate the extent to which they could agree under these scenarios. The options are: against payment with a profit mark-up, against payment as reimbursement of costs, in direct exchange for other data, free data transfer and no data transfer possible or desired. The overwhelming majority of the companies surveyed – almost three quarters – state that no data transfer is possible or desired.

Large companies with more than 250 employees are particularly sparing with their data: here, more than three quarters state that data sharing is not possible or desirable in their company. Interestingly, slightly more companies state that they are willing to exchange data for other data (13.8%) than are willing to sell data for a fee with a profit mark-up (12.9%). Overall, however, the following expected hierarchy with increasing agreement values can be observed: free disclosure, disclosure in return for reimbursement of costs, in return for a profit mark-up or in exchange for other data, no disclosure desired.

Fig. 16: Conditions under which own data will be made available, n = 458



Source: IW-/IWC-Unternehmensbefragung Datenökonomie, 2020,
IW (2020): Datenwirtschaft in Deutschland - Wo stehen die Unternehmen in der Datennutzung und was sind ihre größten Hemmnisse?, p. 30.

The responses of the companies to the question of whether there should be an obligation to provide data are unambiguously negative. It is noticeable here, that the companies hardly distinguish between companies with a dominant position and companies with a 'normal' competitive position, i.e. the vast majority of them apparently do not see any problematic data monopolisation by large platforms. Large companies are the most sceptical when it comes to data access obligations. Among them, only 5% with a 'normal' market position and 4% with a dominant market position are in favour of a data sharing obligation. They may fear that larger companies are often considered to have a dominant position in the market and could therefore be directly affected by the consequences of this obligation. On the other hand, the service providers in particular are more in favour of compulsory contracting: almost 20% of these companies voted in favour of an obligation for market-dominant firms to pass on data. It is possible that this sector has had negative experiences with the business practices of large digital platforms that increase openness to legislative measures to limit market power, or the companies in question are more likely to expect economic benefits from the data they receive.

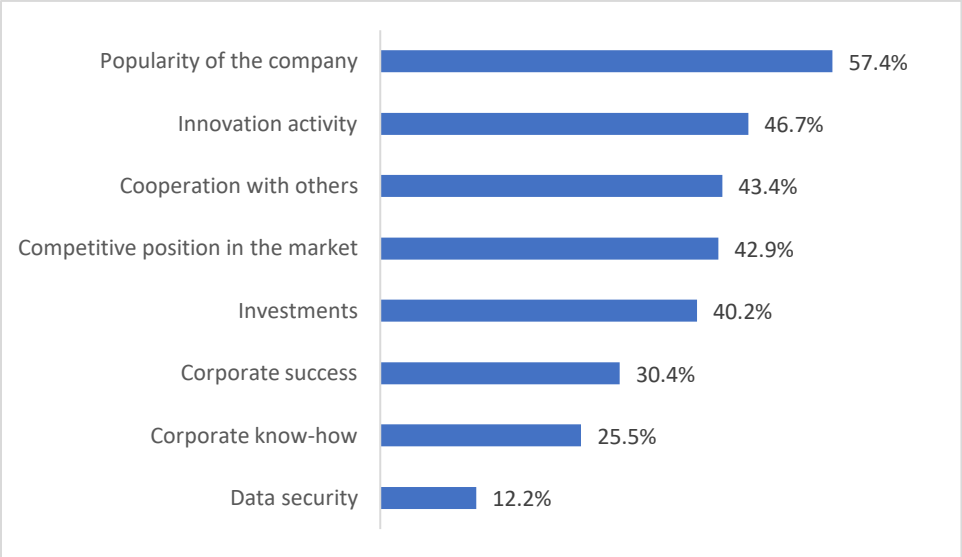
In order to deepen the issue of an obligation to share data once again, the companies were presented with a thought experiment: suppose there was a legal obligation for all European companies to publicly provide non-personal and anonymised personal data of their own company. Would this be more of an opportunity, a risk or both? A distinction was made between eight dimensions of the situation of one's own company (see Fig. 17). Across all groups, the highest values – i.e. the highest opportunity assessment of a data sharing obligation – are achieved for the areas of popularity[244] of my company, innovation activity and cooperation with

[244] Meaning 'Bekanntheit'.

other companies. In contrast, the companies see a greater risk in the areas of security of their own data, company know-how and company success.

Overall, the companies confirm their rather cautious attitude with regard to a legal obligation to disclose data: the most frequently chosen answer option is ‘both risk and opportunity’ or ‘rather risk’. The companies’ answers to this question are relatively homogeneous. Only large companies have clearly different responses: whereas all other groups of companies give the criteria of ‘popularity of my company’, the two thirds of the large companies see the greatest opportunities in the area of cooperation with other companies.

Fig. 17: Assessment of a hypothetical obligation to share data depending on specific conditions, n = between 403 and 448



Source: IW-/IWC-Unternehmensbefragung Datenökonomie, 2020,
IW (2020): Datenwirtschaft in Deutschland - Wo stehen die Unternehmen in der Datennutzung und was sind ihre größten Hemmnisse?, p. 33.

cc) Study on the use of B2B platforms

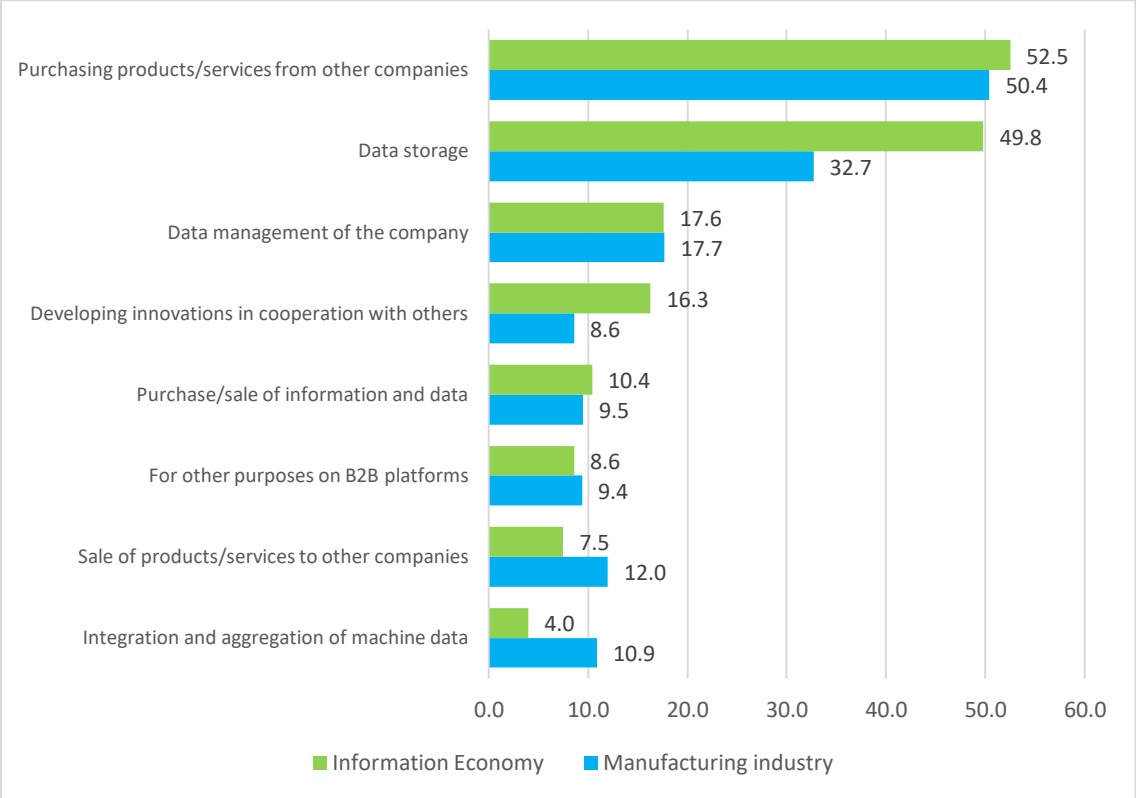
The following findings are based on a company survey, conducted by ZEW within the framework of the ZEW Business Survey.[245] Companies are regularly surveyed with at least five employees in the information and communication technologies (ICT, consisting of ICT hardware and ICT services), media services and knowledge-intensive services (legal and tax consultancy, auditing, public relations and management consulting, architectural and engineering activities, technical, physical and chemical analysis, research and development, advertising and market research and other freelance, scientific and technical activities). All of the above industries together form the information economy.

[245] In the following we present a reduced and modified version of the English translation of the results of EFI, Jahresgutachten 2022, p. 80-93 with reference to ZEW, Konjunkturumfrage Informationswirtschaft 3. Quartal 2021.

The survey was expanded to include the manufacturing industry. This includes the sub-sectors of chemicals and pharmaceuticals, mechanical engineering, vehicle construction and other manufacturing industry. The survey was conducted in September 2021 within the framework of a combined and online-based survey. Overall the extrapolated results are based on 730 usable responses from the information industry and 455 responses from the manufacturing industry. In order to ensure the representativeness of the analyses, the responses of the survey participants were extrapolated to the number of all companies in the industries surveyed.[246]

The survey reveals that around one in ten companies in the information economy and manufacturing industry are active in data marketplaces. Less than 5% of the companies in the in the information economy and slightly more than 10% of the companies in the manufacturing sector currently use B2B platforms for the purpose of integrating and aggregating of machine data.

Fig. 18: Purpose of the use of digital platforms in the B2B sector

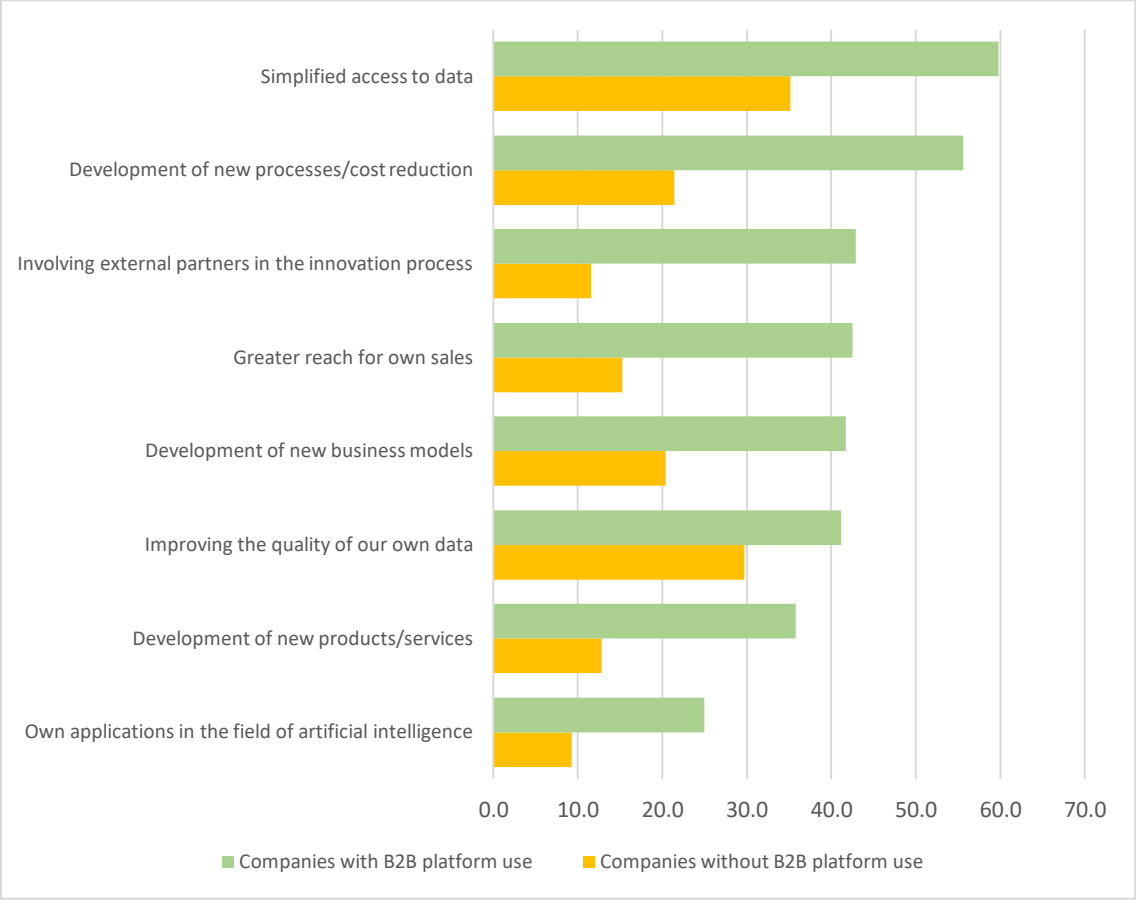


Source: ZEW Konjunkturumfrage Informationswirtschaft 3. Quartal 2021.

[246] For further information on the ZEW Business Survey see https://www.zew.de/en/publications/zew-expertises-research-reports/research-reports/information-economy/zew-branchenreport-informationswirtschaft (last visited 4.7.2022).

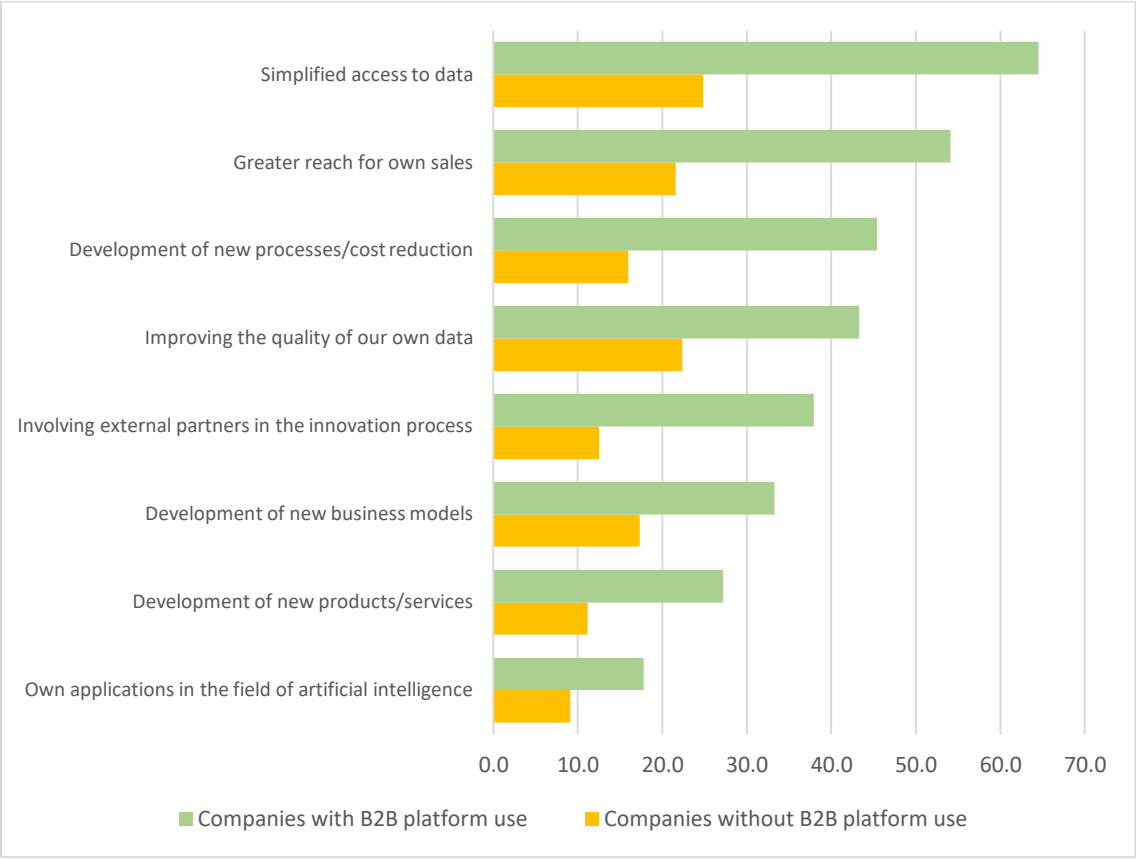
In the survey conducted, the companies were asked about the positive or potentially positive effects of the B2B platform use on innovation activities and innovation-relevant factors (Fig. 19 and 20). The simplified access to data is seen as the most important advantage both in the information economy as well as in the manufacturing industry. Companies that use the platform rate simplified access to data positively more often than companies that do not. At platform-using companies in the information economy, they are followed in second and third place by the development of new processes or cost reductions and the integration of external partners in the innovation process. In the manufacturing sector, companies that use platforms have a greater reach for their own sales and the sales and the development of new processes or cost reductions take these positions.

Fig. 19: Impact of the use of digital B2B platforms on companies in the information economy



Source: ZEW Konjunkturumfrage Informationswirtschaft 3. Quartal 2021.

Fig. 20: Impact of the use of digital B2B platforms on companies in the manufacturing industry

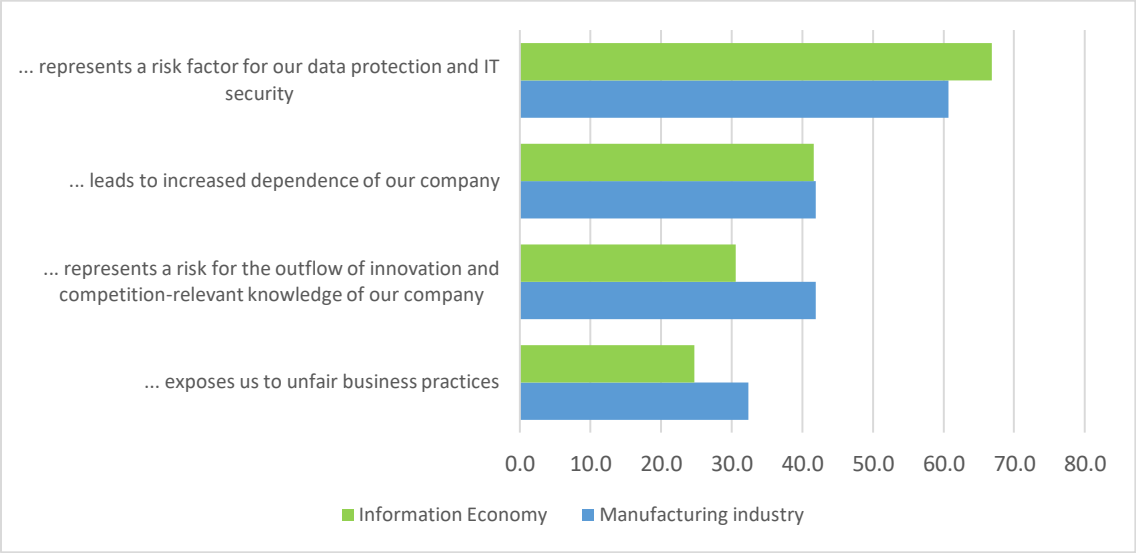


Source: ZEW Konjunkturumfrage Informationswirtschaft 3. Quartal 2021.
© EFI - Expertenkommission Forschung und Innovation 2022, p. 86.

The use of B2B platforms comes with positive effects, but also with various risks. Around two thirds of companies in the information economy and slightly more than 60% of companies in the manufacturing sector refer to risks for data protection and IT security. Another threat, expressed by more than 40% of companies in manufacturing and 30% of companies in the information economy, is the outflow of knowledge relevant to innovation and competition. This assessment points to the central importance of mutual trust between platform actors. The joint operation of a B2B platform could solve the trust problem of companies in platform use. In so-called joint platforms with companies being platform operators and users at the same time, they jointly decide on governance structures, the design of algorithms and data usage rules and can adapt these to their needs.

According to more than 40% of companies in the information economy and in manufacturing respectively, increased dependence of the company on the platform also represents a risk when using digital B2B platforms. A lack of standards and compatibility as well as a lack of interoperability between platforms favour such dependency.

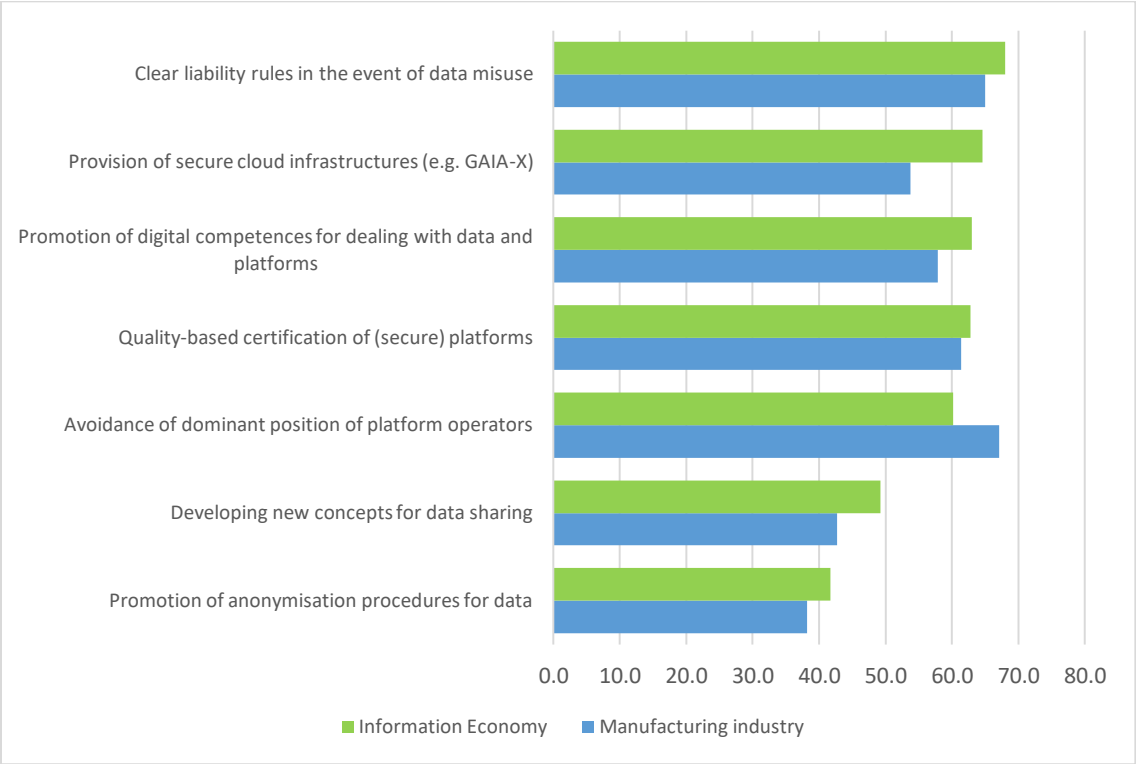
Fig. 21: The use of digital B2B platforms



Source: ZEW Konjunkturumfrage Informationswirtschaft 3. Quartal 2021.

The companies rate various possible governmental measures in relation to B2B platforms as promoting innovation. More than half of the companies in the information economy and manufacturing sector state that their innovation activities would benefit from clear liability rules in the event of data misuse, the provision of secure cloud infrastructures and the promotion of digital skills for handling data and platforms. In addition, quality-based certification of (secure) platforms and the avoidance of a dominant position of platform operators would benefit companies' innovation activities. A slightly smaller share of companies expects positive effects on their own innovation activities through the development of new market dominance concepts for data sharing and the promotion of anonymisation procedures for data.

Fig. 22: Possible measures by the federal government in relation to B2B platforms that would benefit the innovation activity of companies



Source: ZEW Konjunkturumfrage Informationswirtschaft 3. Quartal 2021.
© EFI - Expertenkommission Forschung und Innovation 2022, p. 88.

c) Interviews

The insights gained from the surveys summarised above were broadly corroborated by a couple of interviews with industry representatives, ranging from representatives of large companies and industry associations to start-ups. Here, we summarise the main findings of the interviews that are relevant for the legal analysis that follows in parts E and F. The interviews support the finding that data sharing on a broader scale, in particular the establishment of data sharing ecosystems, is still only starting in Germany. However, it figures rather prominently in a number of sectors, including the automotive/mobility sector, the energy sector, Industry 4.0, the telecommunications sector and, partly, in the start-up scene.

Data sharing is already an important topic in the automotive/mobility industry. Our interviewed car manufacturer outlined how access to their data is granted in a standardised format through APIs, with a latency between 30 seconds and 120 seconds plus trigger interval (e.g. ignition start or ignition end to commit data to the central systems). Among the stakeholders interested in access to data, the insurance sector is among the forerunners. Where car data that qualifies as ‘personal data’ under the GDPR is transmitted to third parties, the consent of the car owner is required. Furthermore, car companies will only be willing to pass on data if they know why it is needed; i.e. they strive to maintain a rather high degree of control. In the same vein, a trend

in many areas of activity is not to grant access to data to third parties, but to keep the data '*in situ'*, merely run the third-party algorithm on the data and provide the third party with the results.

Data protection regulation is named as the most important barrier to data sharing. A more recent evolution in the car-related data economy is pushing data from the vehicle to the cloud. Furthermore, edge analytics plays a role, i.e. performing certain forms of data analytics in the car. Obviously, a lot of investment goes into data security.

In the energy sector – a rather traditional industry and also a critical infrastructure – there is initial caution surrounding data access and data sharing practices but due to legal obligations is nonetheless implemented to a certain extent. As a consequence, regulatory developments in these fields – including the Draft Data Act – are heavily debated. Opportunities are seen in an opening up for broader uses of data, including the sharing of data: the combination of standardised data from different sources could allow for the development of new services.

On the other hand, representatives from a major German OEM and supplier of Industry 4.0 components and automotive parts cautioned against more pro-active access-to-data regulation. Although they may at times be a beneficiary of the proposed new data access rights as proposed by the Draft Data Act, they warn that such regulation might kill innovation. According to them, it would be preferable to await the experience gained with the application of competition law to data-related practices. A cautious opening up of specific types of data – such as repair or maintenance data – may be preferable to an all-encompassing approach.

Representatives from another large German company also heavily involved in Industry 4.0 explain that they mainly deal with machine or industrial data and work within a B2B environment. Even though they are the manufacturer and might be able to access the data, the control of the data generated by the machines would mostly lie with their customers – contrary to what is frequently presumed, including by the Draft Data Act. Furthermore, the customers would view the raw data as their own, but the manufacturer might consider some of the derived and aggregated data as theirs. Similar to the car industry, the trend goes towards storing mission critical data on small servers on the premises of the customer (edge computing). Only those data that do not need to be processed in real time are stored in the cloud. On a voluntary basis, the manufacturer offers to provide predictive maintenance and analytics services to the customer. Industrial customers are very much aware of the sensitivity of their data, however. There is no unequal bargaining power that would favour the manufacturer in these settings. Also, contrary to the business models of B2C platforms or app providers, these business models are not scalable to the same extent, and they do not lend themselves to a 'tipping' of markets. Rather, every plant is different. For these reasons, the representatives of this company do not see a case for regulating data access in the B2B industrial arena, and they are concerned that the debate on data access and data sharing is too much driven by B2C settings which tends towards concentration and asymmetries of power. Indeed, they state that mandating access to data would undermine their costumers' trust as well as willingness to share their data especially if control over it is lost. They do advocate for open standards and open interfaces, and usually

use international standards released by IEC. They support and await the deployment of a reliable 5G network that allows for secure data flows in large quantities in real time.

A lawyer focused on IT and data law for the past 25 years, and whose legal team was, among other things, involved in the development of the GAIA-X project, explained that the largest barrier to data sharing is finding the suitable governance structure. Sharing data may mean sharing one of the most important assets a company may have. Hence, the question of what the preconditions for a data sharing should be, which party shall be endowed with which rights and what may be done with the results of data analytics after different datasets have been combined must be given a lot of thought.

A representative from a major German telecommunications services provider explains that his company controls large amounts of communications data. Given the constraints imposed by certain laws, most importantly the e-privacy-Directive, data sharing is not a business model for the company. Dealing with pseudonymised personal mobile location data would be seen as the most attractive and reasonable way forward. But under the current legal framework, this is not a viable option: in order for the company to be able to process and/or share communications meta data, such data would need to be anonymised, or consent would need to be given.

3. Empirical insights: a summary

Synthesizing the insights from our searches in large company databases and the three empirical studies as well as the interviews, we come to the following conclusions in relation to the existence and role of data sharing in Germany:

Firstly, there are only a few and mainly large companies who consider data sharing as relevant for their business model. In particular, the number of companies serving as data providers is very small, where more companies characterise themselves as data recipient. However, less than half of the companies express a need for external data, which is mainly related to products and less to processes. Digital B2B platforms are used to purchasing or selling data. However, the majority of companies see no option to share data at all.

Secondly, the barriers to sharing data are in general of legal and less of organisational, technical or economic nature. Economic barriers follow from rather unclear benefits, but also from a lack of capacity. The legal problems are related to privacy and data protection issues, the accessibility of the data as well as liability risks that data sharing might generate. Further risks are related to cybersecurity concerns, unintended knowledge spill-overs and unfair practices by other businesses.

From the interviews we ascertained that the perception of mandating data sharing varies significantly depending on the stakeholder. Those companies that have the data or access to it already generally argue and warn against it. The argument being particularly with the case of B2B industrial data, that mandating data sharing would lead to their clients ultimately not providing their data. Other stakeholders though see mandating data sharing as an opportunity

to harmonise data sharing and increase the amount of available data creating further business opportunities. Further important features that came to the fore were firstly, that some stakeholders do not have the technical skills and knowledge with regards to working with data where some organisations that request data cannot actually concretely outline how it benefits the users. Secondly, that there are legal concerns such as compliance with the GDPR as well as how to navigate other horizontal data-related legislation on the horizon and where for example, pseudonymisation of data instead of the required anonymisation was preferred.

From the literature as well as the empirical analysis conducted in this study, the issues and barriers to data sharing can be outlined as either legal, technical or economic. These range from legal uncertainty to requiring a more comprehensive interoperable data sharing infrastructure (including standards) to stakeholder concerns regarding losing control of the data. Overall, what has been underlined is how vital current publicly supported initiatives such as GAIA-X are in already tackling these barriers and concerns, how legal clarity should be prioritised and where caution is recommended regarding initiating any further horizontal legislation that does not sufficiently consider differences among sectors and stakeholder interests. Moreover, the empirical evidence shows that the transformation of the German and European economy towards a data economy has only just begun. Data sharing is still an exception among German companies and time is required to see how the market develops.

IV. The role of the state in data-driven markets – addressing market failures and supporting the transformation

In the ongoing transformation towards a data economy, the German as well as the European legislator have to reconsider their role. A widening of possibilities for accessing and sharing data will be important for realizing the potential of the emerging data economy. The private value of data is often still less than its social value. A combination of datasets may significantly increase the benefits that can be drawn from data. In many areas, data is turning into an essential input to innovate.

A first and necessary step to remedy the current underuse of data is to understand what the reasons for this are. The empirical studies provide helpful insights into the economic, technical and legal reasons why many companies are reluctant to share data. The interviews give reason to think that, frequently, a much more detailed and sector-specific analysis will be needed to fully understand both the needs and hurdles for data sharing in a given area of activity.

The traditional market failure framework continues to be a good starting point for establishing where state intervention may be needed. The existence of data-related market power or cross-market power (partly paired with information asymmetries) is arguably the most important justification to impose obligations to grant access to data. We will look at the relevant legal framework more closely in part E.

When it comes to promoting the evolution of data-driven markets and innovation, the right approach may be less one of addressing well-defined market failures where markets do not yet

exist, or only *in nuce*. Rather, the various types of frictions may need to be addressed that stand in the way of the development of markets. The literature on innovation system failures advises us to turn our attention to possible dysfunctionalities of emerging markets beyond traditional market failure analysis.

In the light of such failures, the best approach may not be one of heavy-handed regulation, including general data access and sharing obligations, however. But rather one of the empowerment of the market: a clear and consistent basic legal infrastructure – on legal entitlements, contract and competition law – is needed. Consequently, public policy should focus on creating and shaping new markets rather early and should not limit itself to market fixing. Given such an early intervention and the lack of knowledge of which opportunities will arise and which direction may take, the pro-active intervention should not so much be about giving markets socially desirable directions, but enabling market actors to exploit the opportunities that may come with the sharing of the already available and further increasing data. Strong incentives for experimentation should be created.

Matching the market formation processes with the empirical evidence on the evolving data economy, and to data sharing in particular, it becomes obvious that the companies are still active in the first two processes, i.e. demand articulation and experimentation. The slow uptake of the data market may partly be caused by the poor articulation of the demand in the current early stages, which hampers the design of technological solutions for providing and sharing data. For policy makers, measures that help to anticipate future demand related to data sharing and to support its articulation may be appropriate.

Obviously, the challenge for companies is to adapt their strategies and processes to the opportunities of data sharing. The analysed surveys suggest that companies partly underestimate the benefits of data sharing. In this regard, measure to raise awareness of the benefits may be needed. Simultaneously, the complexity of data sharing increases where their practices are restricted by data protection rules and intellectual property rights, especially ‘sui generis’ database rights and trade secrets covering datasets. In this respect, a substantial amount of legal uncertainty persists (see part E).

A striking feature of the European data policy agenda is that, while companies are still striving to explore their demand and experiment with new practices, the European Commission is already about to form new institutions – e.g. with the Draft Data Act or the Data Governance Act. Given the limited knowledge on what directions markets will take, such an early intervention comes with risks. The surveys and feedback from company representatives raises doubt whether (some of) the attempts by the EU to establish a legal framework for data-driven markets do what they should do to promote the formation and re-formation of markets, namely reduce uncertainty for all market actors and stakeholders, create transparency, support directionality and foster (beneficial) interaction among stakeholders.

Comprehensive interventions, e.g. via regulations, require a profound understanding of the details of the market format processes – and one may be sceptical to what extent this state of

understanding has already been reached. In very complex markets characterised by a high level of uncertainty, regulatory sandboxes may be preferable and work as an appropriate discovery procedure for establishing the best allocation of rights or adequate rules for access to data. Due to the relevance of sector-specific framework conditions, it may be wiser to experiment first with sectoral legal frameworks before engaging in horizontal law-making.

Arguments in favour of a ‘market design’ approach should, therefore, be considered with a significant degree of caution: the basic principle remains that the market actors themselves should develop business models and come to private arrangements.

We shall further inquire into the appropriateness of the existing and emerging legal framework in supporting market formation and re-formation in part E and F of our study.

E. The current market order for data sharing

In this part, we lay out the existing legal framework regarding data control and data access. Well-functioning markets build up on a set of core legal institutions, namely well-defined (intellectual) property rights, contract law principles which combine default rules for incomplete contracts with mandatory provisions as reactions to market failures and competition law principles which protected markets from anticompetitive agreements of undertakings and abusive practices of dominant undertakings. In accordance with this approach, we examine (I.) the existence and allocation of (intellectual) property or other exclusive rights on data, then (II.) explore the current contract law framework before we provide, in accordance with the research assignment of the BMWK, (III.-V.) a more detailed analysis of the different competition law instruments.

The description of the rules cannot be comprehensive, and in several areas of the law, significant reform processes are ongoing. These are explored later in the part F. The aim of this part is to identify the strengths and weaknesses of the existing legal infrastructure for the emerging data markets. Does it provide for a sufficiently stable and robust basis for data-related transactions? Do the various pillars form a coherent whole? Which potential market failures does the legal framework react to, and does it do so effectively?

I. Intellectual property and ownership of data

Clearly defined property rights are generally considered to be essential for well-functioning markets to evolve. Given the intangible, non-rivalrous nature of data, it is not obvious that anything akin to traditional property rights as they exist for moveables or real estate has emerged or would be needed. On a descriptive level, we should ask whether intellectual property or similar exclusive rights of data holders have taken shape in the emerging data markets. And on a normative level, we have to inquire whether the existing legal framework is functional or dysfunctional.

Databases or datasets may indeed be protected by various exclusive rights or merely factual access barriers. These exclusive positions of the holder of the database may be used to prevent third parties to access the database and protect the data holder's investment. As such, they seem to contradict any policy that promotes broader access to datasets. However, intellectual property and other legal or de facto exclusive positions may also serve as the basis of contractual arrangements between the holder of the protected information and other parties who seek access.[247] From this perspective, intellectual property rights may foster legal certainty and

[247] This basic function of intellectual property rights has been described e.g. by Kitch J Law Econ 1977, 265 (275 et seq.); Shavell, Foundations of Economic Analysis of Law, 2004. More specific on datasets see Drexl JIPITEC 2017, 257 paras. 81 et seq.

facilitate access to data. Depending on the willingness of the data holder to share these assets, intellectual property rights may ease their transfer – or may cause blocking effects.

In the following section, the various relevant exclusive rights or positions are further explored.

1. No specific 'ownership right' on data

After some years of discussion both at the European[248] and the national level[249], it has become the broad mainstream opinion both by policy makers and academics, that data or datasets should not be protected by any additional new and tailor-made property or ownership rights. Property rights on intangible goods, like datasets, should only be introduced on the basis of a clear evidence for market failure with regard to the creation of respective goods. The dearth of data sharing initiatives, in particular when it comes to collections of personal data, is not due to an insufficient quantity of data collection but rather to the lack of business models making use of the existing datasets and the lack of willingness of data holders to enter into access agreements. Therefore, the focus of the debate has shifted from property to access.[250]

2. Copyright and 'sui generis' protection of databases

Data sets may be protected as databases in the sense of the Database Directive 96/9/EC.[251] According to Article 1(2), a 'database' shall mean a collection of independent works, data or other materials arranged in a systematic or methodical way and individually accessible by electronic or other means. Most datasets that have been created for a commercial purpose will meet these basic requirements. In its *Esterbauer* decision of 2015, the CJEU followed an extensive interpretation of the definition of a database. The court stated that even geographical information extracted from a topographic map contains sufficient informative value to be classified as 'independent materials' of a 'database' within the meaning of Article 1(2).[252] However, for being protected by copyright law in accordance with Article 3 or under the so called 'sui generis' protection of Article 7, they must fulfil additional requirements.

Fully-fledged copyright protection under Article 3(1) is granted for databases which, by reason of the selection or arrangement of their contents, constitute the author's own intellectual creation. The database must be original in the sense that its author expresses his creative ability

[248] Earlier statements of the Commission considered the introduction of a 'data producer's right', see COM(2017) 9 final, 13.

[249] See Koalitionsvertrag zwischen CDU, CSU und SPD, 19. Legislaturperiode, 2018, p. 129. See also Amstutz AcP 218 (2018), 438; Fezer, Repräsentatives Dateneigentum, 2018.

[250] See for the majority of commentators Becker ZGE 2017, 253; Drexl et al. GRUR Int. 2016, 914; Specht CR 2016, 288 with further references. For an economic analysis see Kerber GRUR Int. 2016, 989.

[251] OJ 1996 L 77, 20.

[252] Case C-490/14, *Verlag Esterbauer*, ECLI:EU:C:2015:735, para. 29.

by making free and creative choices and "thus stamps his personal touch".[253] This will only apply in exceptional cases.[254]

Of far greater importance is the 'sui generis' protection according to Article 7. Article 7 is not based on the concept of originality but requires instead "that there has been qualitatively and/or quantitatively a substantial investment in either the obtaining, verification or presentation of the contents." The CJEU in the case *British Horseracing Board*, however, made clear that Article 7 must be understood to refer to the resources used to seek out existing independent materials and collect them in the database. It does not cover the resources used for the creation of materials which make up the contents of a database.[255] This restrictive interpretation has led the European Commission to the conclusion that the 'sui generis' right will not apply, if the investment was primarily spent for sensors or devices collecting data.[256] Such an interpretation would limit the scope of application of the 'sui generis' right noticeably and exclude many sets of machine data. But the European Commission's interpretation is controversial. Some commentators argue that machine data is pre-existent and investments in sensors are covered by the 'obtaining' proviso.[257] At the end, different approaches may apply for different categories of datasets with possible overlaps. Neither would it be accurate to say that all datasets are covered by a 'sui generis' right nor the opposite that no collection of machine or personal data is protected. What follows is considerable legal uncertainty.[258]

Further uncertainties may arise with regard to the ownership of database rights. Article 7 Database Directive allocates ownership to the 'maker' of the database. Recital 41 defines the maker as the person "who takes the initiative and the risk of investing". The allocation of rights does not pose specific problems in situations with only one party investing in the creation of the database. More difficult are cases of 'co-generated' data, if e.g. the aircraft manufacturer is investing in sensors and processors creating a dataset and the airline operating the aircraft is paying for the technology embedded in the aircraft and for the maintenance. The CJEU has not yet decided about the allocation of rights in the case of multiple investors.

Furthermore, the relationship between multiple investors is not settled in the Directive or in the German implementing legislation (§ 87b UrhG). The provisions on 'joint authorship' in § 8 UrhG are not applicable to the 'sui generis' database right. One could either refer to them by analogous application or apply general principles of the law of corporations, e.g. by applying

[253] Case C-604/10, *Football Dataco/Yahoo! UK*, ECLI:EU:C:2012:115, para. 38.

[254] Leistner/Antoine/Sagstetter, Big Data, 2021.

[255] Case C-203/02, *British Horseracing Board/William Hill*, ECLI:EU:C:2004:695, Ruling 1.

[256] COM SWD(2018) 146 final, 35 and 40. See also Drexl JIPITEC 2017, 257 para. 47.

[257] Leistner/Antoine/Sagstetter, Big Data, 2021.

[258] See also *European Commission* (ed): Study in support of the evaluation of Directive 96/9/EC on the legal protection of databases, 2018, p. 110 et seq., which illustrates the diverging approaches of the judicature across the Member States.

the rules on partnerships in §§ 705 et seq. BGB or on co-ownership in §§ 741 et seq. BGB,[259] depending on the modalities of their interaction. Depending on the specific relationship of multiple investors, such a joint ownership could serve as a basis for mutual rights and duties including possible access rights of the parties who are excluded from de facto control of the dataset. The basis for such a claim may be contractual if the parties come to an agreement.[260] But the general principles on co-ownership may also apply without a contract. For third parties interested in access, the unclear allocation of ownership and possible conflicts between co-owners may result in blockade.

The 'sui generis' database right protects the database, not single entries as such. Therefore, according to Article 7(1), only an "extraction and/or re-utilization of the whole or of a substantial part, evaluated qualitatively and/or quantitatively, of the contents of that database" amounts to an infringement of the right. The extraction of single data, smaller datasets or derived information (e.g. analytics) does not automatically interfere with the database right.[261]

In June 2021, the CJEU rendered the *CV-Online Latvia* decision, which further cuts back 'sui generis' protection to some extent. By referring to the *ratio legis*, the CJEU stipulated an unwritten requirement, according to which the 'sui generis' right only prohibits extractions and re-use of the database if the acts in question adversely affect the maker's investment in the obtaining, verification or presentation of the database content.[262] This means "that they constitute a risk to the possibility of redeeming that investment through the normal operation of the database in question".[263] Since the CJEU allows for balancing of various interests within this test, the *CV-Online Latvia* decision increases the legal uncertainty as regards the scope of protection with regard to machine-generated data.

Furthermore, statutory limitations and exceptions to the 'sui generis' right may justify extractions from the database. Article 9 Database Directive provides a list of limitations and exceptions most of which will not be of significant importance in the access scenarios discussed in this report, in particular (a) "extraction for private purposes of the contents of a non-electronic database", (b) "in the case of extraction for the purposes of illustration for teaching or scientific research", and (c) "extraction and/or re-utilization for the purposes of public security or an administrative or judicial procedure". The recently introduced exception for text and data mining in Article 4 of the Digital Single Market Directive 2019/790/EU, implemented in §§ 87c(1)(4), 44b UrhG, could play a more important role in the future.[264] According to the provisions, text and data mining may be legal without the consent of the rightholder even for commercial purposes. Recital 8 of the Digital Single Market Directive describes text and data

[259] Dreier in Dreier/Schulze, Urheberrechtsgesetz, 6th ed. 2018, § 87a para. 20; Vogel in Schricker/Loewenheim, Urheberrecht, 6th ed. 2020, § 87a para. 75.

[260] See Leistner/Antoine/Sagstetter, Big Data, Tübingen, p. 88-90.

[261] Drexl JIPITEC 2017, 257 para. 48.

[262] Case C-762/19, *CV-Online Latvia*, ECLI:EU:C:2021:434, para. 47.

[263] Ibid.

[264] OJ 2019 L 130, 92.

mining as "automated computational analysis of information in digital form, such as text, sounds, images or data", "which makes the processing of large amounts of information with a view to gaining new knowledge and discovering new trends possible". This could justify efforts by third parties to analyse a database without the consent of the rightholder, e.g. by systematic request schemes, training of artificial intelligence instances etc.[265] Anyhow, as an exception or limitation, Article 4 does not grant a claim against the rightholder to grant access. Moreover, according to Article 4(3), the rightholder may reserve the right of text and data mining "in an appropriate manner, such as machine-readable means in the case of content made publicly available online".

The current reform agenda of the European Union could result in a change of the protection of 'sui generis' databases. According to Article 35 of the Draft Data Act, the 'sui generis' right provided for in Article 7 Database Directive cannot be invoked for databases containing data obtained from or generated by a product or related service to hinder the effective exercise of the access right or of the right to make data available provided for in the Draft Data Act. It will be explored later in this report whether a weakening of the database producers' legal position is the appropriate means to facilitate data access.

3. Protection of datasets as trade secret

Datasets may be protected as trade secrets under the provisions of the Trade Secret Directive 2016/943/EU.[266] The protection of a database under the Directive 96/9/EC[267] does not pre-empt the application of the Trade Secret Directive. Both legal titles may overlap.

According to Article 2(1) Trade Secret Directive, a 'trade secret' means information that (a) "is secret in the sense that it is not, as a body or in the precise configuration and assembly of its components, generally known among or readily accessible to persons within the circles that normally deal with the kind of information in question", (b) "has commercial value because it is secret", and (c) "it has been subject to reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret". Many datasets of commercial interest will meet these requirements.[268] A typical data collection or dataset is either kept secret and technically locked up on the servers of the person controlling the data (if not sourced out on servers of other providers) or it is stored and embedded into devices or machines where only the controller can access the data. Such datasets are not generally known to persons active in the field, have commercial value and are technically (and legally) protected against unsolicited access by third parties. Of course, a definite evaluation depends on the characteristics of the dataset in question. Difficulties may arise with the determination of the 'holder' of the trade secret. According to Article 2(2) of the Trade Secret Directive, 'trade secret holder' means "any

[265] Meys GRUR Int. 2020, 457; Raue ZUM 2021, 793.

[266] OJ 2016 L 157, 1.

[267] OJ 1996 L 77, 20,

[268] Drexl JIPITEC 2017, 257 paras. 51-56; Leistner/Antoine/Sagstetter, Big Data, 2021, p. 138-151; Wiebe/Schur GRUR Int. 2019, 746 (747-751).

natural or legal person lawfully controlling a trade secret". The German implementation takes up the very same wording in § 2(2) GeschGehG. If only one party is involved in the creation of the datasets and controls it de facto, then the allocation of trade secret is straightforward. 'Lawfully' in this regard refers to the violation of trade secrets of other parties, not to other legal requirements like e.g. data protection law.[269] However, the creation of datasets may also involve contributions of different parties, e.g. one party producing the machine and the sensors and another party operating and maintaining the machine.[270] Neither the Directive nor the German act contain rules on co-ownership of several contributors. Commentators refer to the parties to necessary contractual agreements.[271] But without a contractual agreement, the party with de facto control will be in a favourable situation. Here again, the general private law principles of co-ownership could be used as a model at least for cases without a contractual arrangement. For the time being, all parties involved in the database creation as well as third parties interested in access must live with legal uncertainty.

Trade secrets are protected against 'unlawful' acquisition, use or disclosure, see Article 4(1) of the Trade Secrets Directive and § 4(1) GeschGehG. By contrast, any lawful acquisition in accordance with Article 3 of the Trade Secret Directive and § 3 GeschGehGmay not be prohibited. Lawful acquisition comprises (a) independent discovery or creation, (b) observation, study, disassembly or testing of a product or object that has been made available to the public or that is lawfully in the possession of the acquirer of the information who is free from any legally valid duty to limit the acquisition of the trade secret, (c) exercise of the right of workers or workers' representatives and (d) any other practice which, under the circumstances, is in conformity with honest commercial practices. In sum, third parties may plead on the basis of different legal grounds why their acquisition of data taken from a database does not violate the trade secret. If none of the ground for lawful acquisition is applicable, their conduct may still be justified by one the exceptions listed in Article 5 and § 5, e.g. for exercising the right to freedom of expression and information or for the purpose of protecting a legitimate interest recognised by European Union or Member States' law. It has rightly been said that trade secret protection in the sense of the Directive should not be equated with intellectual property protection.[272] The position of the holder of a trade secret is less exclusive.[273] Yet, both in the case of lawful acquisition and exceptions, third parties may be justified to access and use the secret information, but they may not request that the right holder supplies any data or grants access.

Trade secrets may be the subject matter of license contracts. Such contracts are daily practice in different areas of technology. Disclosure of the trade secret in the framework of a bilateral contractual relationship and the granting of a permission to the licensee to use the trade secret

[269] Alexander in Köhler/Bornkamm/Feddersen, UWG, 40th ed. 2022, § 2 GeschGehG para. 99-103.

[270] Ohly GRUR Int. 2019, 441 (445).

[271] Leistner/Antoine/Sagstetter, Big Data, 2021, p. 157-159.

[272] Ohly GRUR Int. 2019, 441 (445).

[273] See Recital 16: 'In the interest of innovation and to foster competition, the provisions of this Directive should not create any exclusive right to know-how or information protected as trade secrets.'

does not take away the 'secret' character from the respective information. Availability for a specific party does not as such make the secret public knowledge in the sense of Article 2(1)(a) of the Directive.[274] This is even more true if only derived information is disclosed to the contracting party and not a secret dataset as such. Still, a license contract may entail the risk that the trade secret is further distributed by the licensee which could finally endanger its status as a secret. The Trade Secret Directive provides a two-tier protection mechanism against such a disclosure. First, according to Article 4(3)(b), any use in contradiction to a confidentiality agreement or any other duty not to disclose the trade secret is considered as unlawful acquisition. Second, according to Article 4(4), any use by a third party which at the time of the acquisition, use or disclosure, knew or ought, under the circumstances, to have known that the trade secret had been obtained directly or indirectly from another person who was using or disclosing the trade secret unlawfully is also considered as unlawful. This protection against third parties acting in bad faith does not grant the same level of 'absolute' protection as it is characteristic for intellectual property rights. But it does at least establish a limited third party effect.[275] Despite the legal risks associated with contracts, trade secrets do still provide a more solid basis for a license contract than a mere de facto exclusivity where the holder of a dataset can only rely on technical mechanisms and contractual remedies in case of a breach of confidentiality.

The Draft Data Act acknowledges that sets of machine-generated data may be protected as trade secrets of the data holder.[276] Such trade secrets shall not be affected by the access rights of users as provided for in the Draft Data Act. The Draft Data Act tries to avoid any public disclosure of trade secrets by defining obligations of users in Article 4(3): Trade secrets shall only be disclosed to the user provided that all specific necessary measures are taken by the user to preserve the confidentiality of the trade secret especially in relation to third parties. The data holder can agree with the user on measures to preserve the confidentiality of the shared data, in particular in relation to third parties. Similar rules apply to third parties under Article 5(8). The 'Data Act – Impact Assessment' mentions a 'study on the legal protection of trade secrets in the context of the data economy' which has not been published yet.[277]

4. Personal data

If the dataset contains personal data, the requirements of the GDPR with regard to access and processing of data have to be taken into account. In the past, the CJEU has applied a broad concept of personal data. According to the *Breyer* decision[278], a person is 'identifiable' even if the holder or processor of the data in question cannot determine the identity of the data subject but only a third party is able to so. Such an approach, if strictly applied, could result in an

[274] Alexander in Köhler/Bornkamm/Feddersen, UWG, 40th ed. 2022, § 2 GeschGehG para. 34.

[275] Ohly GRUR Int. 2019, 441 (446-447).

[276] Recital 28.

[277] COM SWD(2022) 34 final, 84.

[278] Case C-582/14, *Breyer*, ECLI:EU:C:2016:779.

application of the GDPR to data collected by land machines or aircrafts as long as the farmer operating the machine or the crew of the aircraft are identifiable by any third party. The CJEU in *Breyer*, however, left open a backdoor to avoid overly extreme interpretations. Not any theoretical possible but practically unlikely combination of data controlled by different parties should be considered as being sufficient for making a person 'identifiable'. According to the CJEU, it must be determined whether the possibility to combine different information held by different parties "constitutes a means likely reasonably to be used to identify the data subject".[279] The GDPR also makes use of the 'reasonableness' test in Recital 26. Even though controversial, this line of argument could pave the way out of an overly extensive interpretation of 'personal data'. Still, the question is not as trivial as suggested by the 'Data Act – Impact Assessment' which seems to exclude machine generated data per se from the application of the GDPR.[280] The division of sets of data between different parties, which qualifies as personal data only if combined, may be of practical relevance in scenarios where access to machine-generated data is in question, e.g. if the owner of a rental car fleet requests access to vehicle data from the manufacturer which cannot be used by the manufacturer to identify the driver but which may turn out to be personal data if combined by the rental car service with the driver's name. In such a scenario, a combination of data will be reasonable for car rental services if they are interested in a driver's profiles.

If machine-generated data is 'personal' in the moment it is collected, the data holder may have an interest to anonymise such data in order to facilitate its further processing and sharing. The GDPR recognises the possibility of such an anonymisation. According to Recital 26 sentence 5 "the principles of data protection should therefore not apply to (...) personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable." The GDPR does not require that a 'deanonymisation' is technically impossible in the future. It suffices that such a deanonymisation would require the use of unreasonable efforts and means so that it cannot be expected under the current and the predicted future state of technology.[281] When determining the standard of reasonableness, both the actual and obtainable knowledge and resources of the processor have to be taken into account.[282] In case of data sharing, a full anonymisation would presuppose that neither the (original) data holder nor the recipient have such resources and knowledge. If the (original) data holder can recombine the data and identify the data subjects, such processing and the transfer to the recipient will still require a legal justification under Article 6 GDPR. But the following processing by the recipient can be outside of the scope of the GDPR if the recombination with the (original) data holder's additional data is unlikely or unreasonable.

The GDPR does not prescribe a specific method for anonymisation. The Article 29 Working Party in its Opinion 5/2014 has analysed the effectiveness and limits of existing anonymisation

[279] Id., 45.

[280] COM SWD(2022) 34 final, 1.

[281] Roßnagel ZD 2021, 188 (189).

[282] Ibid.

techniques against the EU legal background of data protection, in particular anonymisation by deletion, generalisation or randomisation of attributes or a combination thereof.[283] The Opinion concluded "that anonymisation techniques can provide privacy guarantees and may be used to generate efficient anonymisation processes, but only if their application is engineered appropriately".[284] This holding is still valid.[285] However, the data holder has to live with uncertainty. The assessment of what is technically possible and reasonable for the data holder and recipient depends on a case-by-case analysis.[286]

Under the GDPR, any processing of personal data must have a clear legal basis. The processing of personal data is lawful under the GDPR if the data subject has given consent to the processing of the data, Article 6(1)(a), or if one of the other grounds for lawful processing in Article 6(1)(b)-(f) is fulfilled, especially if the data processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party. In legal practice, consent is of particular importance since it releases the controller from the uncertainties of the other legal grounds. At the same time, the consent requirement puts the data subject in the position to restrict or to allow the processing of their data. This resembles the exclusive nature of intellectual property rights but serves a different function, i.e. the protection of the fundamental right of protection of personal data.[287] But still, the consent requirement may be conceptualised as the consequence of the original allocation of a valuable legal position. This is relevant for contracts between the controller of the data and third parties. On the secondary market, where a holder of a dataset grants access to a third party, the consent of the data subject may be part of the contractual arrangement. If the holder of a set of personal data has obtained the consent of all data subjects concerned for a data transfer or other data access of third parties, then this 'rights clearance' of multiple consents may be a valuable part of the performance of the holder of the dataset, besides the mere de facto access.[288] Whether the 'licensor' of such a bundle of consents can put the 'licensee' in a legally watertight position depends on the scope and purpose of the consents gathered by the controller. Moreover, any consent can be withdrawn at any time in accordance with Article 7(3) GDPR.

In cases of co-generated data, difficulties may arise in determining the responsible controller who defines the purposes and means of the processing of personal data and is the potential contact person for a GDPR-compliant access request. According to Article 4(7) GDPR, multiple natural or legal persons can jointly exercise the control over personal data. Article 26 GDPR determines that such joint controllers should determine their responsibilities in a

[283] Article 29 Data Protection Working Party, Opinion 05/2014 on Anonymisation Techniques, 0829/14/EN WP216.

[284] Id., p. 3.

[285] For a more recent assessment see Klar/Kühling in Kühling/Buchner, DS-GVO BDSG, 3rd ed. 2020, Article 4 No. 1, paras. 31-34; Roßnagel ZD 2021, 188; Hansen in Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Article 4 No. 5 paras. 50-57,

[286] Article 29 Data Protection Working Party, Opinion 05/2014 on Anonymisation Techniques, 0829/14/EN WP216, p. 3-4.

[287] Specht GRUR Int. 2017, 1040 (1041 et seq.).

[288] Leistner/Antoine/Sagstetter, Big Data, 2021.

contractual arrangement between them. Different to what one would expect at first glance, 'joint control' of several actors for the same processing does not require each of them to have access to the personal data concerned.[289] Also, 'joint control' is not limited to cases where several controllers equally determine the scope and purpose of a processing operation. Instead, the concept is meant to cover also other kinds of 'pluralistic control' which may exist. In this perspective, 'jointly' has been interpreted as meaning 'together with' or 'not alone' in different forms and combinations.[290] If the operator of a website implements a social-media plug-in, e.g. a 'Facebook button', both the website operator and Facebook are 'joint controllers' in the sense of Article 26. As such, they are fully responsible for GDPR compliance and potentially liable for damages under Article 82 GDPR. This distributed responsibility is meant to enhance the data subject's legal situation but complicates the allocation of rights for further access requests of downstream users of the resulting datasets.[291]

In summary, even if interpreted as kind of allocation mechanism or exclusive right, the protection of personal data under the GDPR and the consent requirement rather impede access to data by downstream users than to facilitate it. This is not an unwanted side-effect but the very purpose of the GDPR. Recent instruments and initiatives, like the Digital Content Directive 2019/770,[292] the DGA[293] or the Draft Data Act seem to reflect a new trend in European data policy towards a more market-oriented approach. However, so far, they all repeat as a mantra that the provisions of the new instruments shall be without prejudice to the GDPR.

5. De facto exclusivity

Finally, if the dataset in question is not protected by any intellectual property or other exclusive legal position, the holder can still use the technical 'de facto exclusivity' and grant access only under defined contractual conditions. In this case, the de facto exclusivity is the bargaining chip in the hand of the holder of the dataset which allows him to take a strong position in contract negotiations. Nevertheless, the duties of the contracting party are still of a purely contractual nature. The stronger remedies of intellectual property or trade secret law will not apply. Moreover, third parties will not be bound due to the principle of privity of contracts.

If the holder of a dataset controls the technical access to the dataset and is at the same time owner of an intellectual property right or another exclusive legal position, then both the legal and the de facto exclusivity will be subject matters of a contractual arrangement granting access. More problematic are situations, in which the legal and the de facto exclusivity are controlled by different parties, e.g. one party has the technical control over a server and another party can claim a 'sui generis' right in the sense of Article 7 Database Directive. In this case, third parties seeking access may have problems to identify a possible licensor. And even if one of the parties is willing to permit access, the other party may still

[289] Case C-25/17, *Jehova's witnesses*, ECLI:EU:C:2018:551, para. 69.

[290] See Article 29 Data Protection Working Party, 00264/10/EN, WP 169, p. 18.

[291] Leistner/Antoine/Sagstetter, Big Data, 2021, p. 240-247.

[292] OJ 2019 L 136, 1.

[293] On the DGA see part part F(IV)(4) of the Study.

prevent such access legally or technically. Here again, legal uncertainty or splitting up of ownership may have detrimental effects for the functioning of data markets.

6. Deficiencies of the current legal framework

As shown, the existing legal framework does not provide for clearly defined (intellectual) property rights. Nonetheless, companies collect and store personal and machine data on a massive scale and control access by third parties with technical barriers. This de facto exclusive position, typically perceived by companies as legitimate 'ownership of data', apparently gives strong enough incentives to invest in further data collection and exploitation for internal use. Therefore, it has become a mainstream position that the legislature should not create new (intellectual) property rights for data which would further strengthen the position of data holders.

This well-founded reluctance to create new (intellectual) property rights, however, has the unintended side-effect that limitations and exceptions of the de facto ownership position of data holders are also underdeveloped to this date. The de facto ownership position of data holders is further reinforced by existing intellectual property rights or other legal exclusive positions which, in their current form, lead to legal uncertainties and are in the way of data sharing. Datasets may be protected by 'sui generis' database rights. It is however unclear which data collections at the end meet the requirements of Directive 96/9. Moreover, the allocation of rights in case of co-generation of data is not clearly defined and the existing provisions on the relationships of co-owners are underdeveloped. In addition, many datasets are protected as trade secrets. Here again, questions of allocation of rights may complicate data sharing. Limitations and exceptions both of 'sui generis' database rights and of trade secrets are without teeth because they only justify the use of data to which the user technically has already access whereas they do not help to get around technical barriers. As such, they further increase the risk for hold-ups. Finally, much of the collected data in datasets will be personal data in the sense of the GDPR which raises further legal uncertainties both for data holders and third parties who wish to access and use data collections. The combination of these different intellectual property or other exclusive de facto or legal positions is rather hampering than facilitating data sharing. All in all, it is largely dysfunctional.

II. Contract law for data sharing

1. Freedom of contract

Freedom of contract is one of the cornerstones of a market model. It is widely accepted as guiding principle for B2B contracts in the EU and beyond. Freedom of contract means that parties should be free to decide whether they want to conclude a contract, to choose their contracting partners and to agree freely on the terms of their contract. Modern contract law principles, especially in the EU, have attenuated the rigor of the liberal contract law model in different regards. Consumer protection and other policies (e.g. protection of employees,

commercial agents, authors or other weaker parties) have changed their character. The present European contract law is marked by mandatory provisions, information duties, correction mechanisms, default rules with regulatory objectives, procedural instruments and other kinds of rules which are meant to protect one contracting party from the other in asymmetric relationships. Still, at least for B2B contracts, every intervention into freedom of contract must either be justified by market failures or aim for an appropriate legal framework for the respective market with clear policy choices.

2. Obligation to contract

In light of the principle of freedom of contract, an owner of a dataset has the freedom to choose whether he wants to grant access to the dataset and to whom he wants to grant access. As a matter of principle, contract law does not force an owner of a dataset into a contractual relationship but provides rules for the conclusion and performance of contracts. However, if other legal grounds, e.g. fundamental rights, anti-discrimination laws, competition law, intellectual property ('compulsory license') or other regulatory law provide for such an obligation, contract law may be used for the handling of the details of the transaction, e.g. for the exact scope of access, the remuneration, non-disclosure of data, liabilities etc. Such obligations to contract have their justification in other areas of the law but make use of contract law on an operational level. This interplay of regulatory and contract law is also used by the Draft Data Act (see below in Part F(I)).

Closely related to contract-based claims are pre-contractual duties ('culpa in contrahendo') where parties enter into business contacts without having (yet) come to an agreement, § 311(2)(3) BGB. The 'Datenethikommission' suggested in its final report that § 311 BGB should be amended by an explicit provision which obliges data holders to enter into contract negotiations in certain cases of co-generation of data. This proposal has not been taken up so far by the legislature.[294]

3. Implied access rights based on traditional contract law principles

Once the parties have concluded an agreement, contract law principles may oblige the party controlling or owning a dataset to grant the other contracting party access to that dataset; such contractual access claims may be justified on the basis of implied terms or broad blanket norms like good faith and fair dealing, in Germany § 242 BGB.[295] German law is well known for its strong emphasis on the principle of good faith. German judiciary and doctrine have developed a variety of information duties and other implied secondary obligations of the parties to a contract. The concept of implied secondary obligation is today codified in § 241(2) BGB.

[294] Datenethikkommission, Gutachten, 2019, p. 147. See also Grünberger in German Federal Ministry of Justice and Consumer Protection/Max Planck Institute for Innovation and Competition, Data access, Consumer Interests and Public Welfare, 2021, p. 253 (255).

[295] See also Datenethikkommission, Gutachten, 2019, p. 146.

However, any of the duties of one party to disclose information to the other party to the contract are highly case-specific. Therefore, one might well expect that German courts would grant access rights in specific cases under the guiding principle of good faith. But this approach would certainly not lead to a general right of access and portability in B2B contracts. Also, information duties are not generally of a mandatory nature. Still, one could consider examples of access rights based on such general information duties. If, for example, the owner of an industry machine needs certain data for the maintenance of the machine one could consider such a right of access, at least in cases in which the producer does not offer maintenance services. Or a customer of a cloud service should certainly have a right to access the data and content stored on the cloud server during the contract and after its termination. The OLG München derived such a right of access as an implied term from the principle of good faith and obliged the service provider, after termination of the contract, to support the customer in the porting of its data to a different service provider.[296]

In sum, the traditional contract law principles do not provide for a general access right to data transmitted, created or observed by contracting parties, be it during the contractual relationship or after its termination. The existing information, access and return duties are case-specific and for the most part of a non-mandatory nature. They presuppose a contractual relationship between the parties[297] and additional special circumstances of 'good faith' etc., which may be given in some scenarios of co-generated data.

A related but less far-reaching approach is applied by the EU P2B-Regulation.[298] The P2B-Regulation does not set out a requirement to grant access to data in a contractual relationship, but it does establish transparency obligations for providers of online intermediation services. According to Article 9 P2B-Regulation, "[p]roviders of online intermediation services have to include in their terms and conditions a description of the technical and contractual access, or absence thereof, of business users to any personal data or other data, or both, which business users or consumers provide for the use of the online intermediation services concerned or which are generated through the provision of those services". The basic idea of the P2B-Regulation is to enable business users to constrain the intermediation services provider's access to data by switching to competing providers which offer more favourable terms. The limits to this approach show where business users are dependent on an intermediation service provider – this is here where competition law and gatekeeper regulation kick in (see below in part F(IV)).

4. Default rules

Neither EU law nor national German contract law provide specific default rules for data access.

[296] OLG München 22.4.1999, 6 U 1657/99 = CR 1999, 484.

[297] But see Grünberger in German Federal Ministry of Justice and Consumer Protection/Max Planck Institute for Innovation and Competition (eds.), Data access, Consumer Interests and Public Welfare, 2021, p. 255.

[298] OJ 2019 L 186, 57.

The European Commission has published a number of soft law instruments defining principles on data-sharing between businesses (B2B) and between businesses and governmental authorities (B2G) and describing different models of data sharing with a number of examples.[299] The principles presented in the instruments, 'transparency', 'shared value creation', 'respect for each other's commercial interests', 'undistorted competition', and 'minimised data lock-in', should indeed guide every contractual relationship. However, due to their very general nature, they may not be used as such as to fill gaps in incomplete contracts.

Even though German law does not contain specific contractual access rules, the more general principles of the civil code may still be used for complementing contracts. Depending on the concrete nature of the rights and duties of the parties to the contract, default rules from the specific contracts sections of the BGB may be applicable. According to § 667, in the case of a contract of mandate, "the mandatary is obliged to return to the mandator everything he receives to perform the mandate and what he obtains from carrying out the transaction." The concept of mandate (including paid management of the affairs of another, § 675) is broad and could also cover, e.g. escrow agreements or agreements on the data processing on behalf of a controller in the sense of Article 28(1) GDPR.[300] However, § 667 BGB can be waived. In the case of a contract on safekeeping, according to § 695, "the depositor may at any time demand that the thing deposited is returned, even if a period for safekeeping has been specified." It has been suggested that (at least certain) cloud service contracts be characterised as safekeeping contracts.[301] Such an obligation to 'return' the deposited asset could go beyond a mere duty to delete the data but could also comprise an obligation to transfer the data to the depositor. If the provisions on safekeeping contracts were applicable here, it would still be controversial whether the parties were allowed to exclude the right to claim for return according § 695.[302] Finally, rights and duties in case of termination of a contract could provide a basis for access claims. The basis for such claims could be found in the general contract termination rules, especially § 346(1) BGB, according to which in case of revocation, performances received are to be returned. This could justify a claim by one contracting party against the other contracting party to return data or content transmitted or collected during a contract, e.g. if a buyer of a machine revokes the contract after some months because of lack of conformity and requests access and transmission of valuable data collected and stored by the machine.[303] However, § 346 BGB can be modified and even excluded by the parties. And § 346 is not applicable in case of termination of a long-term contract. In this regard, a claim based on unjust enrichment in accordance with § 812(1)(1) could be considered.

---

[299] See COM(2018) 232 final and COM SWD(2018) 125 final.

[300] See for further example Strittmatter in Schuster/Grützmacher, IT-Recht Kommentar, 2020, § 675 BGB paras. 17-24. See for a client's access claim to data stored by a tax consultant BVerfG 11.32004, IX ZR 187/03 = NJW-RR 2004, 1290.

[301] See e.g. Henssler in MüKo BGB, 8th ed. 2020, § 688 para. 9; Koch ITRB 2001, 39 (42).

[302] See Henssler in MüKo BGB, § 695 para. 2 with further references.

[303] This would require characterizing the active provision of data by the buyer or the passive acceptance of data collection by the seller as the performance of an explicit or implied secondary obligation of the buyer under the contract, the value of which would then be returned in accordance with § 346(1), (2) BGB. On the application of § 346(1) BGB in case of provision of data as performance, see Metzger AcP 216 (2016), 861.

The Draft Data Act contains in Article 34 as one element 'model contract terms' for data sharing that shall be developed by the European Commission. It will be interesting to see whether these model terms will be comprehensive enough so serve as default rules. The ALI-ELI Principles for a Data Economy contain detailed rules for different kinds of data access contracts that could be used as a blueprint for the enactment of default rules.

5. Review of explicit access rights

If the parties have agreed that the owner or controller will grant access, contract law principles may impose mandatory provisions which require a review of the terms of the contract. In Germany, §§ 310(1), 307(1), (2) BGB provide a test of reasonableness for B2B standard terms and conditions. Other EU Member States apply the provisions of the Unfair Terms Directive 93/13/EEC[304] to contracts with small and medium-sized enterprises. This gives courts some leeway to enter into an analysis of the 'reasonableness' or 'fairness' of the conditions of standard data access contracts. However, courts will have difficulties to determine what fairness means in this regard given the sparse knowledge about what 'reasonable parties' would agree upon. The default rules cited above may provide some criteria, but legal practice is still far from having established clear rules. Moreover, review of standard terms under the cited provisions does not justify a price control by judges.[305] For individually negotiated contracts, only extremely unbalanced contracts may be reviewed under general contract law principles, like good faith and fair dealing, in Germany § 242 BGB, or public policy, § 138 BGB. In B2B scenarios, these principles are reserved for extreme cases. One should keep in mind that the B2B contracts in question are not characterised by a structural imbalance, like e.g. employer-employee, trader-consumer, landlord-tenant or publisher-author relationships.[306] Therefore courts will be cautious to interfere with the freedom of contract in cases in which big and small companies conclude contracts, as long as the imbalance does not reach the thresholds of dominance in competition law or of a gatekeeper status under the DMA. The mere imbalance of power does not per se justify state intervention.[307] Nor would a difference in size between the parties justify intervention. However, the Draft Data Act aims to establish a review of standard terms of data access contracts that are unilaterally imposed on micro, small and medium-sized enterprises, Article 13.

6. Deficiencies of the current legal framework

[304] OJ 1994 L 95, 29.

[305] Article 4(2) Unfair Terms Directive.

[306] The argument of structural imbalance is used in German contract law to justify regulatory intervention in the mentioned areas; in this regard see the contributions of Calliess, Kocher and Riesenhuber in Möslein (ed.), Private Macht, 2016, p. 193. From the older literature see Fastrich, Richterliche Inhaltskontrolle im Privatrecht, 1992, p. 159-201, 216-21; Hönn, Kompensation gestörter Vertragsparität, 1982, 153-160.

[307] See in this regard the apparent caution of leading law and economics handbooks, e.g. Posner, Economic Analysis of Law, 9th ed. 2014, p. 127-28; Schäfer/Ott, Lehrbuch der ökonomischen Analyse des Zivilrechts, 5th ed. 2012, p. 487-90.

Contract law should fulfil two main functions for the legal framework of data access and data sharing which overlap to some extent. First, contract law should provide default rules and, where market failures are established, also mandatory standards if the parties have voluntarily concluded a contract under which one of the parties can technically control access to data provided by the other party or generated by its observation. Contract law should clarify if and under which conditions this other party can access such data. In the existing legal framework, the contract law principles are not sufficiently developed to fulfil this function. Even though traditional principles of law like good faith and fair dealing may be used to develop certain rights and obligations of the parties with regard to such data, the legal framework is far from being clear.

Secondly, contract law should also provide default rules and, where necessary, mandatory standards if other, non-contractual legal grounds, especially competition law or regulatory law, impose a right to access data and refer to contract law for the handling of such access rights. The Draft Data Act, once adopted, will provide a set of rules for this purpose which will be discussed later (see below in part F(I)). For the time being, the necessary contract law rules for the implementation of such statutory access rights are not drawn up.

III. Competition law – part 1: anti-competitive agreements and abuses of dominance

For the emerging data economy to flourish, a sound contract law framework for data access and sharing agreements must be accompanied by competition rules. This section focuses on the prohibition of anti-competitive agreements (Article 101 TFEU, § 1 GWB) and on abuses of dominance (Article 102 TFEU, §§ 19, 20 GWB) as they relate to data access and data sharing, including a side-glance at sector-specific data access legislation. Merger control will be addressed in turn (IV.). Finally, we will take a look at specific data-related obligations for gatekeepers (DMA) or undertakings of paramount cross-market significance for competition (§ 19a GWB) (V.).

The aim of this part of the study is to briefly set out the law as it stands and to identify possible shortcomings, gaps and questions. These issues will then be further discussed in part F(II).

1. Data sharing agreements: Article 101 TFEU, § 1 GWB

On a general policy level, data sharing agreements are broadly encouraged: given that data are non-rival in their use, voluntary data sharing agreements in all their many forms and variations would seem to enable market actors to draw greater value from existing data resources.

Surveys on the state of the data economy consistently find that undertakings are hesitant to share data, however, and have identified a number of reasons (on this, see above, part D(III)).[308]

[308] See COM(2022) 68 final, 1.

Among other things, undertakings remain concerned that voluntary data sharing agreements may come into conflict with competition rules (see part D(III)(b)(aa)).

Indeed, data sharing arrangements may raise competition concerns (see below).[309] What is more: this is not only true for voluntary data sharing agreements, but also for those data access and sharing agreements that are concluded to comply with the growing number of data access and sharing obligations: as the relevant regulations specify,[310] competition rules, including Article 101 TFEU, remain applicable also to those agreements.

Most importantly for all practical purposes, data access and sharing agreements must comply with the competition rules applicable to information exchange.[311] The exchange of information may raise two main concerns: it may facilitate the coordination of the competitive conduct between undertakings and thereby promote collusive market outcomes; and it may foreclose competitors that do not participate in the exchange. Additionally, potential adverse effects on innovation incentives may need to be considered.

Possibly, if the information exchanged is protected by intellectual property rights, the rules on technology transfers[312] have to be taken into account. For the type of data exchanges we focus on here, this will rarely be the case, however. Nonetheless, the TT-BER may provide some (limited) inspiration on workable rules (see below, part F(II)(1)(a)).[313] Where information is exchanged in the course of cooperative research and development (R&D) endeavours, the R&D block exemption may come into play.[314] But data sharing agreements that are meant to support joint R&D efforts are not what we focus on here.[315] The legal framework for assessing the compliance of data access and sharing agreements concluded in the context of the three scenarios defined in part B will mainly follow from the competition law rules on information exchange.

---

[309] For an overview see also Crémer/de Montjoye/Schweitzer, Competition Policy for the digital era, Final report, 2019, p. 92 et seq., 96 et seq.; Lundqvist EuCML 2018, 146 (147).

[310] See, inter alia, the European Commission's proposal for a regulation on ensuring fairness in the allocation of value across the data economy (Data Act), which 'should not affect the application of the rules of competition, and in particular Articles 101 and 102 of the Treaty. The measures provided for in [the Data Act] should not be used to restrict competition in a manner contrary to the Treaty', Recital 88, and Draft Horizontal Guidelines, para. 411: '… those subject to regulatory requirements must avoid using these requirements as a means to infringe Article 101'. Furthermore, the information exchange must be restricted to what is strictly required. And the addressees of such regulatory schemes may be required to implement precautionary measures where commercially sensitive information is exchanged. When it comes to data intermediaries that qualify as data information services (DIS) under the DGA, Article 1(2b) DGA states that the DGA is 'without prejudice to the application of competition law' (see also Recital 44).

[311] See OJ 2011 C 11, 1 Chap. 2; C(2022) 1159 final, Chap. 6.

[312] OJ 2014 C 89, 3; OJ 2014 L 93, 17.

[313] See also Picht, Caught in the Acts: Framing Mandatory Data Access Transactions under the Data Act, further EU Digital Regulation Acts, and Competition Law, Max Planck Institute for Innovation and Competition Research Paper No. 22-05, p. 12 et seq.; Lundqvist EuCML 2018, 146 (152).

[314] OJ 2010 L 335, 36. See also the recent draft for a new R&D BER of the European Commission, C(2022) 1161 final.

[315] See for this Schneider ECJ 2021, 1.

a) Collusion

A first and obvious concern that may be associated with data sharing is collusion. According to a fundamental principle of EU competition law, each undertaking must determine independently its economic conduct and its commercial strategy on the relevant market.[316] It follows that competitors must not share commercially sensitive information, i.e. information that, if known to a competitor, reduces his or her uncertainty regarding recent or future action of competitors in the market.[317] Given its commercial sensitivity, the exchange of some sorts of information is generally considered suspect. This is true, in particular, for information on a company's pricing and pricing intentions, on current and future production capacities, on the intended business and on future innovation strategies.[318] In other cases, the type of data, the degree of data aggregation, the 'freshness' of the data and the frequency of a data exchange are to be analysed to determine its strategic value.

Any competition analysis of a data cooperation agreement will, therefore, start with the identification of the type of data that is subject to the cooperation, and the type of information that can be derived from it by those who are granted access to the data. In addition, the business rationale for the collaboration obviously matters. While an anti-competitive agreement does not presuppose anti-competitive intent, its showing would suffice to qualify the cooperation agreement as anti-competitive 'by object'. Where data are being shared to collude or to facilitate an anti-competitive agreement, no further analysis of the effects of the agreement will be needed.

In cases of data exchanges that are not restrictive of competition by object, market characteristics, including the market coverage of the agreement,[319] may matter for assessing the agreement's likely effects – which may range from collusive outcomes to promoting the well-functioning of a market.[320]

While data access and sharing agreements will greatly differ with regard to the type of data concerned and with regard to the uses that those data may be put to, most of these agreements as they are currently explored will not fall into the established 'restriction of competition by object' box. The data to be shared will typically not relate to the type of information that is considered 'suspect'. In its Draft Horizontal Guidelines, the European Commission

---

[316] See relevant case law by CJEU, in particular: Case C-8/08, *T-Mobile Netherlands and Others*, ECLI:EU:C:2009:343, paras. 32 et seq. and Case C-74/14, *Eturas*, ECLI:EU:C:2016:42, para. 27. See also: C(2022) 1159 final, para. 414.

[317] OJ 2011 C 11, 1 paras. 65 et seq.; C(2022) 1159 final, para. 423

[318] See Case C-8/08, *T-Mobile Netherlands and others*, ECLI:EU:C:2009:343, para. 37. See also: OJ 2011 C 11, 1 paras. 73 et seq.; C(2022) 1159 final, para. 424.

[319] Like market concentration, market transparency etc. See OJ 2011 C 11, 1 paras. 77 et seq.; C(2022) 1159 final, paras. 443 et seq.

[320] OJ 2011 C 11, 1 paras. 75 et seq.

distinguishes between data sharing agreements that relate to 'raw data',[321] 'pre-processed data'[322] and 'data that has been manipulated in order to produce meaningful information'.[323] Many of the more recent regulations (or regulatory proposals) that create new rights of access to data and, consequently, will require the conclusion of data sharing agreements in the future relate to what would arguably qualify as 'raw data' or 'pre-processed' data. This is true, for example, for 'data generated by the use of a product or related service', to which the Draft Data Act relates – data that would qualify as 'observed data' in the categorization that is used by the OECD.[324] The same would seem to apply to 'data that is provided for or generated in the context of the use' of a core platform service under Article 6 No. 10 DMA (see under part E(V)(1)(a)).[325] While 'raw data' – e.g. in the form of machine sensor data or user behaviour data – may be of great relevance as an input for improving products or services or for offering complementary services, they will frequently not be commercially sensitive in the 'classical' sense,[326] i.e. reduce the uncertainty about future conduct or strategies of competitors in the market. Typically (although not always),[327] the strategic value of such data will rather lie in their potential for innovation. Which insights are drawn from these data will depend, to a large extent, on the use that they are put to, the type of data analytics that are applied, and possibly on if and how those data are combined with other datasets. The same dataset may, therefore, allow for very different entrepreneurial strategies or types of innovation. Restrictions of competition may become an issue if the sharing of those data goes along with an agreement on

[321] Defined as 'raw and unorganized digital content that will need processing in order to make it useful'.

[322] Defined as data 'that has already been prepared and validated'.

[323] C(2022) 1159 final, para. 407.

[324] For the distinction between volunteered/provided data, observed data and derived data see: OECD, Enhancing Access to and Sharing of Data: Reconciling Risks and Benefits for Data Re-use across Societies, 2019, p. 30 et seq. The term 'observed data' applies to data on user behaviour as it is continuously generated and collected on the internet, and 'machine sensor data', i.e., data that records machine usage patterns etc.

[325] Note that the recitals of European Commission's draft, COM(2020) 842 final, included 'data inferred from such use' (Recital 55). This passage was deleted in the further legislative process.

[326] The Draft Horizontal Guidelines appear to mix up these two issues when it finds that the 'commercially sensitive nature of information depends […] on the usefulness it has to competitors' (C(2022) 1159 final, para. 428). If the information matters because it reduces uncertainty regarding a competitor's future or recent action, the competitive concern differs, however, from a setting where the information matters because it is an important input for innovating or personalizing products. In the first case, the first concern is collusion, in the second case, the first concern is foreclosure.

[327] 'Observed data', too, can be competitively sensitive in some settings. In the European Commission's ongoing proceedings against Amazon, for example (see European Commission, Case AT.40703 – *Amazon Buy Box* (pending)) Amazon is accused of having used non-public business data that has been generated by platform users in their interaction with independent retailers, including the number of visits to seller's offers. It seems reasonable to assume that, in such a setting, a voluntary comprehensive exchange of user click data could amount to a restriction of competition by object. According to the Commission's press release, the business data accessed by Amazon included 'the number of ordered and shipped units of products, the sellers' revenues on the marketplace, the number of visits to sellers' offers, data relating to shipping, to sellers' past performance, and other consumer claims on products, including the activated guarantees' – see European Commission, Antitrust: Commission sends Statement of Objections to Amazon for the use of non-public independent seller data and opens second investigation into its e-commerce business practices (Press release of 10.11.2020), https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2077 (last visited 4.7.2022) and European Commission, Antitrust: Commission opens investigation into possible anti-competitive conduct of Amazon, (Press release of 17.7.2019), https://ec.europa.eu/commission/presscorner/detail/en/IP_19_4291 (last visited 4.7.2022).

how to use and analyse those data. Absent such an agreement, shared access to such data may increase, rather than impede competition. This may differ where 'derived' data are shared – which may amount to a sharing of innovation outputs.[328]

Even where a pool of 'raw' or 'pre-processed' data would theoretically allow competitors to derive commercially sensitive information, depending on the combinations of datasets and analytics that are used, measures may be put in place that prevent that data is accessed in a way that creates a risk of collusion. For example, the governance regime of a given data pool may contain safeguards to ensure that participants to that pool have access only to the data provided by themselves and to the aggregated data of the other participants for a pre-defined, limited and legitimate set of purposes. Access to data may be granted only in a 'query-based' manner and for specified use cases. The possibility to combine the data with data from other sources may be constricted. The management of a pool may be delegated to an independent third party.[329]

The sharing of 'data that has been manipulated in order to produce meaningful information'[330] – or 'derived data' in the categorization of the OECD (2019) (see above) – is likely to require an in-depth analysis case-by-case. Firstly, the commercial sensitivity of the data will need to be determined. Secondly, such agreements may tend to come with greater risks of a restriction of competition on innovation, given that the way data are processed may become an ever more important parameter of competition in itself.

Depending on the circumstances, a 'collusive effects' analysis may be very complex – potentially much more complex than in traditional information exchange settings. The analysis may be more straight forward where voluntary data access or sharing are organised on a sector-specific basis, as is typically the case today. However, datasets may be multi-functional and competitively relevant across markets. If data access and sharing agreements allow for cross-market uses, the competitive effects in different markets and settings may differ.[331] While the cross-market use of data may be desirable from an innovation policy perspective, ways to handle additional risks for competition still need to be found.

b) Foreclosure

The second concern that data access and sharing agreements may raise is foreclosure.[332] Data access and sharing arrangements may put non-participating competitors at a significant competitive disadvantage vis-à-vis the participating competitors.[333] This presupposes that, in the relevant context, the data concerned is an input of strategic importance and that the parties

[328] See C(2022) 1159 final, para. 424.

[329] Id., para. 440.

[330] Id., para. 407.

[331] Examples in Lundqvist EuCML 2018, 146 (149).

[332] See OJ 2011 C 11, 1 paras. 69-71. See also Case C-7/95 P, *John Deere*, ECLI:EU:C:1998:256.

[333] OJ 2011 C 11, 1 para. 70.

to the collaboration hold some relevant degree of market power.[334] The risk of anti-competitive foreclosure increases with the degree of market power and the importance and concentration of the data. Where the data are of cross-market relevance, exclusionary effects may result on various markets. Questions to be considered in the Article 101(1) TFEU analysis include: who participates in the data collaboration? Does the data access or sharing agreement lead to the acquisition or strengthening of data-related market power in any relevant market? Are third parties excluded and thereby hindered from competing? Or is the data exchange open to third parties on non-discriminatory terms?[335] By way of example, the Draft Horizontal Guidelines of 2022 consider a data pooling initiative concerning information of 'strategic importance', which covers a significant part of the relevant market but does not grant third party access to the relevant data. Competitors that do not participate in the data pooling initiative would thereby suffer a significant competitive disadvantage. Also, the entry of new operators on the market would be hampered.[336] Anti-competitive foreclosure may also occur on a related market, where vertically integrated companies exchange or pool data in an upstream market and thereby gain market power on a downstream market.[337]

Again, concerns relating to the exclusionary effects of a data access or sharing agreements may be fixed: in particular, compatibility with Article 101(1) TFEU may be achieved by granting access to the relevant data to all market participants in a non-discriminatory manner – the European Commission has referred to FRAND access at times.[338] The question whether the rules on FRAND access to SEPs[339] can be applied in analogy[340] will be discussed later (see 4).

---

[334] To the same effect see C(2022) 1159 final, para. 442: The assessment of exclusionary effects under Article 101 TFEU depends on the nature of the pooled data, the terms of the data pooling agreement, and the market position of the relevant parties.

[335] For three different business models of B2B data sharing ranging from an Open Data Approach to exclusive data partnerships see COM SWD(2018) 125 final, 5.

[336] C(2022) 1159 final, para. 421.

[337] Id., para. 422.

[338] For the importance of the granting of FRAND access also to third parties see also the ongoing investigation of the Commission in *Insurance Ireland*, which was opened in May 2019 (European Commission, Case AT.40511 – *Insurance Ireland* (pending), see also European Commission, 'Antitrust: Commission opens investigation into Insurance Ireland data pooling system', (Press release of 14.5.2019), https://ec.europa.eu/commission/presscorner/detail/en/IP_19_2509 (last visited 4.7.2022); European Commission, 'Antitrust: Commission sends Statement of Objections to Insurance Ireland for restricting access to a data sharing platform', (Press release of 18.6.2021), https://ec.europa.eu/commission/presscorner/detail/en/IP_21_3081) (last visited 4.7.2022): The Commission is examining Insurance Ireland's data pooling system, to which member companies contribute information about insurance claims. The data pooling system is intended to detect potentially fraudulent claims and ensure that potential customers provide accurate information. Competition concerns have been raised in particular with regard to the access conditions of the data pooling system.

[339] See in particular Case C-170/13, *Huawei Technologies*, ECLI:EU:C:2015:477.

[340] On this question see, in particular, Picht, Caught in the Acts: Framing Mandatory Data Access Transactions under the Data Act, further EU Digital Regulation Acts, and Competition Law, Max Planck Institute for Innovation and Competition Research Paper No. 22-05, p. 26 et seq.; Borgogno/Colangelo, Data Sharing and Interoperability Through APIs: Insights from European Regulatory Strategy, Stanford-Vienna European Union Law Working Paper No. 38, 2018, 37 et seq.; Zoboli, Fueling the European Digital Economy: A Regulatory Assessment of B2B Data Sharing, 2019, https://ssrn.com/abstract=3521194 (last visited 4.7.2022), p. 20 et seq.

Unless competitively sensitive information is disclosed, open membership or access may then mitigate the risk of anticompetitive foreclosure.

c) Adverse effects on innovation

Even if a data access or sharing agreement does not come with a risk of collusion or foreclosure, possible adverse effects on innovation have to be considered: members of the data cooperation and/or other (potential) competitors may be discouraged from developing, differentiating and improving their own data collection or data processing. Where 'inferred data' is pooled, competitors may refrain from trying to develop and apply their own data analytic tools. Data access and sharing cooperation should, therefore, be analysed for their effects on the partners' and on third parties' incentives to innovate in data collection, curation, and analysis.

Given the uncertainties about the effects on innovation, the analysis of this theory of harm is highly complex and difficult. However, one could draw inspiration – at least conceptually – from the competition law framework for R&D agreements.[341] In this context, in addition to effects on existing technology or product markets, possible restrictive effects on competition in innovation are to be taken into account.[342] In particular, if R&D efforts are directed at a technology or product which would create a completely new market, immediate effects on existing markets are less likely.[343]

d) Relevant case law on data access and sharing agreements

So far, the case law on data access and sharing agreements is limited.

At the EU level, the *Asnef-Equifax* judgement[344] is frequently cited as a relevant reference:[345] in this case, the CJEU was asked to decide on the legality of a register set up by financial institutions in Spain to exchange solvency and credit information about their customers. The goal was to better assess the risks of granting credit. The CJEU found no restrictive effects on competition. Three factors were determinative: (i) the degree of concentration in the relevant credit market was not very high, (ii) the arrangement was not capable of revealing the identity of lenders – which would have enabled the cooperating entities to determine the market position and strategy of their competitors, and (iii) the information was accessible in a non-

[341] See the 2011 Horizontal Guidelines, OJ 2011 C 11, 1 Chap. 3, and the 2022 draft Horizontal Guidelines, C(2022) 1159 final, Chap. 2 as well as the R&D BER, OJ 2010 L 335, 36, and the recent draft for a new R&D BER, C(2022) 1161 final.

[342] C(2022) 1159 final, paras. 84-88.

[343] See for an illustrative example C(2022) 1159 final, para. 200.

[344] Case C-238/05, *Asnef-Equifax*, ECLI:EU:C:2006:734.

[345] See, for example Crémer/de Montjoye/Schweitzer, Competition Policy for the digital era, Final report, 2019, p. 95; Graef/Tombal/de Streel, Limits and Enablers of Data Sharing: An Analytical Framework for EU Competition, Data Protection and Consumer Law, Background Note for the meeting of the Digital Clearinghouse of 19 November 2019, p. 7; Feasey/de Streel, Data Sharing for Digital Markets Contestability, CERRE Report September 2020, p. 41.

discriminatory manner to all players in the industry.[346] Regarding the importance given to non-discriminatory access for all for precluding an exclusionary effect, *Asnef-Equifax* may indeed be considered a relevant precedent for data access and data sharing agreements more broadly. Also, the judgment suggests that – where information is capable to improve the functioning of the market – competition law will require safeguards against collusion and exclusion, but will not stand in the way of data sharing.

When it comes to analysing possible risks of collusion, much will depend on the specific facts of each single case. The data at issue in *Asnef-Equifax* was in large parts 'factual' information on contract performance, such as non-payment, outstanding credit balances, collateral, guarantees and security, leasing transactions, or temporary disposal of assets;[347] a type of data that does not fall squarely into any of the categories of 'volunteered', 'observed' or 'derived' data (for this categorization: see above). To ensure that the register is not capable of revealing the market position or commercial strategy of competitors, the Court emphasised the importance of not revealing the identity of lenders.[348]

A second and more recent case at EU level is *Insurance Ireland*.[349] Insurance Ireland is an association of Irish insurers active in the Irish insurance sector. Its members hold a market share of over 90% of the Irish motor vehicle insurance market. Among other things, the association administers a non-life insurance claims data pool ('Insurance Link'). Access to this data pool enabled the eligible insurers to better assess risk, to detect and defend themselves against potential fraud, and thus to offer their products at competitive prices. Access to the pool was linked to membership in the Insurance Ireland association, however. According to the European Commission's findings, the criteria for membership were unclear and intransparent, and were handled in a discriminatory and unpredictable manner. For a number of applicants, the membership application process was seriously delayed. Other applicants – such as insurers established in other Member States – were excluded from membership for prolonged periods of time. The European Commission therefore issued a statement of objections, claiming that the membership criteria established hurdles that led to certain insurers being denied access to the data pool thereby prevented competitive entry of new players into the market.[350] Initially, the European Commission had also investigated collusion concerns. Ultimately, it found the data pooled not to be commercially sensitive, however. The statement of objections was therefore entirely focused on foreclosure. In March 2022, Insurance Ireland offered commitments: it proposed to de-couple access to the data pool from membership in the association; to adopt and make public fair, objective, transparent and non-discriminatory

[346] Case C-238/05, *Asnef-Equifax*, ECLI:EU:C:2006:734, paras. 58-60.

[347] Id., para. 46.

[348] Id., para. 59.

[349] European Commission, Case AT.40511 – *Insurance Ireland*. See in particular the market test notice of 4 March 2022, OJ 2022 C 104, 15.

[350] See European Commission, Antitrust: Commission sends Statement of Objections to Insurance Ireland for restricting access to a data sharing platform (Press Release of 18.6.2021), https://ec.europa.eu/commission/presscorner/detail/en/ip_21_3081 (last visited 4.7.2022).

criteria for access to the data pool, and to apply these criteria in a uniform manner to all applicants; to designate an Insurance Link Application Officer, responsible for independently reviewing and determining applications for access; to introduce a fair, objective, transparent and non-discriminatory fee structure for access to the data pool; and to adopt and make public fair, objective, transparent and non-discriminatory criteria for admission to membership of Insurance Ireland.[351] In June 2022, the European Commission accepted the commitments offered by Insurance Ireland and declared them legally binding.[352]

These commitments may be read as a guide for the data governance structure that the European Commission will request wherever a data pool is established that includes data of significant competitive relevance and that has acquired a large market share. The well-known FRAND-formula – the requirement of fair, reasonable and non-discriminatory conditions of access – is amended by an additional transparency criterion. Also, the appointment of a person may be required that is authorised to decide on access applications independently. This falls short of a requirement to entrust an independent data intermediary with the task to run the data pool. However, it is a step into requiring institutional guarantees of neutrality.

More cases on data sharing have been – and are being – dealt with at the national level.[353] In 2018, the Bundeskartellamt gave green light to the B2B platform XOM Metals, but emphasised that this cooperation must not allow platform users to access the data of their competitors.[354] Similarly, the Bundeskartellamt did not object to the launch of Unamera, an online agricultural trading platform set up by grain trading companies,[355] but reverted to the principles established in the XOM Metal case: "it must be ensured that the trading platform continues to operate separately from partners in personnel, organisational, technical and information terms. […] As regards the planned publication of market statistics, in the authority's opinion the disclosure of prices is conditional on the aggregation of the data to obtain an average price, based on the prices submitted by at least five independent companies."[356] In these cases, the Bundeskartellamt dealt with platform cooperations that included limited information exchange functionalities.

'Real' data sharing arrangements have come into focus in the mobility and automotive sector.

---

[351] OJ 2022 C 104, 15.

[352] European Commission, Antitrust: Commission accepts commitments by Insurance Ireland to ensure access to its data sharing platform (Press release of 30.6.2022), https://ec.europa.eu/commission/presscorner/detail/en/ip_22_4242 (last visited 4.7.2022).

[353] For a brief overview of relevant cases so far see Podszun, Empfiehlt sich eine stärkere Reguleirung von Online-Plattformen und anderen Digitalunternehmen?, Gutachten F zum 73. Deutschen Juristentag, Hamburg 2020/Bonn 2022, F-88-F-89. For the Bundeskartellamt*'s* practise with regard to B2B platforms and marketplaces see Podszun/Bongartz BB 2020, 2882; Podszun/Bongartz ECLR 2021, 247.

[354] Bundeskartellamt 27.2.2018, B5-1/18-001 – *XOM Metals* (case report).

[355] Bundeskartellamt, No objections to launch of online agricultural trading platform (Press release of 5.2.2020), https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2020/05_02_2020_Unamera.html;jsessionid=F95FDF4A455E50A21BF1D347846ED512.2_cid390?nn=3591568 (last visited 4.7.2022).

[356] Ibid.

In the mobility sector, the Bundeskartellamt is advising transportation companies on how to establish a competition law compliant data hub called 'Mobility Inside'[357] that would allow the cooperating companies to bundle timetable information, ticketing and an interconnection of their electronic offers more generally. Furthermore, the Bundeskartellamt accompanies plans pursued by public and private undertakings and supported by the German government's mobility strategy to create a 'mobility data space'. The data space would encompass a broad range of data relevant to the mobility sector, ranging from data on traffic to timetable information, ITS data and data on weather.

As in the *Insurance Ireland* case, the concerns appear to be primarily related to foreclosure. Questions arise whether access to data will be limited to undertakings who are partners to the joint venture or whether access will also be granted to third parties, and if so, on which conditions. Whether access by third party is required will depend on the relevance of such access for effectively competing in the market. This, in turn, may depend on the position that such a cooperation will likely occupy in the relevant market(s). Also, consideration must be given to the effects that such a cooperation will likely have on innovation: while it may well create important opportunities for innovation, it may also reduce incentives to invest in different innovative pathways – e.g. where a data cooperation is linked to a mandatory use of specific apps.

The automotive sector is another sector where data sharing initiatives are currently explored extensively, and where companies willing to cooperate seek the Bundeskartellamt's guidance. Catena-X – a data network for collaboration in the automotive industry – provides a prominent example. On 24 May 2022, the Bundeskartellamt has declared that it has no objections to the planned cooperation.[358] Catena-X is part of the Gaia-X initiative. It is meant to establish an integrated, collaborative, open data ecosystem for all players in the value chain. So far, automotive part suppliers and manufacturers have worked on the digitisation of the production individually and/or in the framework of Industry 4.0 – including e.g. global logistics platforms or AI algorithms to optimise production. In this context, manufacturers have relied on established cloud providers (Amazon, Google, or Microsoft) to offer individual digital solutions. Closed data platforms tend to emerge, each with their own interface to which suppliers then have to adapt. Catena-X, on the other hand, aims to develop uniform standards for data transfers. The stand-alone solutions that have evolved so far shall be made to interoperate. Apart from these standardisation efforts, Catena-X will engage in joint R&D projects with the aim to develop specific applications to be made available in the data network. Such applications should, for example, enable the traceability of components; make it possible to determine the carbon footprint of components along the value chain; or improve quality

[357] For further information see https://www.mobility-inside.de (last visited 4.7.2022).

[358] See Bundeskartellamt, First component for Gaia-X: Bundeskartellamt gives green light for establishing data network for automotive industry (Catena-X) (Press release of 24.5.2022), https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2022/24_05_2022_Catena.html (last visited 4.7.2022).

management.[359] The Bundeskartellamt has recognised the innovative and pro-competitive potential of the network. At the same time, it has set out three competition principles to be observed:

> "(1) The exchange of competitively sensitive information must be limited to what is absolutely necessary for the cooperation.
>
> (2) The standards must be developed in a transparent and non-discriminatory manner in an open procedure. This means that especially third parties must be allowed to participate in the procedure for setting a standard, compliance with the standard must be voluntary and access to the standard must be provided on fair, reasonable and non-discriminatory terms.
>
> (3) The individual development cooperations planned as part of the project must not lead to market foreclosures or other distortions of competition, also with regard to competition in innovation."

These principles appear to be of a general nature: they can provide guidance also to similar projects that strive to establish a sector-wide data collaborations.

e) Standardisation

The Catena-X initiative illustrates the close linkage that may exist between data access and sharing agreements on the one hand, and standardisation agreements on the other: often, the parties to a data sharing arrangement will need to agree on a specific data format[360] as well as on interoperability standards.[361] With regard to this thread of a data access or sharing agreement, the principles for the review of standard-setting initiatives as set out in the Horizontal Guidelines[362] will apply.

While standardisation agreements that are part of a broader anti-competitive agreement and/or aim to exclude actual or potential competitors from the market, or that directly influence prices qualify as infringements by object,[363] standardisation agreements will frequently pursue pro-competitive goals: often, they promote the integration of the internal market and contribute to the development of new and better products or conditions of sale.[364] The European Commission therefore considers that standardisation agreements, by ensuring compatibility and

---

[359] Ibid.

[360] For the importance of standardization for the promotion of data portability and interoperability see Lundqvist EuCML 2018, 146. On the ongoing data-related standardization projects of CEN, CENELEC and ETSI see also: https://www.cencenelec.eu/media/CEN-CENELEC/News/Publications/2021/digitalinstandards.pdf (last visited 4.7.2022).

[361] For the competitive effects of interoperability in the digital economy, see Kerber/Schweitzer JIPITEC 2017, 39.

[362] OJ 2011 C 11, 1 paras. 257 et seq. See also C(2022) 1159 final, paras. 462 et seq.

[363] OJ 2011 C 11, 1 para. 273.

[364] OJ 2011 C 11, 1 para. 263; C(2022) 1159 final, para. 465.

interoperability, will normally promote competition.[365] For industry-wide standardisation agreements, the Guidelines establish a 'safe harbour' where the following four cumulative conditions are met: (i) unrestricted industry participation in a transparent standard-setting procedure, (ii) the inexistence of any obligation to comply with the adopted standard, (iii) good faith disclosure of standard-essential intellectual property rights, and (iv) a clear and balanced IP rights policy, including accessibility to the standard on FRAND terms.[366] In such cases, no market share threshold will apply.

Recently, the European Commission has applied these principles in assessing the membership criteria and internal working rules of GAIA-X under Article 101 TFEU.[367] In particular, it looked into the provisions on voting rights and the composition of the Board of Directors that differentiate between European and non-European members in that non-European members may neither vote on amendments to the Articles of Association nor on the dissolution and liquidation of the Association, nor may they be members of the Board of Directors. Given that adequate access, transparency and participation of relevant industry stakeholders are still effectively guaranteed, the European Commission has not raised concerns.

Where standardization is part of a data collaboration between a limited number of undertakings, the precondition of an unrestricted industry participation in a transparent standard-setting procedure will frequently not be met, however. In such a case, the effects of the standard on the relevant markets will need to be comprehensively analysed.[368] The likely effects will hinge, *inter alia*, on the question whether the standard is open to third parties.[369] Where interoperability and portability standards are set by undertakings with market power, the standard must not have the effect of foreclosing superior standards or of excluding, or discriminating against, certain companies.[370] Again, FRAND access by third parties to the standard may be required.

f) Data collaborations that are linked to R&D projects

Catena-X also shows that data collaborations or data pools may be closely linked to R&D endeavours. The pool may use the data as a basis for the development of new products and services.[371] Or the cooperation may pro-actively develop and provide applications to be used to draw value from the data. For such R&D legs of a data cooperation, the R&D block exemption

[365] OJ 2011 C 11, 1 para. 263.

[366] OJ 2011 C 11, 1 paras. 280-286.

[367] European Commission, Letter to Gaia-X of 19.10.2021, https://gaia-x.eu/sites/default/files/2021-11/Letter%20to%20Gaia-X_update.pdf (last visited 4.7.2022).

[368] OJ 2011 C 11, 1 paras. 292-300.

[369] OJ 2011 C 11, 1 para. 294.

[370] C(2022) 1159 final, para. 465; See also Zingales, Data Collaboratives, Competition Law and the Governance of EU Data Spaces, 2021, https://ssrn.com/abstract=3897051 (last visited 4.7.2022), p. 25.

[371] Lundqvist EuCML 2018, 146 (150, 153); Lundqvist/Murati, Collaborative Platforms and Data Pools for Smart Urban Societies and Mobility as a Service (MaaS) from a Competition Law Perspective, Stockholm Faculty of Law Research Paper Series no 75, p. 15.

rules (BER[372]) and the rules on R&D as they are set out in the European Commission's Horizontal Guidelines will apply.[373]

Given that the aim of data access and sharing agreements in the access scenarios that we focus on in this study will regularly reach beyond a joint R&D endeavour, the R&D BER will typically not provide a safe harbour, however.[374]

g) Gaps and uncertainties in the existing framework

The competition law on information exchange has always been complex and highly context-sensitive.[375] When these rules are applied to data access and sharing agreements, the complexities multiply: the types of data that may be shared, and the contexts in which they may be shared are myriad. New developments in the field of data science and novel data analytics tools may affect what information can be drawn from a given dataset[376] – or combinations of datasets – and may change the ways in which this information is used to develop business strategies.

So far, both the European Commission and the Bundeskartellamt have looked rather favourably at data access and sharing arrangements. When confronted with data cooperations with a significant potential to contribute to the well-functioning of markets, risks of collusion have not been exaggerated, but have been analysed with good judgement and an intention not to stand in the way of innovative endeavours. Risks of foreclosure have frequently been considered more carefully. A set of data sharing governance rules appears to be emerging for settings where the collaborators have a significant degree of market power and the data at issue is competitively

---

[372] OJ 2010 L 335, 36. See also the recent draft for a new R&D BER of the European Commission, C(2022) 1161 final.

[373] See the assessment criteria set out in Chap. 3 of the 2011 Horizontal Guidelines, OJ 2011 C 11, 1 and Chap. 2 of the Draft Horizontal Guidelines of March 2022 on R&D agreements, C(2022) 1159 final. The challenge in applying this framework to data sharing agreements is the complex anticipation of effects – not only on existing technology and product markets, but also on competition in innovation – see Zingales, Data Collaboratives, Competition Law and the Governance of EU Data Spaces, 2021, https://ssrn.com/abstract=3897051 (last visited 4.7.2022), p. 21. This is especially true, since R&D poles within the meaning of Article 1(8) of the Draft R&D BER can hardly be identified if competition in innovation is unstructured – as is typically the case in the digital economy. On the innovation process in the digital economy see Crémer/de Montjoye/Schweitzer, Competition Policy for the digital era, Final report, 2019, p. 35.

[374] For the application of the rule on R&D agreements to data sharing for collaborative research see Schneider ECJ 2021, 1 (9 et seq.).

[375] Schneider ECJ 2021, 1 (20-24), has proposed to systematise the analysis under Article 101(1) TFEU along a set of four criteria, based on 'a combined reading of the framework under Article 101(1) TFEU and the principles grounding the recent Data Governance Act and Digital Service Package': (i) Subjective: type of undertaking involved; (ii) Objective: type of data shared; (iii) Structural: degree of openness; (iv) Teleological: public or commercial-oriented interest. While this is helpful, it only partly covers up the complexity of each criterion and the overall analysis.

[376] See Anzini/Pierrat, Data Pools as Information Exchanges between Competitors: An Antitrust Perspective, cepInout 5/2020, p. 12 for a proposal to take the varying abilities to draw relevant, competition-sensitive information from a dataset in the analysis of Article 101(1) TFEU, e.g. by identifying a statistical threshold for the likelihood of the data being transformed into specific information; or by looking at the mining abilities of the data pooler and the technological advancement in the relevant sector.

relevant. Given the dynamics of this field and the dearth of precedents, a significant degree of uncertainty remains nonetheless.

We will therefore revisit these issues in our policy part (F(II)(1)): is it possible to create a general safe harbour for data access and sharing cooperations? Can specific data sharing governance rules contribute to such a safe harbour? And is there a need for new or improved procedures that may provide greater legal certainty to data access or sharing initiatives?

2. Data-related abuses of dominance – Article 102 TFEU/§ 19 GWB

The series of policy reports on the state of the digital economy as they have been published from 2018 onwards[377] has consistently highlighted the growing competitive relevance of data: data may be the basis for improving production processes, products/services, logistics and marketing, and have opened the possibility for the evolution of individualized or personalized products and services or marketing. As the IoT evolves, data are becoming an ever more important input for predictive maintenance and complementary services. In addition, they have become the driver of a hugely successful new business model, namely targeted online advertising, which lies at the heart of the economic success of some of the largest platforms – Google (Alphabet) and Facebook (Meta) in particular.

As the role of data as a competitively relevant input has increased, so has the risk that data may become a source of market power and contribute to its entrenchment.[378] Simultaneously, unilateral conduct related to the collection, exploitation, and sharing (or non-sharing) of data may raise barriers to entry and result in a – potentially anti-competitive – foreclosure of competitors or help leverage market power to adjacent markets. Also, due to the value of data the incentives to exploit a given market position to accumulate even more data may increase.

Although the potentially huge economic importance and its competitive relevance are generally acknowledged, few cases of data-related abuses have been decided upon so far. In sectors in which data access is considered particularly important for new services to evolve – such as the financial sector or the automotive sector –, sector-specific data access regulation has been put into place or is being discussed. When it comes to access to personal data, Article 20 GDPR has been the focus of the debate, and more recently the Draft Data Act. These provisions are complemented by specific provisions in the draft DMA and/or in § 19a GWB addressed to the largest digital platforms. As far as access to non-personal individual level IoT data is concerned, the Draft Data Act shall provide for a specific data access regime.

---

[377] ACCC, Digital Platforms Inquiry, Final Report, 2019; Crémer/de Montjoye/Schweitzer, Competition Policy for the Digital Era, Final report, 2019; Furman et al., Unlocking Digital Competition, 2019; Schallbruch/Schweitzer/Wambach, Ein neuer Wettbewerbsrahmen für die Digitalwirtschaft, Bericht der Kommission Wettbewerbsrecht 4.0, 2019; Schweitzer/Haucap/Kerber/Welker, Modernisierung der Missbrauchsaufsicht für marktbeherrschende Unternehmen, 2018; Subcommittee on Antitrust, Commercial and Administrative Law of the Committee on the Judiciary, Majority Staff Report and Recommendations, 2020; Stigler Committee on Digital Platforms, Final Report, 2019.

[378] See Bundeskartellamt/Autorité de la Concurrence, Competition Law and Data, 2016, p. 11.

In competition law, the debate has largely focused on the so-called 'essential facilities' doctrine and in Germany on the new § 20(1a) GWB. There is, however, a striking mismatch between the breadth and intensity of the debate and the cases addressed by competition authorities and courts so far. While the reasons for this mismatch remain unclear, the surveys summarized in part D show a high degree of scepticism of market participants vis-à-vis mandatory data access regimes, even where data access obligations apply only to dominant firms. This indicates that in many markets, mere data access mandates would not suffice to effectively promote contestability or promote competition and innovation. The root of the problems to effectively compete in digital markets may frequently be more subtle and complex.

In the following section, we briefly look at data-related market power first (a). It can come in the form of dominance on a separate market for data (aa). More frequently, the control of competitively relevant data will be a factor that contributes to the finding of dominance on a product or services market (bb).

Next, we focus on data-related abuses (b). Firstly, we inquire into when a refusal to grant access to data may constitute an abuse. Secondly, we ask whether there are other settings in which access to data may be an appropriate remedy.

a) Data markets and the role of data in establishing market dominance

aa) Markets for data

Specific types of data are already being traded on 'markets for data'.[379] Yet, for many types of data which have become competitively relevant in the emerging data economy, this is not the case. Competition authorities have not yet found separate input markets for 'raw' machine sensor data in the IoT sector, for example; or for click-data of platform users on the internet.[380]

Where a given input is not openly traded, the demand for this input may sometimes suffice to presume the existence of a 'hypothetical' relevant 'upstream' market for the purposes of Article 102 TFEU. This is what parts of the case law on the 'essential facilities' doctrine (EFD) suggest.[381] Assuming a hypothetical input market amounts to a decision to call the undertaking's vertical integration into question. The EFD suggests that this is justified only where access to the input is absolutely indispensable to compete downstream.

---

[379] Cf. Santesteban/Longpre Antitrust Bull. 2020, 459 (481-483). See also: Graef World Competition 2015, 473; European Commission, Support study accompanying the evaluation of the Commission Notice on the definition of relevant market for the purposes of Community competition law, 2021, p. 90 et seq.

[380] For a review of relevant cases and discussion see Id., p. 90 et seq.

[381] See, in particular Case T-184/01, *IMS Health II*, ECLI:EU:T:2001:259 and Case C-418/01, *IMS Health*, ECLI:EU:C:2004:257, see also Drexl IIC 2004, 788; Graef, Data as Essential Facility: Competition and Innovation on Online Platforms, 2016; Schmidt, Zugang zu Daten nach europäischem Kartellrecht, 2020, p. 211 et seq.

Settings in which access to data as an input is indeed indispensable to compete on a neighbouring market may well exist, and the number of such settings may grow as the data economy continues to evolve. The evolution of the data economy is still at a relatively early stage, however. In many settings, the indispensability, strictly interpreted, will not be met. Substitutes to the relevant datasets may exist, or competition authorities may simply not be willing to presume from the outset that the product/service and the data generated by the product/service and exclusively controlled by the product/service provider must be unbundled.

In such cases, the (possibly exclusive) control of certain types of data – typically data generated in the use of the product or service – may nonetheless be relevant when assessing a data holder's market power on the relevant product or services market, as it may amount to a barrier to entry[382].

bb) The relevance of data for finding a position of dominance

Both EU and German competition law recognise the potential relevance of data for assessing the position of undertakings on a given market. In EU competition law, this is broadly recognised in the case law on Article 102 TFEU in digital settings[383] as well as on merger control (for this see part E(IV)). In Germany, access to competitively relevant data has been explicitly included in the list of factors that are relevant for determining the competitive position of an undertaking on a relevant market (see § 18(3) No. 3 GWB; and § 18(3a) No. 4 GWB with a view to assessing the position of an undertaking on a network market or multi-sided market). Nonetheless, whether and how access to, or control over, data matters must be determined case by case. Exclusive control of data that constitutes a non-substitutable input into data-driven products or services will be a particularly important factor: such control can immunize the data holder from competitive discipline on the relevant product or services market and may, therefore, allow him/her to behave monopolistically. In other cases, access to a specific type of data may contribute to the quality of a service or product, but may not be indispensable. Sometimes, access to inferred data can substitute for access to raw data. Sometimes, control of specific types of data may simply put an undertaking in a position that enables it to innovate faster and with a clearer sense of direction. A broader analysis of the various ways in which data can contribute to dominance is beyond the scope of this study. Suffice is to say that both German and EU competition law are sufficiently flexible to consider the possible relevance of data with a view to establishing market dominance.

A specificity of some types of data is its cross-market relevance. The control of specific types of data may, therefore, come with a possibility to influence competitive dynamics beyond the market(s) in which the undertaking is (already) dominant. The case law on abuses of dominance

[382] See Bundeskartellamt/Autorité de la Concurrence, Competition Law and Data, 2016, p. 11 et seq.

[383] See Case T-612/17, *Google Shopping*, ECLI:EU:T:2021:763; European Commission 18.7.2018, AT.40099 – *Google Android*.

recognises that – where markets are linked in specific ways – even conduct of a dominant undertaking on a market that is distinct from the dominated market and which produces effects on that distinct market may fall under Article 102 TFEU.[384] Control over data that is competitively relevant across market boundaries may be such a relevant link. For the largest digital platforms, this has now been implicitly recognised in § 19a GWB and the DMA (see further below). Outside the scope of § 19a, and even in the absence of market dominance, data-based forms of dependency can be caught by § 20(1a) GWB (see further below). Given this set of provision, German competition law appears to provide for all necessary possibilities to capture the competitive relevance of data.

b) Data-related abuses of dominance

The competitive relevance of data comes with a potential for data-related exclusionary practices.

The joint paper of the Autorité de la Concurrence and the Bundeskartellamt on 'Competition Law and Data' lists, *inter alia*, the following types of data-related exclusionary conduct:[385]

- Discriminatory access to data, e.g. where access to data is denied to customers who entertain a business relationship with a rival undertaking;[386]
- Exclusive contracting with data providers, thereby preventing rivals from data access;
- The tying of access to competitively relevant datasets to the use of the dominant undertaking's data analytics services if this leads to a reduction of competition on the market for data analytics.[387]

These types of data-related exclusionary abuses are relatively straightforward. They are not the focus of this study.

Rather, we will focus, firstly, on the question whether and when a refusal of a dominant company to grant competitors access to data may constitute an abuse of dominance (aa). In doing so, we will distinguish between different typical access scenarios and explore whether the established categories of abuses provide appropriate tests for differentiating between pro- and anti-competitive conduct.

Secondly, we will inquire whether and when certain practices relating to the *use* of data by the dominant company qualify as an abuse – and may possibly result in the imposition of data

[384] See Case C-333/94 P, *Tetra Pak*, ECLI:EU:C:1996:436, paras. 27 et seq.

[385] Bundeskartellamt/Autorité de la Concurrence, Competition Law and Data, 2016, p.17 et seq.

[386] See Id., p. 18-19 – the paper refers to a decision by the Autorité de la Concurrence 8.7.2014, no. 14-D-06 – *Cegedim*.

[387] See Bundeskartellamt/Autorité de la Concurrence, Competition Law and Data, 2016, p. 20, referring to the CMA, The commercial use of consumer data, 2015, p. 90.

access remedies. In this context, we will revisit the German *Facebook*-case, as well as the *Amazon* case (bb).

aa) Refusal to grant access to data

In the emerging data economy, access to data is considered to be key in many respects: among other things, the processing of data may help to identify relevant customer preferences, it may allow undertakings to realize efficiencies in production or logistics, it opens up new opportunities for innovating, including the personalization of products and services, and it may allow undertakings to better target potential customers. In the emerging IoT, access to machine usage data may be essential to be able to offer repair and maintenance services or complementary services. When it comes to online services, access to the behavioural data of the users of a service may provide potentially huge competitive advantages in identifying groups of customers that may be interested in specific kinds of additional services or in providing related services.

Frequently, access to the relevant troves of data is distributed unequally. Specific datasets – e.g. datasets about usage patterns of specific machines or customers – may be exclusively controlled by one undertaking, e.g. the manufacturer of the relevant machine or the provider of a given service. In other cases, important competitive advantages follow from the scale and scope of data that an undertaking controls. Undertakings which lack access to the relevant data may, therefore, request such access from data holders. If the relevant data holder refuses to grant access on a voluntary basis, the question arises whether and when competition law creates an obligation to grant access.

(1) Relevant data access scenarios

Given the multiplicity of categories of data, of stages of data processing (e.g. raw, pre-processed, inferred), of uses that data can be put to, of degrees of necessity of access to data for engaging in certain activities and of substitutability relationships between different datasets, there is no easy answer to this question. In order to develop a framework of analysis, it is useful to distinguish between different types of settings in which requests for access to data may arise. In the Special Advisors' Report on a 'Competition policy for the digital era', three data access scenarios have been distinguished that are of significant practical relevance. They all focus on 'observed' data, typically usage data generated in the use of digital services or machine sensor data[388] – a category that we pay particular attention to in this study.

(a) In scenario 1, a firm has exclusive control of individual level data – whether personal or non-personal – about a specific person or undertaking (or product or service used by a person or undertaking). Typically, this will be data that was provided to the firm by that person or undertaking, or that was generated in the use of the product or service. A third party may need

[388] Crémer/de Montjoye/Schweitzer, Competition Policy for the digital era, Final report, 2019, p. 75 et seq.

access to these data to provide complementary services to the person or undertaking to which the data relates. Where the data is controlled exclusively by the firm providing the primary product or service, the product or service user may be unable to provide the third party with such access, however.

In public debates, request for data access under scenario 1 are typically referred to as requests for data portability. There is, however, no established definition of data portability. Originally – namely in the context of Article 20 GDPR – the term seemed to refer to a one-off transfer of a specified data set. According to Article 6 No. 9 DMA, data portability can also be continuous and real-time, however. Furthermore, the term 'data portability' suggests that an effective transfer of data is required – a mere in situ access would not seem to suffice. Despite the fuzziness of the term, we will use it to describe the totality of access scenarios that fall under scenario 1. This implies that the concept of data portability as we use it here can also encompass a necessity to grant continuous and real-time access. The question whether the data must be effectively transferred or whether in situ access may suffice depends on the competition problem to be solved.

(b) In scenario 2, a firm requests access to bundled individual level data or to aggregate data from a data controller, either because the sort of data analytics that are needed to provide a competitive complementary service to the service provided by the data holder – for example predictions on the need for machine maintenance – depend on access to broader data sets (aa). In this sub-scenario of scenario 2, data access is meant to enable effective competition on an 'aftermarket' on which the data holder is, or is not, active. Or because access to the data is needed to compete on the primary market of the data holder (bb). For example, the data-related advantages of the dominant search engine may be so strong that entry into this market is no longer possible because potential entrants do not have access to the relevant search, click and query data.

(c) In scenario 3, a firm requests data from data controllers for the purpose of training algorithms for uses that are unrelated to the fields of activity of the data controller.

We believe that scenarios 1 and 2 capture the most important data access settings that can potentially be addressed within an 'abuse of dominance' framework, whereas scenario 3 access requests are not covered by competition law: according to established competition law doctrine, a dominant firm is under a 'special responsibility not to allow its conduct to impair genuine undistorted competition on the common market'.[389] However, it is not obliged to broadly enable and promote innovation. Where the legislator wants to impose an obligation to grant access to data as a matter of innovation policy, this will need to be done outside the framework of competition law, therefore.

In this part of our study, we will focus on scenarios 1 and 2. It seems that there is no relevant case law on data access requests of the scenario 1-type, however. Instead, data portability obligations have been imposed by way of sector-specific legislation (see (2)).

[389] Case C-322/81, *Michelin*, ECLI:EU:C:1983:313, para. 57.

By contrast, data access requests of the scenario 2-type have been broadly discussed within the competition law community, mostly by reference to the EFD. Little case law exists, however (see (3)).

An additional scenario is emerging in competition law – namely the question whether an undertaking abuses its dominant position when it obstructs the collection of data by third parties by way of third party cookies. We will briefly revisit this scenario, too (see (4)).

(2) Refusals to allow for the porting of data that was (co-)generated by the use of a product or service

With the growth of the data economy, an increasing number of products are equipped with sensors that collect data on the use of the product on a continuous basis, and ever more online services continuously track the usage of the service. In contractual relationships between businesses, the allocation of rights of control and access to the relevant data will frequently be subject to negotiations. Absent a marked asymmetry of bargaining power, the businesses can be expected to agree on the most efficient allocation. 'Open data' models may compete with 'closed data' models.

The competitive mechanism can fail, however. This is true where an undertaking that is dominant (or even super-dominant, as Google, Apple or Facebook) on the primary product or services market opts for a 'closed data' model. In these cases, there is no competitive pressure that would force this undertaking to offer customer-friendly contract terms and technical data access solutions. Given the competitive relevance of the control of data, customer-unfriendly data portability terms may become a dominant strategy even in oligopolistic market settings. Furthermore, information asymmetries may become a source of market failure. Given the dynamics of the emerging data economy, not only consumers, but also businesses may not be able to adequately assess the risks that go along with a 'closed data' model at the time when they choose the product or service. This is true, in particular, where long-lasting products or services are chosen. An exclusive allocation of access rights to the provider of a service or machine which may have seemed innocuous at the time when the choice was made may result in a data-related lock-in over time.

In B2C settings, the situation will tend to be even worse. The provider of the service will frequently retain exclusive control of the data. To the extent that personal data within the meaning of Article 4(1) GDPR is an issue, Article 20 GDPR provides for a right of data subjects to data portability. While Article 20 GDPR was meant to facilitate the data subjects' possibility

to switch providers, it does not include a right to full and real-time porting or to data-interoperability, however,[390] and has not been very effective in meeting its goal.[391]

For non-personal data, there is, as of now, no horizontal legal obligation for the service or product provider to ensure data portability. For data generated in the use of a product, the Draft Draft Data Act may provide for such an obligation in the future (see below, part F(I)). For data generated in the use of a core platform service by a gatekeeper, the DMA will require data portability (see Article 6 No. 9 DMA). § 19a(2), 1st sentence, No. 5 GWB empowers the Bundeskartellamt to impose data portability obligations upon designated undertakings of paramout cross-market importance. A question remains whether below this threshold, a refusal to grant data portability may amount to an abuse of dominance.

Currently, the possibility for users of services or machines to port and process the data they have generated by their use appears to be the data access scenario of the greatest practical importance. Given the relatively early stage of the data economy, the possibility for a machine or service user to provide third parties with access to individual level usage data that have been collected during the pre-existing relationship in order to switch to a competing product or service, in order to multi-home, or in order to make use of tailored complementary or aftermarket services offered by a third party is a relatively straightforward case of data usage.

Presuming a position of dominance, it seems likely that the unilateral termination of a former possibility to port data would qualify as an abuse, absent an objective justification. A finding of an abuse will be more difficult where the other side requests the introduction of a data portability option for the first time.[392] A denial of data portability could be considered exploitative, but the conceptual benchmark for an exploitation may be difficult to establish. The anti-competitive potential of such practices may be better captured by a hybrid theory of harm along the lines of the BGH's *Facebook* doctrine.[393] Here, a customer-unfriendly online choice architecture is prone to translate into a foreclosure of competitors who need data access to challenge the dominant undertaking in its primary market or to offer complementary services. While such a theory of harm seems viable in principle, it moves beyond the established boundaries of abuses of dominance. A finding of an abuse would not merely require the dominant firm to revert to an established market standard of 'competition on the merits'. Rather, it may require a different design of the service, the introduction of completely novel interfaces, a different way of organising and storing relevant data etc.; and the creation of a possibility to port data may come with important costs for the incumbent.

---

[390] De Hert/Papakonstantinou/Malgieri/Beslay/Sanchez CLSR 2018, 193 (200 et seq.); Schweitzer GRUR 2019, 569 (574).

[391] See Borgogno/Colangelo, Data Sharing and Interoperability Through APIs: Insights from European Regulatory Strategy, European Union Law Working Papers No. 38, 2018, p. 14 et seq.; Hennemann PinG 2017, 5.

[392] Schweitzer/Welker in German Federal Ministry of Justice and Consumer Protection/Max Planck Institute for Innovation and Competition, Data Access, Consumer Interests and Public Welfare, 2021.

[393] BGH 23.6.2020, KVR 69/19 – *Facebook*.

Generally, competition law is cautious with imposing remedies that intervene so severely into the design of a product or service. Also, where competition law would impose a data portability obligation, this would translate into a highly regulatory remedy. Many details would need to be decided in order to make it effective in meeting its goal to protect undistorted competition. Decisions would need to be made on whether data portability must be granted one time only, in regular intervals or continuously and in real time; on the data format; on the design of the interface for the data transfer; on the precise (FRAND) conditions of the transfer, including on the question of a possible remuneration etc.

It does not come as a surprise, therefore, that a multitude of data portability regimes has been emerging recently in various sectors that are outside the realm of competition law.

Arguably, the most prominent example is the PSD2 Directive[394] which promotes the sharing of some types of payment transactional and account information: Articles 64 et seq. of the PSD2 Directive provide for a special access regime for 'payment initiation service providers' (Article 66) and 'account information service providers' (Article 67) to payment accounts of account servicing providers such as banks via APIs, provided that the account holder explicitly requests such access.[395] The goal is, *inter alia*, to open up the financial sector for more competition and innovation in complementary services provided by Fintechs (cf Recitals 3 et seq.).[396] The European Banking Authority will define common and open standards to be implemented by all account servicing payment service providers (Recital 93).[397]

In the energy sector, customers are to be granted access to data on the electricity they feed into the grid and on their electricity consumption 'through a standardised communication interface or through remote access, or to a third party acting on their behalf, in an easily understandable format allowing them to compare offers on a like-for-like basis' (see Article 20 lit. e of the EU Electricity Directive 2019/944,[398] which is tailored to facilitate switching of electricity suppliers). Data access for complementary services (smart home devices or other consumer energy management systems) can be obtained through Article 23(2) of Directive 2019/944.[399] While Article 23 does not clearly state that data access is to be provided via real-time or near real-time APIs, Article 19(1) shows that the policy goal of such data access is to promote 'smart metering systems that are interoperable, in particular with consumer energy management

[394] OJ 2015 L 337, 35.

[395] For an attempt to conceptualize this right to data access see Schweitzer/Welker in German Federal Ministry of Justice and Consumer Protection/Max Planck Institute for Innovation and Competition, Data Access, Consumer Interests and Public Welfare, 2021, p. 122-125.

[396] Ibid.

[397] For a fuller discussion see Omlor ZEuP 2021, 821.

[398] OJ 2019 L 158, 125.

[399] According to this provision, 'the parties responsible for data management shall provide access to the data of the final customer to any eligible party […]. Eligible parties shall have the requested data at their disposal in a non-discriminatory manner and simultaneously. Access to data shall be easy and the relevant procedures for obtaining access to data shall be made publicly available'.

systems'. The European Commission shall specify interoperability requirements and procedures to ensure an effective implementation of this right to data access (see Article 24(2) of Directive 2019/944).

With regard to access to, and the portability of in-car data, a broad discussion on the most appropriate data access and governance regime has emerged. The European Commission is currently consulting whether – in addition to the Draft Data Act – a special legal regime for access to vehicle data, functions and resources is needed.[400]

In the agricultural sector, agricultural data is predominantly collected by the farms, but it is private third-party software that is used to process said data. The data is typically stored in locked data-sets controlled by the producer of the land machine or technical component. Farmers have called for more control of the data that they generate as well as avenues to tackle information asymmetries as well as power imbalances that exist with the digital service providers.[401] There are also concerns regarding problematic clauses for farmers in contracts with their service providers that stipulate that they cannot share their agricultural data across a variety of suppliers. This has led farmers to request the right to data portability to avoid lock-in. In addition, there has been the request for the 'right to repair' meaning 'right to access the data and software needed to repair their own machinery – rather than being contractually obliged to use licenced repairers (who may be costly and not readily available in remote areas), as it is currently often the case of digital equipment'.[402] On the other hand, there are concerns that if the agricultural data is not correctly shared, it could result, inter alia, in 'commodity speculation' and market manipulations.[403] It is believed that the EU's 'Code of Conduct on Agricultural Data Sharing by Contractual Agreement'[404] could help tackle several of these issues, e.g. by clarifying roles and who has control of the data or in providing a framework for data portability.

This experience suggests that a lack of data portability can lead to, or aggravate, competition problems, and that a well-functioning data portability regime can lower barriers to entry, whether into the primary product or services market or into complementary markets.

The emerging horizontal framework for the porting of co-generated data appears to acknowledge as much. For data generated in the use of a product, the Draft Data Act may, in the future, establish a useful baseline on which competition law can build: a refusal by a

---

[400] See the European Commission's Call for Evidence for an Impact Assessment regarding Access to Vehicle Data, Functions, and Resources, 29.3.2022, Ref. Ares(2022)2302201. For the debate on access to in-car data see: Martens/Müller-Langer J. Compet. Law Econ. 2020, 116. See also Kerber JIPITEC 2018, 310.

[401] Jouanjean/Casalini/Wiseman/Gray, Issues around data governance in the digital transformation of agriculture: the Farmers' Perspective, OECD Food, Agriculture and Fisheries Papers No. 146, p. 7.

[402] Id., p. 7 et seq.

[403] Ibid.

[404] https://cema-agri.org/images/publications/brochures/EU_Code_of_conduct_on_agricultural_data_sharing_by_contractual_agreement_2020_ENGLISH.pdf (last visited 4.7.2022).

dominant firm to design products accordingly will arguably amount to an abuse, as will a discriminatory downgrading of data portability by a dominant undertaking.

However, designing an appropriate data portability regime will remain a challenging and highly sector-specific task. A malfunctioning of data-driven competition in a given sector can – and arguably should – be a trigger for the development of a data portability regime. However, competition authorities may not be best placed to design and monitor such a regime. Typically, a regulatory framework will be needed.

(3) Refusals to grant access to bundled individual level or aggregate data

Access to individual level usage data pertaining to a particular user will not always suffice for a third party competitor to enter the market and compete – whether on a complementary market or on the primary product or services market. Sometimes, a (potential) competitor may need access to large sets of *bundled* individual level usage data for anonymous use[405] or to *aggregated* usage data[406] to provide complementary products or services that are competitive, or to enter the primary market. Imagine, for example, a predictive maintenance service that requires aggregated data about the 'wear and tear' of a piece of equipment as training data for its prediction algorithm; or a firm that strives to offer road maintenance and would need access to aggregated in-car sensor data on the road quality for this purpose. To the extent that bundled individual level data or aggregated data is not available through, say, a data pool established by a larger number of car owners, machine users or an intermediary (see part F(IV)(6)(e)), the complementary service provider would need to turn directly to the data holder for data access, i.e. the firm active on the primary market. Article 6 No. 11 DMA, which will oblige gatekeepers, who offer online search engines as a core platform service to provide competing online search engine providers with access to ranking, query, click and view data in relation to searches generated by end users, may be an example for a case where access to a large pool of data is needed to enter the primary market to compete.

Sometimes, competitors will request access to data which are not usage data. the Bundeskartellamt's DB mobility proceeding provides an example: in this case, mobility platforms request access to the Deutsche Bahn's real-time data about train departures and in

[405] Cf. Crémer/de Montjoye/Schweitzer, Competition Policy for the digital era, Final report, 2019, p. 25-26: sets of anonymously used individual-level data are typically needed to extract (prediction) patterns out of usage data, but the goal is not to directly provide a service to the individual who generated the data in the first place. For example, with individual-level usage data of a significant amount of subscribers to a video streaming platform, one could train a neural network to make good movie recommendations based on the favourite movies of any given user.

[406] Crémer/de Montjoye/Schweitzer, Comptition Policy for the digital era, Final report, 2019, p. 26: "aggregated data, refers to more standardised data that has been irreversibly aggregated. This is the case for e.g. sales data, national statistics information, and companies' profit and loss statements. Compared to anonymous use of individual-level data, the aggregation is standard enough that access to the individual-level data is not necessary."

order to enable users to find and book the best connection to a given destination across all means of transportation (see on this case b).[407]

In well-functioning, fully competitive markets, access to the necessary bundled and aggregated datasets could arguably be expected to be made available by the data controller at an efficient market price. Where the market for the primary product or service is fully competitive, firms active on that market should again be expected to develop different approaches to data openness that cater to the different preferences of their customers. Open systems would try to convince their customers with their broad range of diverse complementary services offered on competitive aftermarkets. Closed systems would point to the benefits of a more controlled aftermarket environment, possibly with higher quality standards and a higher degree of cybersecurity.[408] Also, a higher commitment to privacy standards may be an argument for not passing on customer usage data, even in the aggregate form.

However, the possibilities for market failures are manifold. In principle, they resemble those identified for the data portability scenario: dominant data holders may be reluctant to grant access to their data where these data may contribute to the entrenchment of their monopoly position on the primary market or allows them to enjoy competitive advantages when expanding into neighbouring markets. Furthermore, information asymmetries between suppliers and their customers and bounded rationality may lead customers to accept 'data-closed' environments even where this may lead to a durable and costly 'lock-in'.

(a) The applicability of the EFD to data

The question of when a dominant undertaking's denial of access to data would – under EU or national competition law – constitute an abuse continues to be debated.[409]

---

[407] Bundeskartellamt, Proceeding against Deutsche Bahn AG - Bundeskartellamt examines possible anticompetitive impediment of mobility platforms (Press release of 28.11.2019), https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2019/28_11_2019_DB_Mobilitaet.html (last visited 4.7.2022).

[408] On the comparison of the pros and cons of open vs closed systems see, inter alia, Shapiro/Varian, Information Rules: A Strategic Guide to the Network Economy, 1998, p. 148; Autorité de la concurrence/CMA, The economics of open and closed systems, 2014, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/387718/The_economics_of_open_and_closed_systems.pdf (last visited 4.7.2022).

[409] See, *inter alia*, Crémer/de Montjoye/Schweitzer, Competition Policy for the digital era, Final report, 2019, p. 98 et seq.; Schweitzer/Haucap/Kerber/Welker, Modernisierung der Missbrauchsaufsicht für marktbeherrschende Unternehmen, 2018, p. 162 et seq.; Schallbruch/Schweitzer/Wambach, Ein neuer Wettbewerbsrahmen für die Digitalwirtschaft, Bericht der Kommission Wettbewerbsrecht 4.0, p. 36-37; Graef/Tombal/de Streel, Limits and Enablers of Data Sharing: An Analytical Framework for EU Competition, Data Protection and Consumer Law, TILEC Discussion Paper No. DP 2019-024, p. 13 et seq.

The academic debate has heavily focused on the question whether[410] and under which preconditions the EFD will apply, and whether it should be adjusted or refined when applied to data.[411]

A significant part of the debate revolves around the indispensability criterion: generally, data – like any other resource – can, in a given situation, be an input that is essential for competing effectively.[412] While there may be substitutes for many datasets,[413] some data are unique. The uniqueness can result from the uniqueness of the product or service that the dominant undertaking provides and to which the data pertains. This will typically be the case where the undertaking is a monopolist on the relevant market. As the IoT gains traction, the uniqueness of bundled individual level or aggregate usage data may result from the control of a primary product which generates the usage data. Even where the portability of individual level data may be ensured in such cases in the future (see the Draft Data Act– on this: part F(I)), the producer or provider of the primary product may be the only undertaking with access to the bundled individual level or aggregate data – which may be needed to provide predictive maintenance services or to develop competitive complementary services.

The lack of substitutes for some types of datasets will not suffice for establishing the indispensability of access under the EFD, however. Generally, the preconditions for applying the EFD are strict.[414] Some unique datasets may be substitutable by others. 'Raw data' may be substitutable by 'derived data'. Assessing the substitutability of datasets may be a very difficult task.[415] Given the non-rivalry of the use of data and the fact that many datasets are not protected

[410] Schmidt, Zugang zu Daten nach europäischem Kartellrecht, 2020; Graef, Data as Essential Facility, 2016.

[411] See, for example, Crémer/de Montjoye/Schweitzer, Competition Policy for the digital era, Final report, 2019, p. 98 et seq.; Graef, Data as Essential Facility, 2016; Graef/Tombal/de Streel, Limits and Enablers of Data Sharing: An Analytical Framework for EU Competition, Data Protection and Consumer Law, TILEC Discussion Paper No. DP 2019-024, p. 14 et seq.; Graef, Rethinking the Essential Facilities Doctrine for the EU Digital Economy, TILEC Discussion Paper No. DP2019-028, p. 19-23; Drexl JIPITEC 2017, 257 (280 et seq.); Schweitzer/Haucap/Kerber/Welker, Modernisierung der Missbrauchsaufsicht für marktbeherrschende Unternehmen, 2018, p. 171; Feasey/de Streel, Data Sharing for Digital Markets Contestability, CERRE Report 2020; Martens et al. JRC121336 (2020), 35 et seq.; Schmidt, Zugang zu Daten nach europäischem Kartellrecht, 2020.

[412] Crémer/de Montjoye/Schweitzer, Competition Policy for the digital era, Final report, 2019, p. 101 et seq. The German legislator has clarified the essential facilities doctrine in this regard. In the course of the 10th amendment to the GWB, § 19(2) No. 4 GWB was amended to specify that data can qualify as 'essential facility'. This amendment is generally perceived to be purely declaratory in nature: see, inter alia, Körber NZKart 2019, 633 (634).

[413] According to the Special Advisors' report, the substitutability of data may also depend on the type of data at issue: e.g. volunteered data will possibly be provided again, personal data could be retrieved under the framework of Article 20 GDPR, or IoT data may be accessed in the future with the data access rights set forth in the Data Act. See Crémer/de Montjoye/Schweitzer, Competition Policy for the digital era, Final report, 2019, p. 101 et seq. Especially in merger cases, the Commission has often argued that there are comparable datasets available on the market for purposes of e.g. targeted advertisement or for improving existing or developing new products (see part E(IV)(2)(b)).

[414] See Mestmäcker/Schweitzer, Europäisches Wettbewerbsrecht, 3rd ed. 2014, § 19 paras. 66-80.

[415] Drexl JIPITEC 2017, 257 (281): "since even the petitioner for access, such as a big data analyst, will often only have a vague understanding about the kind of data contained in the dataset and about which data will produce the most valuable new information based on observable correlations."

by full-scale property rights, but merely by trade secrets, some have proposed to generally lower the indispensability threshold for data access. According to this view, a dominant undertaking's interest in an exclusive data use may be less worthy of protection, and a refusal to grant access to data may, therefore, more easily qualify as an exclusionary abuse. This may be true, in particular, where access can be granted in a way that respects trade secrets.

However, while mandating access to data may improve competition on a downstream market in the short term, this improvement must be balanced against the negative incentive effects on the dominant firm that may result from a requirement to share. For example, the dominant firm may no longer be willing to invest in data collection in the first place.[416] Also, where access to an input is granted, competitors are relieved from the need to compete on the primary market. More competition downstream may, therefore, come at the cost of durable entrenchment of market power upstream. Furthermore, access remedies frequently require the precise specifications of access conditions and price as well as intense and constant oversight within a framework that can come to resemble a regulatory scheme. Against this background, the question whether any given input qualifies as an 'essential facility' in any given case must be analysed with caution.

Another part of the debate relates to the applicability of the so-called 'new product rule' to access to data cases. In cases that concerned refusals by a dominant undertaking to license intellectual property rights, the CJEU has applied the EFD, but with an additional requirement that access must be granted only where access is indispensable to offer a new product.[417] However, the 'innovation threshold' to be applied has never been particularly clear and has been diluted over time. In *Microsoft*, the General Court merely required showing that the refusal to grant access was prone to limiting the technical development to the prejudice of consumers (Article 102, 2nd sentence, lit. a TFEU).[418] This should be the standard also in access to data cases – all the more since data are not generally protected by property rights (see above, part E(I)).[419]

---

[416] For a need to precisely examine the incentive effects case by case, see de Streel, Essential Facilities Doctrine in the data-driven economy, presentation for FSR and FCP Annual Scientific Seminar in Florence on 22.3.2018, https://www.slideshare.net/FSRCommunicationsand/essential-facilities-doctrine-in-the-datadriven-economy-alexandre-de-streel (last visited 4.7.2022).

[417] See Joined Cases C-241/91 P and C-242/91 P, *RTE and ITV v Commission ('Magill')*, ECLI:EU:C:1995:98; Case T-184/01, *IMS Health II*, ECLI:EU:T:2001:259; Case C-418/01, *IMS Health*, ECLI:EU:C:2004:257 and Case T-201/04, *Microsoft*, ECLI:EU:T:2007:289.

[418] See Case T-201/04, *Microsoft*, ECLI:EU:T:2007:289.

[419] Against the application of a 'new product rule' see Crémer/de Montjoye/Schweitzer, Competition Policy for the digital era, Final report, 2019, p. 106 et seq. See also Feasey/de Streel, Data Sharing for Digital Markets Contestability, CERRE Report 2020, p. 37, in favour of a 'consumer harm approach': it should be examined whether, for consumers, the negative consequences of refusing to share data outweigh the negative consequences of mandating data access under competition law. Similarly: Graef/Tombal/de Streel, Limits and Enablers of Data Sharing: An Analytical Framework for EU Competition, Data Protection and Consumer Law, TILEC Discussion Paper No. DP 2019-024, p. 15 et seq.

To this academic debate, the German legislator has reacted by amending § 19(2) No. 4 GWB, which codifies the preconditions for applying the EFD under German competition law. The provision now specifies that, absent an objective justification, a refusal to grant access to data against reasonable remuneration – such as a refusal to grant access to networks and other infrastructure facilities[420] – will constitute an abuse where such access is objectively necessary for becoming active on an upstream or downstream market and where the refusal threatens to eliminate effective competition on that market. Apart from an explicit mentioning of data, the 10th amendment to the GWB has come with some additional changes of the text of § 19(2) No. 4 GWB:[421]

- Whereas in the previous version of the GWB, access had to be 'legally or factually impossible', it must now be 'objectively necessary' in order to operate in an upstream or downstream market;
- The condition that the facility owner operate 'as a competitor' in the relevant upstream or downstream market has been abandoned;
- The criterion that 'the refusal threatens to eliminate effective competition on that market' was introduced.

Although these amendments to § 19(2) No. 4 GWB are mostly considered to be declaratory adjustments of the German version of the EFD to the CJEU's EFD jurisprudence, some questions remain debated:

- A debate has emerged whether § 19(2) No. 4 GWB will only apply to data that has been commercially traded before.[422] Given a clear case law on the EFD at the EU level according to which the doctrine applies irrespective of whether the dominant undertaking has already opened a market for the relevant input, this would come as a surprise.[423]
- In view of the deletion of the 'as competitor'-requirement, the question has been raised whether § 19(2) No. 4 GWB applies only if there is a vertical relationship between the activities of the data holder and the activities of the access seeker, or whether § 19(2) No. 4 GWB applies to activities in all markets in which the data is necessary to operate.[424] In direct opposition to the

[420] Such as platforms, interfaces and intellectual property rights, see Bundestag publication 19/23492, p. 27.

[421] See Brenner in Bien et al., Die 10. GWB-Novelle, 2021, Ch. 1 paras. 102 et seq.

[422] Criticizing the wording of § 19(2) No. 4 GWB in this regard (the dominant undertaking has to deny access 'as a supplier or purchaser', and the data has to be necessary in order 'to operate') and demanding clarifications: Höppner/Weber K&R 2020, 24 (46); Schweda/Schreitter WuW 2021, 145 (152). Generally on the debate whether the EFD should only apply if the data has been traded before, see Feasey/de Streel, Data Sharing for Digital Markets Contestability, CERRE Report 2020, p. 36; Graef/Tombal/de Streel, Limits and Enablers of Data Sharing: An Analytical Framework for EU Competition, Data Protection and Consumer Law, TILEC Discussion Paper No. DP 2019-024, p. 15.

[423] Some refer to § 20(1a)(3) GWB to support this argument: "This shall also apply even if such data have not yet been commercially traded." There is no reason why an undertaking with only 'relative market power' should be exposed to a more extensive liability – see Schmidt, Zugang zu Daten nach europäischem Kartellrecht, 2020, p. 551; Schweda/Schreitter WuW 2021, 145 (152).

[424] Some argue that, in order to prevent § 19(2) No. 4 GWB from losing its contours, it may be necessary to introduce some form of limitation – see Brenner in Bien et al., Die 10. GWB-Novelle, 2021, Ch. 1 para. 122 with further references in fn. 234. Otherwise, the 'special responsibility' of the dominant undertaking could be stretched too far and translated into a general obligation to promote innovation with far-reaching practical implication for the norm addressee. In any case, data access for the sole purpose of reselling would fall outside the scope of § 19(2) No. 4 GWB (Brenner in Bien et al., Die 10. GWB-Novelle, 2021, Ch. 1 para. 115). See also: Weber WRP 2020, 559 (562). Others argue that the particularities of data may require a reading independent of

legislator's explicit intention, Körber has argued that the 'as competitor' requirement would continue to apply, given the aim of § 19(2) No. 4 GWB to enable competition with the facility holder in adjacent markets and prevent the monopolisation of adjacent markets.[425]

- The standard for assessing whether data access is 'objectively necessary' to compete in an upstream or downstream market has remained somewhat controversial.[426]

Simultaneously, there is broad consensus that the 'new product' rule that the CJEU has developed to limit the scope of the EFD when it comes to a compulsory licensing of IP rights under EU competition law is not part of the test as it is set out in § 19(2) No. 4 GWB.[427]

(b) Relevant case law

The intense academic debate on the role and scope of the EFD as applied to data has not been followed up by relevant cases. The 'access to data' cases that have been decided on the basis of the EFD so far are old ones.[428] Cases relating to the new realities of the data economy are hard to find. To our knowledge, no Article 102 TFEU 'access to data' case is currently pending before the European Commission.

The Bundeskartellamt, for its part, is investigating the DB Mobility case – but the case will likely not be based on § 19(2) No. 4 GWB. Nonetheless, the DB Mobility case is an interesting example of when and how a refusal to grant access may amount to an abuse of dominance. On 20 April 2022, the Bundeskartellamt has issued a statement of objection against Deutsche Bahn with a view to a possible hindrance of mobility platforms – inter alia, by refusing to provide

---

the notions of upstream and downstream markets: Given the wide variety of purposes for which data can be used, any market could be regarded as upstream or downstream from the relevant data market – see Schweda/Schreitter WuW 2021, 145 (151). In the end, a difficult balancing act must be carried out between the realization of potentially far-reaching data-based business opportunities without direct reference to the data owner's activities and the data owner's legitimate interests – see Brenner in Bien et al., Die 10. GWB-Novelle, 2021, Ch. 1 para. 115.

[425] Körber FS Wiedemann, 2020, 559 (562); see also Körber, Die Digitalisierung der Missbrauchsaufsicht durch das „GWB-Digitalisierungsgesetz" im Spannungsfeld von moderater Anpassung und Überregulierung, 2020, https://ssrn.com/abstract=3543719 (last visited 4.7.2022), p. 13, 15 et seq.

[426] Most authors argue that data access is 'objectively necessary' if the available data cannot be reproduced with reasonable effort – see Brenner in Bien et al., Die 10. GWB-Novelle, 2021, Ch. 1 para. 108; Schweda/Schreitter WuW 2021, 145 (147); Weber WRP 2020, 559 (562). According to Körber, data access cannot be considered 'objectively necessary' if market access is possible via comparable data sets – even if the data is non-replicable – Körber FS Wiedemann 2020, 361 (363 et seq.); see also Körber, Die Digitalisierung der Missbrauchsaufsicht durch das „GWB-Digitalisierungsgesetz" im Spannungsfeld von moderater Anpassung und Überregulierung, 2020, https://ssrn.com/abstract=3543719 (last visited 4.7.2022), p. 8.

[427] Brenner in Bien et al., Die 10. GWB-Novelle, 2021, Ch. 1 para. 109; Weber WRP 2020, 559 (561). This is contested by Körber, however, who argues that the 'new product rule' nevertheless applies because it has been developed in case law and is generally approved – see Körber, Die Digitalisierung der Missbrauchsaufsicht durch das „GWB-Digitalisierungsgesetz" im Spannungsfeld von moderater Anpassung und Überregulierung, 2020, https://ssrn.com/abstract=3543719 (last visited 4.7.2022), p. 10.

[428] See, for example Joined Cases C-241/91 P and C-242/91 P, *RTE and ITV v Commission ('Magill')*, ECLI:EU:C:1995:98 on a refusal to provide access to lists of television programmes that were protected by a copyright under national law. See on these cases Drexl, Designing Competitive Markets for Industrial Data: Between Propertisation and Access, Max Planck Institute for Innovation and Competition Research Paper No. 16-13, p. 45 et seq.

them with in-time train traffic data. Mobility platforms offer online solutions for integrated route planning across various means of transportation, including rail. For the quality and usefulness of such services, forecast data on passenger rail services – including, in particular, information on delays, cancellations or platform changes – are of the essence. The data is exclusively held by DB. DB refuses to provide such data to mobility platforms, however. Instead, DB – which offers a mobility platform itself, namely bahn.de and the app 'DB Navigator' – reserves these data to itself. In addition, some selected mobility service providers such as Google receive preferential treatment. The proceeding against DB is based both on Article 102 TFEU and on §§ 19, 20 GWB. The Bundeskartellamt has not yet specified the precise category of abuse on which the case will be based. The facts which have been made public suggest that this will not be an EFD case, however. Rather, there appears to be an element of discrimination between business partners – with a preferred treatment for Google. Also, § 20(1a) GWB may play a role. Whether the Bundeskartellamt will try to base its case on an abusive self-preferencing is unclear.

The relevance of the DB Mobility case notwithstanding, the dearth of cases and complaints regarding refusals to grant access to data in scenario 2-settings is striking. A number of explanations seem plausible. Firstly, the data economy is still at an early stage. Many firms are struggling with making good use of the data that they themselves control. Experimenting with huge 'external' data troves is beyond what they can and want to do at this stage. Also, requests for data access would presuppose a relatively well-defined idea of what to do with the data. Such projects may be lacking at this point of time, given that market actors have not yet been able to gather sufficient experience. Frequently, the whole purpose of data access would be to enable them to experiment – which may not be sufficient for requesting access to data under Article 102 TFEU/§§ 19, 20 GWB. Secondly, developing more specific projects of what could be done with bundled individual level or aggregate data may presuppose more precise information about the types of usage data that the dominant data holder controls. At this moment, data holders – even dominant ones – are not required to provide such information. Thirdly, data holders will collect, structure and format data with a view to the business purposes they pursue. It may not be easy to make good use of the data for different purposes. The common comparison of 'raw data' with 'raw oil' may be misleading in this regard. Fourthly, at least when it comes to very large and diverse data troves of the kind that the large consumer-facing digital platforms control, potential competitors may lack the data processing capabilities, the skills and the specialized and experienced data science staff to put these resources to good use.

Overall, it seems quite unlikely that the inherent constraints of the existing EFD are to be blamed for the slow increase of the new possibilities of the emerging data economy. The friction seems to lie somewhere else. A focus on strengthening effective data portability in relevant sectors (scenario 1 – see above) and on data access within data-driven ecosystems may be of greater practical relevance at this stage (see part F(II)(2)(b)). Empowering undertakings to process data in these settings may allow them to learn and acquire the skills that are needed to later expand data-driven business models.

(c) Refusals to grant access to data in data-driven value-creation networks and ecosystems/discriminatory access to data and self-preferential access in data-driven networks

While the EFD may provide an appropriate framework for some – but arguably limited number of – settings, it is not the sole framework for analysing situations in which access to data held by a dominant undertaking is at issue.[429]

In *Google Shopping*,[430] the General Court has found that, while the case could be construed as one about equal access to Google's general search results pages, and hence as an EFD case, this did not preclude the possibility of looking at Google's conduct from a different angle and finding that the practice at issue met the preconditions of an independent form of abuse distinct from that of a refusal to supply.[431] In *Google Shopping*, the abuse consisted in an "active behaviour in the form of positive acts of discrimination in the treatment of the results of Google's comparison shopping service, which are promoted within its general results pages, and the results of competing comparison shipping services, which are prone to being demoted" (at para. 240) – and hence in an 'internal discrimination' which amounted to a "leveraging from a dominant market characterised by high barriers to entry, namely the market for general search services" (at para. 237). In such a case, the relevant conduct may qualify as an abuse without the EFD's 'indispensability' criterion being met. Furthermore, the General Court emphasized that – where a platform has gained a dominant position based on a model of openness to all content providers and the promise to rank results based on their presumed relevance for search engine users, and where this promise are the source of the relevant network effects and economies of scale that now significantly reduce contestability – a change of that model, and the pro-active preferencing of their own content, could also vindicate the finding of an abuse.

While none of these considerations directly relate to 'access to data' issues, *Google Shopping* does show that the abuse analysis may need to be reconsidered in settings where a gatekeeper controls access to data which significantly affects the ability to compete in a data-driven ecosystem. This is so, in particular, because the EFD's indispensability requirement may not be very meaningful in these settings. At least at this stage of development of the data economy, access to a given dataset alone will frequently not be absolutely indispensable to compete. In a broader and more holistic perspective, it may nonetheless raise the barriers to entry and expansion so significantly that an exclusionary effect is likely to result, or at least be

[429] For this see already: Crémer/de Montjoye/Schweitzer, Competition policy for the digital era, Final report, 2019, p. 98 et seq.: the criteria are only proxies for the fundamental cost-benefit analysis underlying the antitrust case-law on the duty to deal, i.e. whether the positive effects of entry by an access seeker on competition, innovation, diversity and choice in the secondary market outweigh the reduced investment incentives of the data holders and of access seekers to collect data themselves. See also: Graef/Tombal/de Streel, Limits and Enablers of Data Sharing: An Analytical Framework for EU Competition, Data Protection and Consumer Law, TILEC Discussion Paper No. DP 2019-024, p. 16. See also Feasey/de Streel, Data Sharing for Digital Markets Contestability, CERRE Report 2020, p. 37 et seq. Others have argued that the structured balancing of interests as developed by the CJEUin Bronner must be applied to access to data cases – see, for example, Schmidt, Zugang zu Daten nach europäischem Kartellrecht, 2020, p. 381 with further references at fn. 138 at the same page.

[430] Case T-612/17, *Google Shopping*, ECLI:EU:T:2021:763.

[431] Id., paras. 220 et seq.

strengthened. The combined effect of an exclusive access of a large and dominant ecosystem orchestrator to data generated in the context of the ecosystem, together with strong positive network effects, economies of scale etc. may otherwise be used to entrench established bottleneck positions for a long time and to reinforce the potential for anti-competitive platform envelopment strategies. In particular, (i) data from one machine user may lead to positive externalities for other machine users (e.g. more effective maintenance based on a predictive AI algorithm), and (ii) data may provide a competitive advantage not only in the market for secondary goods, but also when it comes to the replacement of the machine, as competitors have less information on which to base their offers.[432] In focusing on data portability only, and largely excluding access of third parties to bundled individual level or aggregate data, both the DMA and § 19a GWB may, therefore, not fully address the data-related competition law problems (see part E(V)). Along these lines, smart device manufacturers and consumer IoT service providers expressed competition concerns about the strong position of voice assistants at the centre of data collection in the consumer IoT in the recent sector inquiry into the consumer IoT sector. They consider, *inter alia*, that the limits on the data they receive from leading voice assistant providers hinder them in their own business development.[433] Furthermore, privileged access to data allows voice assistant providers to more easily improve the quality of their services, thus raising barriers to new entrants on the voice assistant market and hindering the development of smaller competitors.[434] According to the Final Report on the sector inquiry, these concerns, if linked to anti-competitive practices, may lead to future investigations under competition law or inform legislative reform projects like the DMA.[435]

Simultaneously, within a competition law framework, a highly context-specific balancing of interests will be required, with an emphasis on an analysis of the likely foreclosure effects in a given setting. In data-driven markets, the exclusive control over the usage data of a product or service will automatically lead to significant competitive advantages of the data holder for all related complementary or aftermarket services, irrespective of whether that data holder holds a dominant position on a broader market for such products or services. Nonetheless, the efficiencies related to 'closed systems' strategies should arguably be recognised – also under the novel conditions of the data economy. Not every data-related lock-in should lead to the acknowledgment of a dominant position on a narrowly defined 'aftermarket'. A small IoT system provider's refusal to grant access to data may need to be assessed differently from a dominant gatekeeper that controls access to consumers across many markets.

---

[432] Kerber/Frank, Data Governance Regimes in the Digital Economy: The Example of Connected Cars (3.11.2017), https://ssrn.com/abstract=3064794https://ssrn.com/abstract=3064794 (last visited 4.7.2022). However, Kerber/Frank also note that providing data might reveal some of the intellectual property rights of the machine user, which could argue for some restriction of data access.

[433] COM(2022) 19 final, para. 42.

[434] Id., para. 44. See also SWD(2021) 144 final, paras. 418 et seq.

[435] COM(2022) 19 final, paras. 51 et seq.

The traditional **aftermarket doctrine** may, therefore, need to be further refined with a view to the specifics of data, in particular in the IoT and digital ecosystem context.[436] The stakeholder contributions to the European Commission's ongoing evaluation of the market definition notice[437] indicate that there is a need for more clarity and explanations of the European Commission's practice with regard to the aftermarket doctrine.[438] More recent decisions (e.g. *CEAHR v Commission*[439]) may provide a starting point for developing a conceptual framework that may identify the factors to be considered in establishing whether the provider of an IoT product or a digital ecosystem orchestrator is to be considered a monopolist on a (hypothetical) market for data that is generated by the product or service.[440]

bb) Other data-related abuses

Data-related abuses of dominance are not limited to refusals to grant access to data. Given the focus of our study, we will touch only briefly on other data-related theories of harm.

(1) The obstruction of competitors in their endeavours to collect data

Some undertakings – in particular those undertakings that have recently been subjected to special gatekeeper regulation (DMA) or ecosystem regulation (§ 19a GWB) – may have the ability to obstruct third parties in collecting data on the internet. In 2021, Apple came under competition law scrutiny because of its App Tracking Transparency framework, which requires apps to obtain user permission for tracking through a pop-up window.[441] Based on similar concerns, the CMA looked into Google's plan to remove third party cookies (TPCs) on its

---

[436] Crémer/de Montjoye/Schweitzer, Comptition Policy for the digital era, Final report, 2019, p. 87 et seq., 101 et seq., 125; Kerber/Frank, Data Governance Regimes in the Digital Economy: The Example of Connected Cars (3.11.2017), https://ssrn.com/abstract=3064794https://ssrn.com/abstract=3064794 (last visited 4.7.2022). See also Schweitzer, GRUR 2019, 569 (578 et seq.).

[437] See OJ 1997 C 372, 3, at para 56. The Commission currently revises the Market Definition Notice, see European Commission, Competition: Commission consults stakeholders on the Market Definition Notic (Press release of 26.6.2020) https://ec.europa.eu/commission/presscorner/detail/en/IP_20_1187 (last visited 4.7.2022).

[438] SWD(2021) 199 final, 52 et seq.

[439] Case T-427/08, *CEAHR v Commission*, ECLI:EU:T:2010:517.

[440] See also European Commission, Summary of the stakeholder consultation to the Evaluation of the Market Definition Notice, 2020, p. 21. European Commission, Support study accompanying the evaluation of the Commission Notice on the definition of relevant market for the purposes of Community competition law, Final report 2021, p. 84 et seq. points out that digital ecosystems, in particular user facing services, can take the form of aftermarkets and can be regarded as a primary core product and several secondary products whose complementarity is created through technical means or interoperability between products. To define a secondary market under the aftermarket doctrine, it is necessary that there is no interoperability between secondary products of different systems. However, the study does not specifically address the importance of data for applying the aftermarket doctrine. 'Data as such' is only analysed in more general terms for the assessment of market power.

[441] Bundeskartellamt, Bundeskartellamt reviews Apple's tracking rules for third-party apps (Press release of 14.6.2022), https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2022/14_06_2022_Apple.html?nn=3591568https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2022/14_06_2022_Apple.html?nn=3591568 (last visited 4.7.2022).

Chrome browser and replace their functionality with a range of 'Privacy Sandbox' tools.[442] The CMA ultimately closed the case based on commitments offered by Google to, *inter alia*, establish a public stakeholder engagement process to allow advertisers, publishers, ad tech providers and consumer groups to engage in the development and implementation of the 'Privacy Sandbox'.[443]

Furthermore, the Italian AGCM has launched an Article 102 TFEU investigation into Google's data access policies on the market for online advertising. Google allegedly denies its competitors access to its ID decryption keys and to third-party tracking pixels for the targeting of their display advertising campaigns, while at the same time using data collected through its various applications, in particular through tracking elements enabling its advertising intermediation services, to achieve a higher targeting capability. In such a setting, equally efficient competitors may not be able to compete effectively without being granted access to Google's vast amount of data on non-discriminatory grounds.[444]

An abuse of dominance may also be considered where digital platforms do not supply their business users with sufficient data on the competitive dynamics on the marketplace. Businesses who offer their products and services via digital platforms frequently lose the direct contact to the consumers they serve. A dominant platform may then be required to grant access to the data generated on the platform to an extent that enables business users to adjust their offers to the preferences of consumers and to innovate. Restrictions on such access may be justified to the extent this is necessary to protect against the free riding of business users on the platform's investment. However,such measures must be proportionate to the risks.

(2) A platform's seizing of business opportunities developed by platform business users based on the processing of 'their' data

In another group of cases, platforms have (allegedly) used data generated by the business users' activity on their platform to the benefit of their own retail activity on the platform. For example, independent retailers on the Amazon Marketplace have complained that Amazon gains a

---

[442] CMA, CMA to investigate Google's 'Privacy Sandbox' browser changes (Press release of 8.1.2021), https://www.gov.uk/government/news/cma-to-investigate-google-s-privacy-sandbox-browser-changeshttps://www.gov.uk/government/news/cma-to-investigate-google-s-privacy-sandbox-browser-changes (last visited 4.7.2022); see also Cowen/Barraclough/Koran, "Privacy Fixing" After Texas et al v. Google and CMA v. Google (Privacy Sandbox): Approaches to Antitrust Considerations of Privacy (26.1.2021), https://www.competitionpolicyinternational.com/privacy-fixing-after-texas-et-al-v-google-and-cma-v-google-privacy-sandbox-approaches-to-antitrust-considerations-of-privacy/https://www.competitionpolicyinternational.com/privacy-fixing-after-texas-et-al-v-google-and-cma-v-google-privacy-sandbox-approaches-to-antitrust-considerations-of-privacy/ (last visited 4.7.2022); Geradin/Katsifis/Karanikioti, Google as a de facto Privacy Regulator: Analyzing Chrome's Removal of Third-party Cookies from an Antitrust Perspective, TILEC Discussion Paper No. DP2020-034, https://ssrn.com/abstract=3738107 (last visited 4.7.2022).

[443] CMA 11.2.2022, Case 50972, Decision to accept commitments.

[444] AGCM, A542 - ICA: investigation opened against Google for an alleged abuse of dominant position in the Italian market for display advertising (Press release of 28.10.2020), https://en.agcm.it/en/media/press-releases/2020/10/A542https://en.agcm.it/en/media/press-releases/2020/10/A542 (last visited 4.7.2022).

competitive advantage for its own retail activities on the platform by utilizing aggregated data regarding user search and click behaviour on the marketplace.[445] Similar accusations were made by app developers against Apple's App Store. Purportedly, Apple collects sensitive information about popular apps and then develops competing apps or integrates the popular app's functionality into iOS (so-called 'Sherlocking').[446]

Article 6 No. 2 DMA now prohibits gatekeepers from using data provided or generated by business users in the context of their use of the core platform service and which is not publicly available, in competition with those business users. Similarly, § 19a(2), 1st sentence, No. 4 lit. b GWB empowers the Bundeskartellamt to prohibit a designated norm addressee from processing competitively relevant data sourced from other undertakings for purposes that go beyond what is necessary to provide their services to these undertakings. For a further-reaching agreement to be valid, the undertakings must be granted sufficient choice regarding the circumstances, purposes and ways of data processing by the norm addressee.

(3) Data access remedies to address abusive combinations or uses of data by dominant firms?

Yet another group of cases of data-related abuses of dominance is concerned with the way a dominant undertaking collects, combines or uses its data troves. The most prominent case in this category is the Bundeskartellamt's proceedings against Facebook.[447] According to the Bundeskartellamt, Facebook's practice of combining, without the users' valid consent under the GDPR, personal data sourced from the social network with personal data sourced from other services, including WhatsApp and Instagram, but also from third parties services, constituted an abuse under § 19(1) GWB. In a preliminary proceeding, the BGH has upheld the Bundeskartellamt's finding, but without relying on the alleged invalidity of the users' consent under the GDPR. Rather, the BGH found that an abuse under the general clause of § 19(1) GWB may follow from the use of general terms and conditions by a dominant undertaking that restrict their customers' freedom of choice between a service based on the personal data generated on Facebook alone and a service based on a broader set of data services, where this restriction simultaneously tended to obstruct competition. An overall interest balancing will be

[445] The European Commission is currently investigating this conduct, see Case AT.40462 – *Amazon Marketplace* (pending). See also European Commission, Antitrust: Commission opens investigation into possible anti-competitive conduct of Amazon (Press release of 17.7.2019) https://ec.europa.eu/commission/presscorner/detail/en/ip_19_4291 (last visited 4.7.2022). On the antitrust hearing before the U.S. Congress, see i.a. Washington Post Online, Amazon may have used proprietary data to compete with its merchants, Bezos tells Congress (30.7.2020), https://www.washingtonpost.com/technology/2020/07/29/bezos-testimony-data-antitrust/https://www.washingtonpost.com/technology/2020/07/29/bezos-testimony-data-antitrust/ (last visited 4.7.2022).

[446] Subcommittee on Antitrust, Commercial and Administrative Law of the Committee on the Judiciary, Majority Staff Report and Recommendations (2020), 361 et seq.

[447] See Bundeskartellamt 6.2.2019, B6-22/16 – *Facebook*, and BGH 23.6.2020, KVR 69/19 – *Facebook*, effectively upholding the decision.

required to establish whether the goal to protect competition prevails over the legitimate interests of the dominant firm.[448]

The German legislator has meanwhile broadened the § 19(1) GWB provision: following the 10th amendment to the GWB, a violation of a law that is meant to protect the other market side from some sort of heteronomy or unfair treatment will amount to an abuse where the conduct is engaged by a dominant undertaking. The causality of the norm addressee's market power for the resulting disadvantages for the other side of the market is thought to follow from the fact that their outside options are constrained by the norm addressee's dominance.[449] This theory of harm may significantly impact the review of a dominant company's contract terms under German competition law in the future. For example, an unlawful restriction of a data subject's right to port personal data under Article 20 GDPR would simultaneously amount to an abuse under § 19(1) GWB. Similarly, to the extent that a combination of usage data that flow from the usage of different services without informed consent by the data subject would infringe Article 6(1) lit. a with Article 7(4) GDPR – and not be covered by Article 6(1) lit. b GDPR –, the GDPR violation would be accompanied by a violation of § 19(1) GWB.

Simultaneously, Article 5 No. 2 lit. a DMA will prohibit designated gatekeepers from, inter alia, combining personal data sourced from a core platform service with personal data from other core platform services or from any other service provided by the gatekeeper or from third party services; and/or cross-using personal data from a core platform services in other services provided separately by the gatekeeper; and/or the signing-in of end users to other services of the gatekeeper in order to combine personal data in the absence of specific choice and valid consent under Article 4 No. 11 and Article 7 of the GDPR. And § 19a GWB empowers the Bundeskartellamt to prohibit an undertaking of paramount cross-market significance for competition from making the use of its services dependent on the users' consent to the processing of data sourced from other services of the norm addressee or from third parties; or to process competitively relevant data collected by the norm addressee in ways that noticeably raise barriers to entry.

There is no case law under general EU competition law, however, that would clarify the conditions under which this type of conduct would constitute an abuse. Data-related conduct may qualify as an exclusionary abuse where it leads to an anti-competitive foreclosure of competitors. However, a theory of harm according to which a deprivation of the demand side of its freedom of choice will constitute an abuse of dominance if such a conduct comes with a potential for exclusionary effects has not yet been tested before the Union courts so far.

Whether and, if so, under what preconditions an abuse may be established in cases that are based on a dominant undertaking's practice of combining data from different sources or processing data in specific ways is not the subject of this study. However, what we do want to

[448] For an in-depth analysis of the case see Schweitzer JZ 2022, 16.

[449] See on this: Id., 21.

highlight is a certain mismatch between a theory of harm that relies on the combination of a deprivation of choice, combined with a potential for exclusionary effects, and a remedy which relies solely on a requirement of choice and valid consent to a combination or further-reaching processing of data. Such consent will restore freedom of choice, but the exclusionary potential remains. One may, therefore, ask whether a requirement for choice and valid consent should be combined with a requirement for requesting users to grant third parties with equal access to the combined data pool such as to enable them to compete effectively. Such a remedy would reach beyond the right to data portability as currently foreseen in Article 6 No. 9 DMA, and arguably also beyond what the empowerment of the Bundeskartellamt under § 19a(2), 1st sentence, No. 5 GWB (see further part F(II)(2)).

(4) Anti-competitive platform envelopment strategies

The theory of harm according to which depriving the demand side of its freedom to choose will constitute an abuse of dominance, if such a conduct comes with a potential for exclusionary effects lowers the burden of proving exclusionary effects. The literature on data-driven platform envelopment strategies[450] strives to define the preconditions for establishing data-related anti-competitive foreclosure on more traditional grounds, i.e. within the framework of 'pure' exclusionary abuses. In their joint paper on Competition Law and Data, the Autorité de la Concurrence and the Bundeskartellamt have considered that the use of data collected in one market for entering another market may amount to an abuse if the competitive advantage of exclusive access to the relevant data is so significant that competitors active on the second market are effectively foreclosed.[451] Such a competitive advantage may at times result not from the exclusive control of one dataset alone, but from the combination of such a dataset with other data. Both the cross-use of data collected in the provision of one service for the purpose of offering other services and the combination of different datasets will frequently be an issue where the data – whether personal or anonymised – relates to consumer behaviour and can therefore be used to predict consumer choices in different markets. It is in consumer-facing markets in particular that a data-driven prediction of consumer behaviour can be combined with specific choice architectures that may allow undertakings to steer consumer conduct.

The role of Article 102 TFEU and § 19 GWB in these settings is not yet clear. In principle, a cross-market use of data in line with the GDPR may constitute competition on the merits. In other settings, it may amount to an exclusionary abuse. This may be true in particular where the dominant undertaking has accumulated the data based on a bottleneck position that is based on strong network effects, as such dominance is not based on the superior quality of the dominant undertaking's offer alone. The superior quality rather results from the cumulative presence of other market actors on both sides of the platform and the difficulty of coordinated switching. If the access to data partly results from collaboration, the exclusive exploitation of this data advantage by the dominant undertaking with exclusionary effects may constitute an abuse. The

[450] Condorelli/Padilla J. Compet. Law Econ. 2020, 143.

[451] See Bundeskartellamt/Autorité de la Concurrence, Competition Law and Data, 2016, p. 20.

appropriate remedy in such cases may not be a renunciation of a cross-market use of data – but rather the granting of equal access to the data to competitors.

3. Data-related abuses of 'relative market power' – § 20(1a) GWB

a) § 20(1a) GWB as compared to § 19(2) No. 4 GWB

In Germany, a special focus has been on enabling undertakings to access data where such access is needed to compete in complementary or aftermarkets and to innovate. In an attempt to strengthen data access in these settings, a novel § 20(1a) GWB has been introduced with the 10th amendment to the GWB. Contrary to EU competition law, German competition law does not only prohibit abuses of dominance, but also abuses of so-called 'relative market power', i.e. abuses of a special type of bilateral dependency. According to § 20(1) GWB, the prohibition of abuse in § 19(1) and § 19(2) No. 1 GWB also applies to undertakings to the extent that other undertakings are dependent on them for the supply or purchase of certain types of goods or services. Such a dependency presupposes that these other undertakings have no sufficient and reasonable outside options for the supply or purchase of these goods or services and that the relationship is characterised by a significant imbalance of power. The new § 20(1a) GWB now recognises that bilateral dependency can arise from the fact alone that an undertaking is dependent on access to data controlled by another undertaking.[452] According to this provision, an undertaking may request access to data where it is '*dependent on* access to data controlled by another undertaking *for its own activities*' even 'if there is not yet a commerce opened for such data', i.e. even if the data controller has not marketed the data before.[453]

Like Article 102 TFEU/§ 19 GWB, § 20(1a) GWB can apply to data access requests of the scenario 1 type (i.e. requests for data portability of usage data in value creation networks) or the scenario 2 type (i.e. access to bundled individual data or aggregate data)[454] – as well as to other data access scenarios that may be caught by the open-ended wording of § 20(1a) GWB.[455]

With regard to requests for the porting of data which was generated by the use of a certain machine or service, § 20(1a) GWB would appear to typically oblige a data holder with 'bilateral power' to grant a petitioner access to those data if it is needed to provide competitive

---

[452] Schweitzer/Haucap/Kerber/Welker, Modernisierung der Missbrauchsaufsicht für marktbeherrschende Unternehmen, 2018, p. 192-93.

[453] Schweitzer/Haucap/Kerber/Welker, Modernisierung der Missbrauchsaufsicht für marktbeherrschende Unternehmen, 2018, p. 192-93.

[454] Bundestag publication 19/23492, p. 80 et seq. See Nothdurft in Bunte, Kartellrecht, 14th ed. 2022, § 20 GWB paras. 80 et seq.; Brenner in Bien et al., Die 10. GWB-Novelle, 2021, Ch. 1 paras. 137 et seq.; Markert/Podszun in Immenga/Mestmäcker, GWB, 7th ed. 2022, § 20 paras. 135 et seq. These scenarios can be traced back to Schweitzer/Haucap/Kerber/Welker, Modernisierung der Missbrauchsaufsicht für marktbeherrschende Unternehmen, 2018, p. 187 et seq., 190 et seq.

[455] Furthermore, it discussed to apply § 20(1a) GWB where dependence is based on intermediary services and where data is traded by the data access seeker, see Brenner in Bien et al., Die 10. GWB-Novelle, 2021, Ch. 1 paras. 137 et seq.; Markert/Podszun in Immenga/Mestmäcker, GWB, 7th ed. 2022, § 20 paras. 137, 140.

aftermarket or complementary services – provided that the relevant user consents. Where tailored aftermarket or complementary services presuppose access to individual level usage data, substitutes to those data will be lacking by definition.[456] Each case will remain subject to balancing of interests. With regard to individual level data generated by the use of a product, the practical relevance of § 20(1a) GWB will be reduced if the Draft Data Act were to enter into force, given that the Data Act would create a general portability right for the machine user, irrespective of market or bilateral power (see below, part F(I)). In the presence of bilateral power within the meaning of § 20(1a) GWB, such data portability rights would be mandatory.

When it comes to requests for access to bundled individual level or aggregate data, § 20(1a) GWB significantly extends the right to access to data when compared with the EFD. Access petitioners will not have to demonstrate market dominance of the data holder.[457] Furthermore, it will typically be easier to establish that 'an undertaking is dependent on accessing data controlled by another undertaking in order to carry out its own activities' (§ 20(1a) GWB) than to show that 'the granting of access is objectively necessary in order to operate on an upstream or downstream market' (§ 19(2) No. 4 GWB). Furthermore, § 20(1a) GWB – contrary to § 19(2) No. 4 GWB – does not require a showing that 'the refusal threatens to eliminate effective competition on that market'. Some consider that these advantages of § 20(1a) GWB could be offset by the fact that, under § 20(1a) GWB, the access petitioner has to show that the refusal to grant access constitutes an unfair impediment – whereas under § 19(2) No. 4 GWB, the burden of proof for an objective justification for the refusal to grant access is on the data holder.[458] Access claims under § 20(1a) GWB will require a comprehensive interest balancing. Issues to be considered include the type of data that shall be accessed; whether the data holder has granted access to the relevant data before; all burdens that would follow from the need to provide access to data for the data holder, including a loss of exclusivity and the concomitant competitive advantages; a risk to trade secrets and security etc. Aspects that may argue in favour of data access may include the fact that data are non-rival in use, the fact that observed data frequently comes as a by-product to the use of a machine and a duty to grant access will typically not compromise the incentives of the data holder to invest and process the data; any substantial added value that the data access petitioner may be able to create; and the fact that the data holder may be adequately compensated for granting access.[459]

Overall, one should expect that, in the future, data access petitioners would primarily base their requests for access to data on § 20(1a) GWB. However, no judgments on data access under

[456] See Nothdurft in Bunte, Kartellrecht, 14th ed. 2022, § 20 GWB para. 97.

[457] For a detailed comparison between § 19(2) No. 4 and § 20(1a) GWB see Schweda/Schreitter WuW 2021, 145 (146 et seq.).

[458] Schweda/Schreitter WuW 2021, 145 (150); Weber WRP 2020, 559 (561, 564).

[459] For a comprehensive description of the criteria to be considered see Markert/Podszun in Immenga/Mestmäcker, GWB, 7th ed 2022, § 20 paras. 155-164; Hetmank in Bacher/Hempel/Wagner-von Papp, BeckOK Kartellrecht, 4th ed. 2022, § 20 GWB para. 69-72. For a discussion of the principles that will apply in deciding about such compensation see Nothdurft in Bunte, Kartellrecht, 14th ed. 2022, § 20 GWB para. 105; Markert/Podszun in Immenga/Mestmäcker, GWB, 7th ed. 2022, § 20 paras. 142-154; Hetmank in Bacher/Hempel/Wagner-von Papp, BeckOK Kartellrecht, 4th ed. 2022, § 20 GWB para. 68.

§ 20(1a) GWB have been published so far. This does not imply that § 20(1a) GWB has had no effect. Possibly, it already influences contract negotiations regarding data access in favour of data access petitioners.[460] The Bundeskartellamt's proceedings against DB mobility's refusal to make train traffic data available to third mobility platforms (see above, 2(b)(aa)(3)(b)) could be a first 'official' test case for § 20(1a) GWB.

b) Open issues

Given the novelty of § 20(1a) GWB, some questions have not yet been settled.

aa) Scope

Some authors have argued that § 20(1a) GWB should also apply to scenario 3-settings, i.e. to settings where there is no prior vertical or contractual access between the data holder and the access petitioner and where access to data is sought for purposes that are completely unrelated to the activity of the data holder and the network within which the data holder is operating.[461] For example, the data access petitioner may want to have access in order to engage in entirely unrelated innovation. However, the special responsibility of an undertaking with 'relative' market power does not reach beyond the special responsibility of a dominant undertaking in this regard (see above, 2(b)(aa)(1)): a firm with 'bilateral' power must not allow its conduct to impair genuine undistorted competition.[462] But it is under no obligation to broadly enable and promote innovation.[463] If the legislator wants to introduce such a broad responsibility, this should be done outside the framework of competition law.

bb) What does 'dependence' mean in the context of § 20(1a) GWB?

While there is broad agreement that § 20(1a) GWB lowers the threshold for data access requests by requiring 'dependence' of the access petitioner instead of an 'indispensability' of access within the meaning of the EFD,[464] it is not entirely clear what 'dependence' shall mean in the context of § 20(1a) GWB; in particular, whether the notion is entirely congruent with the notion of 'dependence' under § 20(1) GWB or whether it follows its own logic.[465] Nothdurft has argued that § 20(1a) GWB deviates from and replaces § 20(1) GWB.[466] According to him,

---

[460] Markert/Podszun in Immenga/Mestmäcker, GWB, 7th ed. 2022, § 20 paras. 101, 107.

[461] See Markert/Podszun in Immenga/Mestmäcker, GWB, 7th ed. 2022, § 20 paras. 138 et seq.

[462] Case C-322/81, *Michelin*, ECLI:EU:C:1983:313, at para. 57.

[463] To the same effect: Brenner in Bien et al., Die 10. GWB-Novelle, 2021, Ch. 1 para. 162 et seq.: Such a broad obligation would come with a risk of adverse effects on the data holder's incentives to innovate.

[464] Hetmank in Bacher/Hempel/Wagner-von Papp, BeckOK Kartellrecht, 4th ed. 2022, § 20 GWB para. 66; Brenner in Bien et al., Die 10. GWB-Novelle, 2021, Ch. 1 para. 132; Markert/Podszun in Immenga/Mestmäcker, GWB, 7th ed. 2022, § 20 paras. 131;

[465] For the fact that the government's reasoning is not clear in this regard see Schweda/Schreitter WuW 2021, 145 (152 et seq.) who refer to Bundestag publication 19/23492, p. 80.

[466] Nothdurft in Bunte, Kartellrecht, 14th ed. 2022, § 20 GWB para. 79.

§ 20(1a) sentence 1 GWB is a 'functional aliud' to the requirement that 'sufficient and reasonable possibilities for switching to third parties do not exist', and the criterion of 'significant imbalance' does not cover the situation of data access, since a 'significant imbalance' presupposes a mutual interest in a contractual relationship, which is typically not the case in data access scenarios. By contrast, Schweda/Schreitter submit that – while § 20(1a) GWB, contrary to § 20(1) GWB, does not require a prior relationship – the other requirements for dependency as set out in § 20(1) GWB, i.e. that 'sufficient and reasonable possibilities for switching to third parties do not exist' and that 'there is a significant imbalance between the power of such undertakings or associations of undertakings and the countervailing power of other undertakings', should also be 'considered' when applying § 20(1a) GWB.[467] Finally, Brenner argues that § 20(1a) sentence 1 GWB is meant to specify that the second criterion for a 'dependency' in § 20(1) GWB.[468]

Ultimately, the notion of 'dependence' in § 20(1a) GWB will need to be clarified by the courts. § 20(1a) GWB explicitly states that no prior vertical relationship between the data access seeker and the data holder is required. Rather, 'dependence' may follow from the fact that the access petitioner requires data access 'in order to carry out its own activities'.[469]

cc) Enforcement

Although § 20(1a) GWB significantly broadens the possibilities to request access to data under competition law, significant difficulties remain. They start with pervasive information asymmetries between the data holder and the access petitioner: under German law on civil procedure, the access petitioner would have to precisely state which data shall be accessed ('Bestimmtheitsgrundsatz', § 253(2) No. 2 ZPO). However, frequently the access petitioner will not know exactly what data is in the possession of the data holder.[470] Secondly, although the threshold for showing 'dependence' under § 20(1a) GWB is lower than the indispensability criterion under § 19(2) No. 4 GWB, it is not yet clear, and arguably highly case-specific, which types of outside options would be considered reasonable and sufficient in a given setting. Thirdly, there are no precedents yet on how the different interests will be balanced in different setting, how an 'adequate compensation' will be determined[471] and how fair, reasonable and non-discriminatory (FRAND) access can be effectively established and enforced (see below, 4). Creating full-fledged and effective data access regimes based on § 20(1a) GWB will be a challenge. Ultimately, the value of § 20(1a) GWB may rather lie in establishing a conceptual

[467] Schweda/Schreitter WuW 2021, 145 (153).

[468] Brenner in Bien et al., Die 10. GWB-Novelle, 2021, Ch. 1 paras. 131, 133.

[469] See also Markert/Podszun in Immenga/Mestmäcker, GWB, 7th ed. 2022, § 20 para. 112.

[470] Markert/Podszun therefore argue for rethinking the standard to be applied according to the 'Bestimmtheitsgrundsatz' in order not to thwart the legislative mandate to promote data access – *inter alia*, it should be considered to work with 'circumscriptions' – see Markert/Podszun in Immenga/Mestmäcker, GWB, 7th ed. 2022, § 20 paras. 166-168.

[471] Podszun, Handwerk in der digitalen Ökonomie, 2022, p. 92 et seq., 150 et seq. For § 20(1a) GWB see Markert/Podszun in Immenga/Mestmäcker, GWB, 7th ed. 2022, § 20 paras. 94, 107.

benchmark for competition law-based data access requests that reaches beyond § 19(2) No. 4 GWB, but may also be applicable under § 19(1) GWB with § 19(2) No. 1 GWB.

In any case, there does not seem to be a need to reform § 20(1a) GWB for the time being. Rather, it remains to be seen which types of cases will arise and to what extent § 20(1a) GWB provides a useful legal framework.

4. Data access remedies – FRAND access to data

Wherever an obligation to allow for – or enable – data portability or data access is the appropriate remedy to an abuse, access will have to be granted on fair, reasonable and non-discriminatory (FRAND) terms. The obvious question then is what conditions of portability and access will be considered FRAND.

At first glance, the case law on rights to a license for standard essential patent (SEP)[472] may seem to provide a rough role model for the process by which contractual negotiations on data access should take place. However, data access regimes may turn out to be even more complex and diverse in practice:[473] firstly, the information asymmetry regarding data is particularly pronounced. Whereas the granting of a patent is conditional upon the patented technology being published, there is no public register on data. Information on which data a dominant undertaking controls, on how it is structured and formated, is only available from the dominant undertaking itself. Secondly, the proposed use cases for data may differ widely and affect the conditions at which data access should be granted as well as the access pricing. Different bundles of data may be needed, at different levels of aggregation. Data access may be requested at different levels of the value chain. Thirdly, different modes of data access may be appropriate in different settings – ranging from query-based data access to a broader *in situ* access to models in which data is transferred to the petitioner. In the latter case, the necessary degree of interoperability will need to be determined.[474] Fourthly, the requisite timing of data access may differ: in some settings, the provision of historical data will suffice, in other settings, near-time or real-time access may prove necessary to compete effectively. Fifthly, where data is transferred through interfaces, the formats in which data access must be granted and the design of the access interfaces must be determined. The question needs to be resolved whether and to what extent FRAND access includes an obligation to re-structure or re-format data such that it is (more) easily available to different potential users. With respect to all of these issues, conflicts will likely be frequent and – in a competition law framework, i.e. absent regulation – highly case-

[472] See in particular Case C-170/13, *Huawei*, ECLI:EU:C:2015:477.

[473] See on this: Schweitzer/Welker, A legal framework for access to data – a competition policy perspective, in German Federal Ministry of Justice and Consumer Protection/Max Planck Institute for Innovation and Competition (eds.), Data Access, Consumer Interest and Public Welfare, 2021.

[474] For the different forms of interoperability see Crémer/de Montjoye/Schweitzer, Competition Policy for the digital era, Final report, 2019, p. 83 et seq. A lack of data interoperability has been identified as one of the hurdles for an increased flow of data B2B and G2B – see COM (2020) 66 final, 8. On data interoperability see also: Gal/Rubinfeld NYU L. Rev. 2019, 737.

specific. Fast-track procedures for resolving such disputes will be needed if data access is to be effective.

Little experience with such mandated data access regimes exists so far. Competition law enforcement does not seem well placed to master this task. Sometimes, it may be possible to remedy the relevant competition problems by setting up a highly standardised data access regime. In particular, access to individual level usage data with the consent of the relevant individual can be – and has been – organised at reasonable cost. In other areas, the complexity of the challenge may caution against the attempt to set up a compulsory data access regime. Sometimes, the interposition of a trustee or data intermediary may offer a solution (see part F(IV)). In other cases – in particular where a continuous oversight and frequent adaptations would be needed – a regulatory model would be called for – or elsewise a structural solutions where the entity mandated with organising access would have incentives to establish a well-functioning market.

We will revisit the question of how to implement obligations to grant FRAND access to data in part F(II)(2)(d) of this report.

IV. Competition law – part 2: merger control

1. Background and focus

Over the last 15 years, access to data has turned out to be more and more important in merger review in jurisdictions around the globe. The key question is whether merger review is effective in capturing data-induced competitive harms to date and how data-related remedies (such as access and separation commitments) address them. The following analysis outlines the current legal framework for and practice of merger review and enforcement in the EU, Germany and the U.S. It provides the factual basis for discussing policy options later on for possible amendments of the wider legal framework on merger review (part F(II)(4)).

The analysis faces the challenge to separate the role of access to data from general economic features in digital markets that are relevant for merger review. In practice, the role of data is assessed as one, albeit important or even decisive, out of several factors that may contribute to the concentration in markets. Nevertheless, rather than generally elaborating on mergers in the digital sectors, this analysis focuses on the contextualization of data access,[475] including looking at the types and competitive function of data involved. It also covers the design of data-related remedies and an enquiry into their effectiveness, because looking at remedies appears important with regard to the advancement of merger review given that technical innovations allow for new solutions in the frame of merger commitments.

[475] For a numerical overview on mergers involving GAFAM firms see Parker/Petropoulos/Van Alsytne Ind. Corp. Change. 2021, 1307 (1312).

Within the broader category of 'data-related' mergers, we distinguish between 'data-driven' mergers on the one hand and mergers, which simply involve datasets, on the other hand. In this regard, we understand data-driven mergers as transactions that relate to business models in which data stems from the continuous interaction with existing and potential customers or machine generated data. Nevertheless, the following case analysis also puts a side glance at mergers that involve 'conventional' markets of dataset provision and information services, as far as it can inform remedy practice also with respect to data-driven mergers.

2. European Union

a) EU merger review and data – legal standard and recent reforms

The EU Merger Regulation (EUMR)[476] empowers the European Commission to review and prohibit major cross-border mergers, acquisitions and joint ventures under certain conditions. For this purpose, the European Commission has to enquire into whether the proposed transaction would significantly impede effective competition (SIEC) in the common market or a substantial part of it. The European Commission can clear the merger straight away if not in doubt, approve the merger subject to the conditions of the commitments, or prohibit the transaction. Merger Guidelines set out the details,[477] but they do not address data-related mergers in particular, so that they give the European Commission ample room to assess data-related mergers.

To some extent, EU merger review has been reformed in recent times. In March 2021, the European Commission published guidance on referrals pursuant to Article 22 EUMR of transactions which fall below the thresholds of EU Member States.[478] This aims to encourage Member States to refer cases to the European Commission, which will also accept referrals if a Member State lacks jurisdiction over the case. The Guidance is motivated by bringing acquisitions by established players of start-ups or innovators within the scope of the EUMR, which often take place in digital sectors. This approach is controversial and challenged before the courts (for further discussion see part F(II)(3)(c)(cc)), and the German government does not support this practice in case of mergers below notification threshold, which can potentially lead to contradicting merger decisions across the EU.

Furthermore, the DMA also contains provisions for mergers within the EU. Article 14 DMA obliges gatekeepers to inform the European Commission on intended mergers "where the merging entities or the target of concentration provide core platform services or other services in the digital sector or enable the collection of data".[479] This obligation is regardless of whether

[476] OJ 2004 L 24, 1 Article 8.

[477] OJ 2004 C 31, 3; OJ 2008 C 265, 7.

[478] OJ 2021 C 113, 1.

[479] Furthermore, the Commission can temporarily block gatekeepers from making acquisitions in areas relevant to the DMA in case of systematic infringements under Article 18 DMA.

the gatekeeper would be required to notify the concentration under the EUMR or national merger rules. Article 14 DMA obliges the gatekeeper to provide particular information about the intended transaction to the European Commission,[480] who can use the information to monitor the gatekeeper status and consider it in the frame of market investigations under the DMA.[481] The obligation serves the DMA's goal to ensure the effectiveness of the review of the gatekeeper status and to adjust the list of core platform services.[482] But besides increasing the European Commission's abilities to monitor broader contestability trends in the digital sector, Article 14 DMA requires the European Commission to inform competent national authorities of the Member States on the intended mergers it has been informed of.[483] Article 14(5) DMA allows national authorities to use this information for national merger control purposes as well as to request the European Commission to examine the merger pursuant to Article 22 EUMR, should the conditions be met.[484] Therefore, the mandated information sharing between the authorities should enlarge the pool of mergers, which ultimately come under scrutiny of the EU merger control regime.

Nevertheless, neither increasing referrals under Article 22 EUMR nor fostering information exchange between authorities under Article 14 DMA does change the substantive standard for merger review in the EU. In this regard, the European Commission's practice of applying the EUMR remains authoritative. Therefore, it will be outlined in the following how the European Commission has assessed data-related competition concerns in merger decisions (see b). The European Commission has not yet blocked a merger on the grounds that accessing or combining data would give rise to competition concerns.[485] Rather – albeit in only few cases – it required commitments to remedy the competition concerns, which deserve a closer look (see c).

b) Restrictions of competition through data-related mergers

aa) Overview

Mergers can affect the parties' ability to access existing and collect new data. This can bear pro-competitive consequences and foster innovation. In particular, access to data and enriching datasets may enable companies to improve its products or services[486] and to provide new services. Moreover, data-related acquisitions can also effectuate substantial synergies between start-ups and established companies.[487]

---

[480] See Article 14(2) DMA.

[481] See Recital 71 DMA.

[482] Ibid.

[483] See Article 14(4) DMA.

[484] See Recital 71 DMA. Correspondingly, Article 36 DMA allows for using the received information in EU and national merger control.

[485] See Feasey/de Streel, Data Sharing for Digital Markets Contestability, CERRE Report September 2020, p. 38.

[486] Bundeskartellamt/Autorité de la concurrence, Competition Law and Data, 2016, p. 17.

[487] See Crémer/de Montjoye/Schweitzer, Competition Policy for the Digital Era, Final report, 2019, p. 110–111.

However, data-related mergers raise competition concerns if improved data access translates into a 'data advantage' that increases data concentration, which would ultimately restrain competition on relevant markets and raise objections of the regulatory authorities. This applies to horizontal mergers as well as to vertical and conglomerate mergers, which are a typical feature of the digital economy. It is a case-specific question how data access can restrict competition in the context of merger transactions in detail. In general, it is often held as decisive, whether competitors could replicate the information that can be extracted from the data and therefore contest the data advantage.[488] The European Commission's case practice on data-related mergers has gradually developed over time. The following enquiry into it illustrates different constellations and provides a contextualised taxonomy on the restrictions of competition through data-related mergers.

bb) Data concentration of dataset providers and information services

The first group of data-related concerns primarily horizontal mergers, in which undertakings are involved who offer datasets and information services. This means that they have offered substitutable datasets/information on the market as competitors prior to the merger. These mergers are data-related, but not data-driven in a narrower sense. Competitive concerns relate to their high market shares in offering similar products and to the likely barriers that a transaction would create for rivals to enter the market and offer similar datasets.

In 2008, the European Commission approved the acquisition of Reuters by Thomson subject to conditions. Thomson and Reuters are leading financial information providers, which source, aggregate and disseminate real-time and historical market data. They deliver such data as datafeed and supply content sets directly to end users as well as via redistributors.[489] The European Commission expected the transaction to impede competition in several markets of the financial information sector.[490] In this regard the merger could cause horizontal restraints, given that it would eliminate rivalry between two leading data suppliers and reduce choice of customers and enable Thomson-Reuters to increase prices as a consequence.[491] Another concern related to the possible exclusion of downstream services, which obtain and integrate such data into their own offerings to customers. In this regard, vertical restraints were expected in a way that Thomson-Reuters could foreclose its competitors by increasing prices for market data distributed via redistributors or by limiting the access to such data that is integrated in its

[488] Bundeskartellamt/Autorité de la concurrence, Competition Law and Data, 2016, p. 16; Taylor et al., (Re)making Data Markets: An Exploration of the Regulatory Challenges, 2020, p. 21. See also Heim, Datenbasierte Marktmacht in der europäischen Fusionskontrolle, 2021, on different means for replication in this context.

[489] See European Commission 19.02.2008, COMP/M.4726 – *Thomson Corporation/Reuters Group*, para. 28.

[490] I.e. aftermarket broker research reports, earning estimates, fundamental financial data of enterprises, and time series of economic, see Id., para. 455.

[491] See Id., e.g. paras. 300, 380.

own products (complete desktop solutions from Thomson/Reuters).[492] As a remedy addressing all these concerns, the European Commission accepted commitments (see c).

In contrast, the European Commission unconditionally cleared the acquisition of Thomson Reuters Financial and Risk Business by Blackstone in 2018.[493] Both parties offer financial information, which they provide to customers as 'datafeeds' through an API. This means that the customers obtain their content in a direct or 'raw' data format.[494] However, the European Commission considered the combined market share too low to raise competition concerns.[495]

cc) Data concentration as advantage in advertising markets

For a long time, the European Commission considered the impact of data concentration only with regard to advertising markets.[496] This concerned mainly[497] vertical and conglomerate mergers, in which the access to data of the target company would enable the acquirer to impede competition on the digital advertising market, in which it has already been present. In this regard, Google is the dominant player, and it was the first time only in 2020, that the European Commission demanded remedies to address concerns of increased data-driven post-merger concentration in the markets for digital advertising.

As first notable case, the European Commission approved the acquisition of DoubleClick by Google in 2008.[498] DoubleClick's technology ensures that advertisements are posted on the relevant websites and to report on the performance of such advertisements. The European Commission analysed, *inter alia*, the potential effects of foreclosure that occur if Google combines its data with DoubleClick's data.[499] In particular, some stakeholders argued that combining DoubleClick's with Google's customer provided data, which is generated by the use of internet (e.g. IP addresses, cookie IDs, connection times) would allow Google to achieve a position that could not be contested by its competitors.[500] The European Commission acknowledged that information from combining such data could potentially be used to better target ads to users. However, it held that such web surfing behaviour data is available to a number of Google's competitors, either by collecting it directly or through purchasing it via the

[492] See Id., para. 381.

[493] European Commission 20.07.2018, M.8837 – *Blackstone/Thomson Reuters F&R Business*.

[494] See Id., para. 12.

[495] See Id., paras. 50–67.

[496] See Monopolkommission, Sondergutachten 68, Wettbewerbspolitik: Herausforderung digitale Märkte, 2015, para. 110.

[497] Regarding the big tech companies, only horizontal concerns in 2 out of 13 mergers: FB/Whatsapp and Microsoft/Yahoo (unlike conglomerate effects, which the Commission analyzed in 8 out of these 13 cases), see Witt Antitrust Bull. 2022, 208 (221).

[498] European Commission 11.03.2008, COMP/M.4731 – *Google/DoubleClick*.

[499] See Id., paras. 359–366.

[500] See Id., para. 359.

market.[501] Therefore, the European Commission did not raise any further concerns with regard to competition and approved the merger unconditionally.

Following this line, the European Commission approved Microsoft's acquisition of the Yahoo search business in 2010. However, data was not explicitly addressed in the decision.[502] Ultimately, the European Commission held that by acquiring Yahoo search business, Microsoft could increase its scale in search advertising and may even become an alternative to Google.

In contrast, data also played a role with regard to Facebook's position in the online advertising sector in the acquisition of WhatsApp by Facebook, which the European Commission cleared without conditions in 2014.[503] Remarkably, the European Commission held that WhatsApp did not collect any user data that were valuable for advertising purposes; therefore, the merger would not increase the amount of data available to Facebook for advertising purposes.[504] However, compared to previous case analysis, the European Commission extended its enquiry and examined whether the merged company could hypothetically begin to collect data from WhatsApp users to improve the accuracy of targeted ads served on Facebook's social networking platform to WhatsApp users who are also Facebook users.[505] Still, the European Commission concluded that in any case, a sufficiently large amount of internet user data was available on the market for advertising purposes that does not lie within Facebook's exclusive control (i.e. mainly Google, but also among others Apple, Amazon, eBay, Microsoft, AOL, Yahoo!, Twitter, IAC, LinkedIn, Adobe and Yelp).[506]

In 2016, the European Commission approved the acquisition of Yahoo! by Verizon.[507] The European Commission considered that both parties have user data (data generated by user activity on their websites and apps and other services)[508] that can be used for advertising purposes. However, after analysing the potential data concentration as a result of the acquisition, the European Commission excluded competition concerns as it held that the datasets held by Verizon and Yahoo! cannot be classified as unique and a large amount of such user data would continue to be available on the market.[509]

The European Commission approved the acquisition of LinkedIn by Microsoft in 2016 subject to conditions.[510] Also in this case, the European Commission inquired into the concentration of

[501] See Id., para. 365.

[502] European Commission 18.02.2010, COMP/M.5727 – *Microsoft/Yahoo! Search Business*.

[503] European Commission 03.10.2014, COMP/M.7217 – *Facebook/WhatsApp*.

[504] See Id., para. 166.

[505] See Id., paras. 180–189.

[506] See Id., paras. 188–189.

[507] European Commission 21.12.2016, M.8180 – *Verizon/Yahoo*.

[508] European Commission 21.12.2016, M.8180 – *Verizon/Yahoo*, para. 80.

[509] See Id., paras. 90–93.

[510] See European Commission 6.12.2016, M.8124 – *Microsoft/LinkedIn*; the commitments did not relate to data access, however.

the parties' user data that can be used for advertising purposes. Again, the European Commission argued that a large amount of such user data would continue to be available on the market and that third parties cannot obtain such data from Microsoft and LinkedIn prior to the acquisition[511] and once more that the combination of data did not raise serious concerns regarding the compatibility of the merger with the market for online advertising.[512]

The acquisition of Fitbit by Google in 2020[513] is remarkable, as it was the first merger in the EU where the European Commission had such significant concerns on the anti-competitive effect of data-driven advantages in advertising markets that it required commitments from the parties (see c). The competitive assessment stands in stark contrast to the approval of Google's Doubleclick acquisition in 2008. Fitbit devices and services collect different types of data:[514] observed data through devices – this means wellness data collected by sensors from wearables and other Fitbit devices (e.g. heart rate, steps, sleep, location); volunteered data – this means manual data input by a user on the Fitbit apps (user profile, weight, food log, menstrual cycle); inferred data – this means calculations on basis of observed and/or volunteered data; according to Fitbit, the calculations take place on the device itself without the raw data being transferred to the Fitbit server. The European Commission feared that the acquisition of Fitbit and access to the device generated data would significantly strengthen Google's ability to personalise ads. In particular, this would increase barriers for entry and expansion of Google's competitors in the markets for online search advertising, online display advertising, and the entire 'ad tech' ecosystem.[515] Ultimately, the European Commission approved the acquisition of wearables manufacturer Fitbit by Google, conditional on compliance with a commitments package offered by Google (see c).

In its most recent decision on data-driven mergers of January 2022, the European Commission enquired into the acquisition of Kustomer by Meta.[516] Kustomer is a small but successful company founded in 2015, which offers customer service and support customer relationship management ('CRM') software that businesses use for engaging with their customers, *inter alia*, via messaging channels. One concern related to advertising markets. However, the European Commission held it as unlikely that Meta could significantly impede effective competition in the market for the supply of online display advertising services by acquiring additional data through Kustomer. As reasons, the European Commission puts forward the dependency on consent of Kustomer's customers, the small size and limited growth potential of Kustomer, and

[511] See Id., para. 180.

[512] See Feasey/de Streel, Data Sharing for Digital Markets Contestability, CERRE Report September 2020, p. 40.

[513] European Commission 17.12.2020, M.9660 – *Google/Fitbit*.

[514] See Id., paras. 414–418.

[515] It considered the horizontal anticompetitive effects, see Id., paras. 419–468; for a differentiated discussion of the theory of harm see Van Gerven et al., https://globalcompetitionreview.com/guide/digital-markets-guide/first-edition/article/data-and-privacy-in-eu-merger-control (last visited 4.7.2022).

[516] European Commission 27.01.2022, M.10262 – *Meta (formerly Facebook)/Kustomer*, decision not yet published.

alternative providers of online display advertising services who have access to similar commercial data.[517]

dd) Data advantage for improving existing or developing new products

More recently, the European Commission dealt with the issue how data concentration might help companies to improve their existing or develop new products,[518] while this would at the same time increase entry barriers for competitors and lower the contestability of the relevant market.

The European Commission enquired into data related to music apps in the acquisition of Shazam by Apple in 2018.[519] Apple offers its music streaming service, while Shazam provides a music recognition application. The European Commission examined the competitive effects if Apple integrates Shazam's data in its own services/datasets to improve existing functionalities or offer additional functionalities on digital music streaming apps. Shazam's datasets cover information regarding the user's identity, behavioural data (i.e. the user's recognition activity performed through the Shazam app like track title, artist, time at which the song was recognised, and location where the app was used), and which buttons or features within the Shazam app itself the user clicks on.[520] Yet, the European Commission argued that integrating such data would not amount to a negative impact on competition, in particular with regard to prices and choice in the markets for the digital music streaming apps.[521] The European Commission compared the Shazam User Data to other dataset available on the 4 V's (variety, velocity, volume, and value of the data)[522] and held, *inter alia*, that there are other sources, one needs more than this data for providing personal suggestions.[523]

In the frame of the acquisition of LinkedIn by Microsoft, the European Commission discussed the significance of the full dataset of LinkedIn explicitly for machine learning of Microsoft's customer relationship software solutions.[524] But given that LinkedIn was found to be only one out of many data sources for machine learning that was held as unlikely to be essential, the

---

[517] European Commission, Mergers: Commission clears acquisition of Kustomer by Meta (formerly Facebook), subject to conditions (Press release of 27.1.2022), https://ec.europa.eu/commission/presscorner/detail/en/ip_22_652 (last visited 4.7.2022).

[518] See also Monopolkommission: Sondergutachten 68, Wettbewerbspolitik: Herausforderung digitale Märkte, 2015, para. 110; however, there was no such case back in 2015.

[519] European Commission 06.09.2018, M.8788 – *Apple/Shazam*.

[520] See Id., para. 69.

[521] See Id., para. 315.

[522] See also Zingales, https://www.competitionpolicyinternational.com/wp-content/uploads/2018/12/EU-News-Column-December-2018-Full.pdf (last visited 4.7.2022).

[523] See European Commission 06.09.2018, M.8788 – *Apple/Shazam*, paras. 318–328.

[524] See European Commission 6.12.2016, M.8124 – *Microsoft/LinkedIn*, para. 257.

European Commission did not have any serious doubts with regard to input foreclosure effects to the detriment of providers of CRM software solutions.[525]

ee) Data and input foreclosure

The European Commission has increasingly enquired into competitive restraints that occur if the merger leads to an input foreclosure with regards to data as vertical effect. This is the case if the transaction provides incentives to decrease the availability of data, which would have been supplied to the customers (and potential competitors) downstream otherwise.[526] It is relevant for conglomerate mergers, which cause actual or potential rivals' access to supplies, data, or markets to be hampered.[527] Such data input foreclosure[528] can take different forms, i.e. termination of data provision, higher prices, or a degradation of data quality or interoperability.

A straight-forward case of input foreclosure is the acquisition of Tele Atlas by TomTom in 2008.[529] Tele Atlas provides digital map data, TomTom provides navigation software and portably navigation devices (PND), which use such map data as input. The European Commission inquired into TomTom's ability and incentives to limit the access of other PND manufacturers to digital map data. The European Commission concluded that such foreclosure is unlikely, because of the existence of the upstream competitor Navteq, and also because the sales of digital maps lost by Tele Atlas would not be compensated by additional sales of PNDs.

Data input foreclosure also played a role in the acquisition of GitHub by Microsoft in 2018. GitHub supplies DevOps tools and is a popular platform for software development. It holds significant amounts of data about users and programming that Microsoft could use (i.e. user-generated content, users' personal information, and metadata). The European Commission also examined whether Microsoft could further integrate its own DevOps tools with GitHub while limiting the integration with third parties' DevOps tools by means of restricting access to data. The European Commission did not expect anti-competitive vertical non-coordinated effects in this regard.[530] Rather it held that Microsoft would not be able to restrict access to most of the data that is currently accessible to third parties (source code, revision history, identity of author, commit messages in relation to public repositories).[531] As regards to data currently not accessible to third parties, Microsoft could not deny access to competitors without breaching GitHub's Terms of Services with its customers.[532]

---

[525] See Id., para. 277; see also Heim, Datenbasierte Marktmacht in der europäischen Fusionskontrolle, 2021, p. 61 et seq.

[526] See OJ 2008 C 265, 6 paras. 31–57

[527] See Crémer/de Montjoye/Schweitzer, Competition Policy for the Digital Era, Final report, 2019, p. 116, 121.

[528] See Taylor et al., (Re)making Data Markets: An Exploration of the Regulatory Challenges, 2020, p. 21.

[529] European Commission 14.05.2008, COMP/M.4854 – *TomTom/Tele Atlas*.

[530] See European Commission 19.10.2018, M.8994 – *Microsoft/Github*, paras. 131–153.

[531] See Id., para. 141.

[532] See Id., para. 153.

The BMW/Daimler mobility services joint venture[533] of 2018 concerned free-floating car sharing services via DriveNow (BMW) and car2go (Daimler). The European Commission feared that the joint venture would allow Daimler and BMW to shut out rival providers in the vertically affected market for multimodal integrator apps to the benefit of Daimler's own integrator app 'moovel'[534] in six cities. Such apps aggregate several different transport options, including free-floating car sharing as the services of DriveNow and car2go. Considering that data on BMW's and Daimler's fleet was considered as 'must-have' for rival multimodal apps, the European Commission concluded that the parties would have the ability and incentive to foreclose rival multimodal apps.[535] To address these concerns, Daimler and BMW offered commitments (see c).

Also, the acquisition of Fitbit by Google in 2020 (see above) raised concerns with regard to vertical anticompetitive effects[536] in the form of data input foreclosure. In particular, this concerned Fitbit's Web API: prior to the merger, Fitbit provided some health and fitness data to others via API, so that these third parties could provide services to Fitbit users and obtain their data in return. The European Commission feared that after the acquisition Google could restrict competitors' access to the Fitbit Web API and thereby harm start-ups. To address these concerns, the European Commission ultimately accepted data access commitments of Google (see c).

Foreclosure was also the major concern in Meta's acquisition of Kustomer in 2022 (see above). In particular, the European Commission feared that the acquisition would harm competition in a way that Meta could engage in foreclosure strategies vis-à-vis Kustomer's rivals and new entrants by denying or degrading access to the APIs for Meta's messaging channels (i.e. WhatsApp, Instagram and Messenger of Meta). This decision did not concern access to datasets as such, but rather access to integrate Meta's services as an important function for CRM software. However, it is worth mentioning, because the European Commission confirmed the trend of accepting API access commitments (see c).

c) Remedies

aa) EU Merger remedies and data

If the European Commission raises specific competition objections regarding the compatibility of a concentration, the parties may offer remedies (commitments) in order to meet these objections. These commitments should be proportionate to the competition problem and

[533] European Commission 07.11.2018, M.8744 – *Daimler/BMW/Car Sharing JV*.

[534] Which combines on one platform a variety of offers such as the car sharing provider car2go, Deutsche Bahn, mytaxi, rental bicycles and public transport.

[535] See European Commission 07.11.2018, M.8744 – *Daimler/BMW/Car Sharing JV*, para. 319.

[536] See European Commission 17.12.2020, M.9660 – *Google/Fitbit*, paras. 497–531.

eliminate it entirely.[537] If the European Commission regards the commitments as sufficient, it can approve the merger subject to the conditions of the commitments as remedies,[538] otherwise the European Commission prohibits the merger. Details are set out in the European Commission's Notice on Remedies.[539]

When looking at data-related remedies in particular, the general distinction between structural and behavioural remedies serves as a starting point:

- Structural remedies (such as e.g. divesting a business unit) change the structure of the relevant markets directly and permanently. They aim at strengthening existing competitors or fostering the emergence of new ones. The European Commission regards structural remedies as the preferred option.[540] In contrast to behavioural remedies, structural remedies have the advantage that they eliminate anticompetitive problems and incentives at root, while they do not need monitoring and regulatory oversight.[541]

- In contrast, behavioural remedies address ongoing and future conduct of the merging entities. They can require or prohibit a certain business conduct (e.g. mandate conditions for pricing or prohibit to refuse deals).[542] In merger cases, behavioural remedies are only accepted under exceptional circumstances,[543] because they leave anticompetitive incentives of the parties unchanged and their implementation and effective oversight appears questionable.[544]

What has become increasingly relevant with regard to data-related mergers are access remedies. The notion of 'access' as remedy is broad and not limited to data.[545] Access remedies concern cases in which the merging parties have to make assets[546] and in this particular case data accessible to third parties, usually on a non-discriminatory basis.[547] Providing access should enable third parties to enter markets or to compete for a larger share of the market.[548] There is a vivid debate on whether access remedies are to be classified as structural or as behavioural or constitute a distinct or hybrid category of remedies.[549] The regulatory aim of such remedies is to have a structural effect,[550] but in fact, data access remedies address the behaviour of the party through imposing an obligation for conduct in first place, which may also require constant

[537] See Recital 30 EUMR.

[538] See Article 6(2), 8(2) and Recital 30 EUMR.

[539] OJ 2008 C 267, 1.

[540] See Id., para. 15.

[541] See Ducci/Trebilcock CPI Antitrust Chronicles April 2020, p. 3

[542] See Maier-Rigaud/Loertscher CPI Antitrust Chronicles April 2020, p. 4.

[543] See OJ 2008 C 267, 1 para. 17.

[544] See Maier-Rigaud/Loertscher CPI Antitrust Chronicles April 2020, p. 5.

[545] The Commission has imposed access remedies also in other cases in the technology field, see European Commission 27.02.2018, COMP/M.8665 – *Discovery/Scripps*, on access to TV channels in Poland.

[546] E.g. infrastructure, intellectual property, networks, essential inputs etc.

[547] See OJ 2008 C 267, 1 para. 62.

[548] See Maier-Rigaud/Loertscher CPI Antitrust Chronicles April 2020, p. 6.

[549] For the discussion see Ibid.

[550] See Bundeskartellamt, Guidance on Remedies in Merger Control, 2017, para. 74.

future implementation and monitoring. A look at the European Commission's merger decisions that involve commitments illustrates the nuanced differences and tendencies of the European Commission's merger decision practice regarding data access remedies.

bb) Access to data as merger remedy

Data access remedies have to be distinguished from divestments of businesses which may also include to the provision and licensing of data as structural remedies. In 2021, the European Commission approved the acquisition of IHS Markit by S&P Global under the condition of the divestment of businesses in the areas of commodity price assessments and financial data.[551] Also, the acquisition of Monsanto by Bayer in 2018 required Bayer to divest its digital agricultural business worldwide to competitor BASF, while Bayer would receive a non-exclusive, royalty-free, license back regarding certain digital agricultural assets.[552] This divestment addressed the concern that the acquisition would eliminate (potential) competition in the field of digital agriculture between Bayer's and Monsanto's agricultural platforms, which analyses public data (e.g. satellite pictures and weather data) and privately collected data to provide services to farmers how to best manage their fields.

The remedies in the Thomson-Reuters acquisition also strongly resemble structural remedies in the form of a divestiture. However, they bear features of an access remedy because instead of entirely divesting and transferring assets to a third party, the European Commission agreed that Thomson and Reuters must sell copies of four databases[553] to a third party while they may retain ownership and continue to use their databases to commercialise the respective data to their own customers. For the transfer of the copies, Thomson and Reuters had to provide technical support services to enable third party purchasers to integrate the databases into their own existing offerings.[554] Also, Thomson and Reuters committed to provide regular updates to the databases to enable the purchasers to compete effectively.[555] These commitments aimed to quickly establish competitors to the merged entity[556] and thereby provide sufficient post-merger alternatives to customers of financial information. What happened was that the merging parties sold a copy of one of the concerned datasets[557] to competitor FactSet[558] for approx. 70 Mio. USD shortly after the approval of the acquisition.[559] This transaction also included the

[551] European Commission 22.10.2021, M. 10108 – *S&P Global/IHS Markit*.

[552] See European Commission 11.04.2018, M.8084 – *Bayer/Monsanto*, para. 15

[553] Thomson WorldScope, a fundamentals database; Reuters Estimates, an earning estimates product; Reuters Aftermarket Research database, an analyst research distribution product; and Reuters Economics.

[554] See European Commission 19.02.2008, COMP/M.4726 – *Thomson Corporation/Reuters Group*, para. 480. It was not feasible to divest distinct business units, see Weitbrecht Eur. Compet. Law Rev. 2010, 276 (282).

[555] See European Commission 19.02.2008, COMP/M.4726 – *Thomson Corporation/Reuters Group*, para. 480.

[556] See Id., para. 482.

[557] Thomson fundamentals WorldScope.

[558] An American provider of integrated financial information and analytical applications.

[559] Additionally, there was an agreement to transfer a percentage of annual revenues to FactSet, which were expected to be around $2 million to $3 million annually, see Finextra, FactSet completes acquisition of Thomson Fundamentals database copy, 2008.

possibility to hire certain key employees and an agreement which requires Thomson Reuters to provide services (including consulting and support and regular updates) to FactSet for up to 18 months after the completion of the sale.[560] Thomson thereby met parts of the requirements set forth by the European Commission and the U.S. DoJ. To this day, the copy of the Thomson Reuters database has been developed and turned into 'FactSet Fundamentals' is still sold.[561] In contrast, Thomson Reuters put forth an acquirer regarding the other databases (Earnings Estimates and Aftermarket Research Databases) in August 2008;[562] however, neither the name of the buyer nor information on the success of the sale itself could be found.

While Thomson-Reuters was a step towards data-related access remedies, the commitments in the European Commission's decision on the Daimler-BMW Mobility JV of 2018 constitute data access remedies of a 'newer generation'. The European Commission cleared the Daimler-BMW JV under conditions to prevent data input foreclosure on the upstream market for mobility apps and to restore effective competition with regard to the concern that providers of multimodal apps other than Daimler's Moovel.[563] In particular, the JV must provide an API, which enables third party aggregator platforms for mobility solutions to access mobility data on request and therefore allows such platforms to display certain information.[564] The conditions covered six cities and API access is limited to three years after closing of the transaction.[565] A monitoring trustee was appointed (for details see dd). As for the technical and legal implementation,[566] a 'closed API approach' was chosen.[567] This means that on request of aggregator platforms who meet specific criteria API access is granted on basis of a standard contract for free in a non-discriminatory manner. Aggregator platforms may use the data only for the purpose of car sharing activities and not for e.g. data analytics. Moreover, the data is not provided to large technology companies who would use the data in the area of mobility services and autonomous driving. The commitments expired on 31 January 2022, but the European Commission extended them by another two years for the cities of Cologne, Düsseldorf and Vienna. The reason is that the European Commission observed that no meaningful market

[560] See Bobsguide, FactSet Research Systems Agrees to Acquire a Copy of Thomson Fundamentals Database and Related Assets from Thomson Reuters, 2008.

[561] See FactSet, FactSet Fundamentals – Data Feed by FactSet, 2022.

[562] See Memorandum in Support of Plaintiff´s Unopposed Motion to Modify Final Judgement, U.S. v. The Thomson Corporation, Case No.: 1:08-cv-00262 (D.D.C., Aug. 20, 2008).

[563] See European Commission 07.11.2018, M.8744 – *Daimler/BMW/Car Sharing JV*, para. 321.

[564] In particular, access includes unique identifier to the vehicle, position, status (available/ not a.), license plate, URL leading to the booking screen for the vehicle in the provider´s app, other relevant info (model, color, fuel type etc.); on the material terms see Id., Commitments, p. 13.

[565] For details Id., Commitments, p. 3.

[566] For more on the commitment, see Id., Commitments (after p. 65).

[567] See https://docs.partner.share-now.com/docs/overview (las visited 4.7.2022).

entry[568] of other car sharing providers had taken place in these cities.[569] With regard to the data access commitment, the European Commission found that several third-party aggregator platforms have indeed obtained API access and that a majority of respondents intends to do so in the future with regard to these cities.[570]

The Google-Fitbit acquisition has been cleared under the condition that Google must maintain access for API users for 10 years, subject to user consent and without charge for access under further specified conditions.[571] This also includes new data types to be shared through the Web API "within one to two years if they qualify as Supported Measured Body Data and at least 3 of the 5 largest wearable OEMs make available an equivalent data type".[572] The designated monitoring trustee performs an ex-ante review of Google's and Fitbit's terms and conditions for data access.[573] As for the implementation, Fitbit requires applications use a specific framework to securely authorise access to its user data.[574] Data requesters have to comply with Fitbit Platform Terms of Service, Google Terms of Service and the Service User Data Policy, and additional privacy and security requirements.[575]

Recently, the European Commission cleared the acquisition of Kustomer by Meta under conditions. These conditions confirm the very recent practice towards access remedies and bear implications for the advancement of data-related merger commitments. In particular, Meta must guarantee free and non-discriminatory access to its publicly available APIs for its messaging channels also to CRM software providers and new entrants that compete with Kustomer's CRM software. Also, Meta must make improvements of features and functionalities of its messaging services equally available to Kustomer's rivals and new entrants. These access commitments last for 10 years. Moreover, a trustee who may access "Meta's records, personnel, facilities or technical information, and can appoint a technical expert to assist in the performance of its duties"[576] was appointed to monitor compliance.[577] Finally, the commitments also include a dispute resolution mechanism that third parties can invoke.

---

[568] Meaningful market entry is defined in the Commitments as one or more other car-sharing provider(s) has/have entered the market in the relevant city and then reach(es) more than 60% of the average fleet size of Daimler/BMWs fleet of the previous year, see European Commission 07.11.2018, M.8744 – *Daimler/BMW/Car Sharing JV*, Commitments, p. 2; European Commission 31.01.2022, M.8744 – *Daimler/BMW/Car Sharing JV*, Clause 5.

[569] See European Commission 31.01.2022, M.8744 – *Daimler/BMW/Car Sharing JV*, Clause 6.

[570] See Id., Clause 9.

[571] See European Commission 17.12.2020, M.9660 – *Google/Fitbit*, Summary paras. 49, 56–60.

[572] See Id., para. 57.

[573] See Id., para. 58.

[574] See https://dev.fitbit.com/build/reference/web-api/developer-guide/authorization/ (last visited 4.7.2022).

[575] See European Commission 17.12.2020, M.9660 – *Google/Fitbit*, Summary para. 49.

[576] See European Commission, Mergers: Commission clears acquisition of Kustomer by Meta (formerly Facebook), subject to conditions (Press release of 27.01.2022), https://ec.europa.eu/commission/presscorner/detail/en/ip_22_652 (last visited 4.7.2022).

[577] European Commission, Monitoring Trustee in Case M.10262 – *META (formerly Facebook)/Kustomer*.

cc) Restrictions on the use of data as merger remedy

The Google-Fitbit acquisition has entered new terrain with regard to data-related merger remedies: to address the concern of leveraging Google's data advantage in the markets for digital advertisement, Google ensured to not use any data collected via sensors (including GPS) as well as manually inserted data for Google ads for 10 years as a commitment to the merger. Google will store these data in a 'data silo' that is separate from any other Google data that is used for advertising.[578] In detail, the data silo will be a virtual storage environment within Google. Google's access to this environment will be restricted through internal firewalls and logged, while these restrictions must be auditable by the appointed monitoring trustee with the help of an independent technical expert (see dd below for details). At the same time, Google provides users the choice to grant or deny use by Google Services other than Google Ads of any Measured Body Data.[579]

This obligation of data separation resembles Article 6 No. 2 DMA and Article 11(1) DGA. But as a behavioural remedy which needs permanent oversight, it is a new approach in the context of merger remedies and poses significant challenges (see part F(II)(3)(c)(bb)(2)).

dd) The Monitoring Trustee's role for effective implementation of data-related remedies

When it comes to data-related behavioural commitments, the newer remedy practice of the European Commission hints to the central role that the monitoring trustee plays for effectively implementing the remedies. The European Commission refers to the monitoring trustee as its 'eyes and ears'.[580] Its main task is to oversee the implementation of the parties' compliance with the commitments,[581] which is further specified in the trustee mandate that is concluded between the trustee and the parties and in a further working-plan.[582] The monitoring trustee is usually appointed by the parties and approved by the European Commission.[583] It must be independent, qualified and may not be exposed to a conflict of interests.[584]

In the Daimler-BMW JV case, Nocon (a Berlin-based company which is specialised in competition-related monitoring trustee projects) was appointed as monitoring trustee. Amongst other, its tasks are to propose to Daimler and BMW necessary measures to ensure compliance with the commitments, to act as a contact point for any requests by third parties in relation to the commitments, to write reports to the European Commission if it concludes the parties to fail compliance.[585] Correspondingly, the parties have to provide all necessary information to enable

[578] See European Commission 17.12.2020, M.9660 – *Google/Fitbit*, Summary para. 47.

[579] See Id., para. 54.

[580] See OJ 2008 C 267, 1 para. 118.

[581] See Id., para. 117.

[582] See Id., para. 119.

[583] For the procedure see Id., paras. 123–127.

[584] See Id., para. 124.

[585] See European Commission 07.11.2018, M.8744 – *Daimler/BMW/Car Sharing JV*, para. 29.

the monitoring trustee to fulfil its tasks.[586] Also it has to provide regular reports and a final report to the European Commission about the status of compliance with the commitments.[587] The monitoring trustee played a crucial role regarding the extension of the Commitments, as it presented evidence to the European Commission that the extension would be appropriate and in line with the commitments to the decision.[588]

In the Google/Fitbit acquisition, the ING Bank was appointed monitoring trustee. Its tasks are, *inter alia*, regular auditing and reporting to the European Commission, assessing technical means through which Google generates access logs, propose to Google such measures ensure compliance with the commitments, promptly report on non-compliance, act as a contact point for questions from third parties about the nature and scope of the commitments.[589] In particular the tasks include also to assess technical measures put in place to comply with the data separation,[590] to oversee the update mechanism with regard to new data types to be made available,[591] and an ex-ante review of the terms and conditions, so that Google has an obligation to notify amendments ten days before they become effective.[592] For these purposes the monitoring trustee has access to Google's records, personnel, facilities or technical information. The ING Bank has appointed U.S. privacy consulting company Sentinel as independent technical expert,[593] which supports the monitoring trustee to fulfil its tasks.

3. Germany

a) Data-related merger review in Germany and recent competition law amendments

In general, German merger control rules (§§ 35 to 43a GWB) apply to concentrations which are not subject EU Merger Regulation.[594] The Bundeskartellamt is the national authority in charge. To a large extent, the basic underlying concepts are similar to EU merger control. However, there are notable differences (see c) also on remedies) and clarifications with particular respect to digital markets and the role of data, which the German legislator has addressed in recent reforms, and which are relevant for merger control.

With the 9th Amendment to the GWB, which entered into force in June 2017, the legislator introduced a duty to notify the merger if the transaction value exceeds EUR 400 Mio. This complements the turnover-based notification thresholds, which were held as insufficient to

[586] See Id., para. 30.

[587] See Id., Commitments Clause 18.

[588] See Id., Clause 12.

[589] See European Commission 17.12.2020, M.9660 – *Google/Fitbit*, Commitments, Clause 24.

[590] See Id., para. 959.

[591] See Id., para. 960.

[592] See European Commission 17.12.2020, M.9660 – *Google/Fitbit*, Summary para. 58.

[593] Chiavetta, https://iapp.org/news/a/how-a-technical-expert-factors-into-the-google-fitbit-acquisition/ (last visited 4.7.2022); European Commission 17.12.2020, M.9660 – *Google/Fitbit*, Commitments, Clause 28.

[594] § 35(3) GWB.

capture cases prototypical in digital markets. It enables the Bundeskartellamt to enquire into cases in which established players reduce competition by buying small innovative competitors which e.g. hold important data.[595] Moreover, § 18(2a) GWB has been introduced to clarify that when analysing whether a company may hold a dominant position, the provision of free services does not invalidate the assumption of a market. With particular respect to markets involving multi-sided markets and networks, the legislator introduced § 18(3a) GWB, which lists elements to be taken into account when assessing the market position of an undertaking, including the undertaking's access to data relevant for competition.

The 10th Amendment to the GWB entered into force in July 2021. The legislator has substantially reformed the rules on the abuse of market power, which are highly relevant for data access (see part E(III)(2)). Relevant for merger control is § 18(3) No. 3 GWB, which added the undertaking's 'access to data relevant for competition' also as a further criterion for assessing the market position of an undertaking in relation to its competitors beyond multi-sided markets and networks. Moreover, the legislator revised merger control provisions, which are however general and not specifically tailored to digital markets.[596]

b) Cases

Cases which concern data and data-related advantages have so far been rare before the Bundeskartellamt. In 2015, the Bundeskartellamt approved the acquisition of the 'HERE mapping service' (formerly part of Nokia), by a consortium of BMW, Daimler and Audi.[597] HERE creates databases of digital maps as a basis for classic navigation applications. Such digital maps, in conjunction with the sensors installed in the vehicles, will allow the maps to be updated in real time. The automotive industry considers them as an essential element for connected and autonomous driving. The Bundeskartellamt did not have any concerns regarding an exclusion of other car manufacturers from the supply of digital maps, because automobile customers can still buy digital maps from TomTom. Therefore, car manufacturers could still develop autonomous driving systems in cooperation with TomTom.

Notable is the Bundeskartellamt's prohibition of the planned acquisition by CTS Eventim of Four Artists in 2017. It was not directly related to data markets, but data played a crucial role for the competitive assessment of the acquisition. Amongst others, CTS Eventim operates a

---

[595] This was the case in the acquisition of Whatsapp by Facebook. For background see Scholl JECLAP 2017, 219 (219–220). In January 2022, the Bundeskartellamt published guidelines jointly with the Austrian Bundeswettbewerbsbehörde, which provides details on calculating the transaction thresholds, see Bundeskartellamt/BWB, Leitfaden Transaktionswert-Schwellen für die Anmeldepflicht von Zusammenschlussvorhaben (§ 35 Abs. 1a GWB und § 9 Abs. 4 KartG), 2022.

[596] E.g. increase of domestic turnover thresholds; changes in procedure; better control of gradual takeovers of small undertakings.

[597] Bundeskartellamt, BMW, Daimler, and Audi can aquire Nokia's HERE mapping service (Press release of 06.10.2015), https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2015/06_10_2015_HERE.html (last visited 4.7.2022).

ticket online shop, provides ticketing services and organises events. At that time, 60–70% of all tickets sold in Germany via ticketing system were sold through CTS Eventim's ticketing platform. The Bundeskartellamt held that by acquiring Four Artists, CTS Eventim would gain control of additional relevant ticket quotas and expand its market position further. What was relevant for the assessment (even though not decisive for the prohibition) was the undertaking's access to data relevant for competition under § 18(3a) No. 4 GWB. The Bundeskartellamt held that CTS Eventim has a significant and competitively relevant data advantage.[598] Especially the ticket brokerage via its online store would enable CTS Eventim to extensively customer data (e-mail address, street, house number, postal code, city, country, date of birth (optional), telephone, payment data), which could then be linked and used for marketing purposes and market analyses. Moreover, it generates sales data in the ticket system, in the case of sales via stationary sales outlets that are connected to the CTS Eventim system,[599] which allows to gain insights into the regional and temporal distribution of demand for the specific events. All this would enable CTS Eventim to better target customers, which leads to higher ticket bookings;[600] to use this data to increase customers' willingness to pay;[601] to better forecast demand for certain events and use it to the advantage of the Group's own event organisers.[602] The Bundeskartellamt held that the data cannot be duplicated by competing ticket systems, due to the high market share of CTS Eventim.[603] Therefore, the vertical integration of Four Artists through the proposed transaction would lead to an increase in the possibility of external promoters being disadvantaged, amongst other because it would make CTS Eventim less dependent on demand from external promoters, which would strengthen its market position and even increase the possibility of data collection.[604] The prohibition of the merger was confirmed by the BGH.[605]

The Meta/Kustomer merger was also subject to German merger review before the Bundeskartellamt. There was a procedural hurdle: the Bundeskartellamt only refers cases to the European Commission under Article 22 EUMR if they are notifiable under German competition law.[606] This contrasts the Article 22 Guidance of the European Commission, which assumes an impact of competition in the single market even if the transaction would not meet national notification thresholds. For clarifying this issue, the Bundeskartellamt could not join other Member States' request[607] to refer the Meta/Kustomer acquisition to the European Commission and launched a parallel procedure. Ultimately, the Bundeskartellamt held the merger should have been notified in Germany under §§ 35(1a), 39(1) GWB by confirming the local nexus as

[598] See Bundeskartellamt 23.11.2017, B6-35-17 – *CTS Eventim/Four Artists*, para. 190.

[599] See Id., para. 191.

[600] See Id., para. 192.

[601] See Id., para. 193.

[602] See Id., para. 194.

[603] See Id., para. 195.

[604] See Id., para. 290.

[605] BGH 12.01.2021, KVR 34/20 – *CTS Eventim/Four Artists*.

[606] Bundeskartellamt 12.12.2021, B 6 – 37/21 – *Meta/Kustomer*, para. 59.

[607] Austria, joined by nine other Member States.

Kustomer performed substantial operations in Germany, which the Bundeskartellamt confirmed[608] as it concluded that Kustomer is sufficiently active in Germany and that the transaction will have effects in Germany. The Bundeskartellamt decided shortly after the European Commission had cleared the merger under conditions. For its assessment, the Bundeskartellamt could account for the findings and also on the agreed commitments. In substance, it concluded that existing competition law would not have warranted a prohibition,[609] but casted some doubts on the assessment performed by the European Commission.

c) Remedies

While especially the CTS Eventim case shows that the Bundeskartellamt duly considers the relevance of data access for impeding competition, there is no case practice in Germany that relates to data-related (access) remedies and respective post-merger monitoring. This can be explained by restrictions on the admissibility of behavioural remedies according to § 40(3) sentence 2 GWB, which states that the conditions and obligations which should ensure that the undertakings concerned comply with the commitments "must not aim at subjecting the conduct of the undertakings concerned to continued control". The German Guidance on Remedies explains that this would require the conduct to be constantly monitored by the competition authority or a third party and that such effective control could not be maintained.[610] It declares market access remedies as inadmissible if they require constant market monitoring.[611] For this reason, also 'Chinese-Wall' commitments, which would shield sensitive information from different business units, are not considered as suitable to remedy competition harm, due to the extreme difficulty to identify, stop and prevent con-compliance.[612]

In the literature, it has been debated where to draw the line between structural remedies and behavioural remedies which are prohibited under § 40(3) GWB. In fact, the Bundeskartellamt has accepted access to networks as remedy in the (regulated) gas sector, but only to a certain extent.[613] A major point for discussion is the requirement of '*continued control*', e.g. if this criterion is met if the commitment is limited in time.[614] Regardless of where exactly German competition law draws the line, it is evident that the Bundeskartellamt has less leeway than the European Commission in designing access remedies. Such commitments which the European Commission accepted in Google-Fitbit – and arguably also in the BMW-Daimler JV – would not have been admissible under merger control in Germany. These different stands on

---

[608] Bundeskartellamt 12.12.2021, B 6 – 37/21 – *Meta/Kustomer*, paras. 19–59.

[609] Bundeskartellamt, Bundeskartellamt clears acquisition of Kustomer by Meta (formerly Facebook) (Press release of 11.02.2022), https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2022/11_02_2022_Meta_Kustomer.html (last visited 4.7.2022).

[610] See Bundeskartellamt, Guidance on Remedies in Merger Control, 2017, para. 26.

[611] See Id., para. 28.

[612] See Id., paras. 86–87.

[613] See Thomas in Immenga/Mestmäcker, Wettbewerbsrecht, Vol. 2 GWB, 6th ed. 2020, § 40 para. 112.

[614] For different means of interpretation see Picht in BeckOK Kartellrecht, 4th ed. 2022, § 40 GWB para. 70; Thomas in Immenga/Mestmäcker, Wettbewerbsrecht, Vol. 2 GWB, 6th ed. 2020, § 40 para. 113.

behavioural remedies feed into the debate about the appropriate legal framework and policy options with particular respect to data-related merger remedies (see part F(II)(3)).

4. Excursus: U.S.A.

a) Data-related merger review in the U.S.

In the U.S., antitrust agencies have investigated early on whether bringing together significant datasets may result in anticompetitive harm. Looking at the cases[615] illustrates some considerable similarities – not the least because in some cases, the European Commission and their U.S. counterparts have co-operated and reviewed the merger with comparable outcomes. At the same time, it is striking that a larger number of cases involves divestitures to mitigate competition concerns. Also, access remedies have been imposed already in the Ticketmaster/Live Nation merger of 2010, while 'next generation' remedies such as identified in BMW/Daimler and Google/Fitbit cannot be recognised.

In the U.S., the DoJ and the FTC share jurisdiction over merger review. Under the Hart-Scott-Rodino Act of 1976, their notification is required if filing thresholds are surpassed. Once the authorities are notified, they allocate the merger to one agency for review, which can then close the investigation or challenge it. Upon challenge, it could enter into a negotiated consent agreement with the companies to restore competition, or it could file a preliminary injunction in federal court to stop the merger.[616] Section 7 of the Clayton Act outlines the substantive rules for merger review. It prohibits mergers, acquisitions, and certain joint ventures where the effect may be to substantially lessen competition (SLC). The Horizontal Merger Guidelines of 2010[617] and Vertical Merger Guidelines of 2020[618] of the DoJ and FTC give guidance. However, the FTC withdrew from the Vertical Merger Guidelines, so that they remain in effect only for the DoJ.[619] The DoJ has modernised its Merger Remedies Manual in 2020,[620] while the FTC follows its Statement Negotiating Merger Remedies of 2012.[621]

b) Cases and remedies

[615] On the methodological differences with regards to lower availability of information on the competitive assessments in the U.S. see Anne C. Witt, *Who´s Afraid of Conglomerate Mergers?*, 67 Antitrust Bull. 208, 223–224 (2022).

[616] See FTC, Premerger Notification and the Merger Review Process.

[617] U.S. Department of Justice, the Federal Trade Commission: Horizontal Merger Guidelines, 2010.

[618] U.S. Department of Justice, the Federal Trade Commission: Vertical Merger Guidelines, 2020.

[619] See FTC, Federal Trade Commission Withdraws Vertical Merger Guidelines and Commentary, 2021; on the discussion also Witt, *op. cit.*, 226.

[620] U.S. Department of Justice, Antitrust Division: Merger Remedies Manual, 2020.

[621] See Feinstein, Negotiating Merger Remedies – Statement of the Bureau of Competition of the Federal Trade Commission, 2012.

aa) Data concentration of dataset providers and information services

Also in the U.S., data-related divestitures as structural merger remedies were imposed early on. As a prototype, the FTC challenged the Dun & Bradstreet Corporation acquisition of Quality Education Data of 2009.[622] The FTC alleged that the combination of data sold by these companies gave Dun & Bradstreet, through its subsidiary Market Data Retrieval, more than 90% of the market for K-12 educational marketing data. The data included names, job titles, course titles, demographic information and/or contact information of education industry participants.[623] A consent agreement required Dun & Bradstreet to divest assets to competitor MCH, to restore competition that was eliminated as a result of the transaction. In particular, Dun & Bradstreet were required to sell MCH an updated K-12 database.[624] There are several other mergers in which the FTC required that databases should be divested by third parties to compete with the combined firm.[625]

The acquisition of Reuters by Thomson in 2008 (see above) was also under scrutiny of the DoJ.[626] In line with the European Commission, the DoJ obliged Thomson and Reuters to sell copies of the data, to enable the acquirer of each set of data to offer institutional financial data products comparable to those offered by Thomson or Reuters.[627] The DoJ had to approve the buyer of each of set of assets (see above).

A comparable case was the acquisition of Arbitron by Nielsen in 2014, which risked to substantially lessen competition for national syndicated cross-platform audience measurement services.[628] Nielsen and Arbitron provide audience measurement services. The FTC found that the proposed merger would eliminate their future competition.[629] In order to compete in the market for cross-platform audience measurement services, a firm must have access to data with individual demographics.[630] The FTC required Nielsen to divest assets and license certain data for a minimum period of eight years related to Arbitron's cross-platform audience measurement

---

[622] The Dun & Bradstreet Corporation, FTC File No. 091 0081, Docket No. 9342 (2010).

[623] See Id., p. 12.

[624] See FTC, Dun & Bradstreet Settles FTC Charges that 2009 Acquisition was Anticompetitive, 2010.

[625] See Fidelity National Financial, Inc., FTC File No. 091 0032, Docket No. C-4300 (2010); Fidelity National Financial, Inc., FTC File No. 131 0159, Docket Number C4425 (2014); also CoreLogic, Inc.'s acquisition of DataQuick Information Systems in 2014, where the FTC required CoreLogic to license to Renwood RealtyTrac (RealtyTrac) national assessor and recorder bulk data as well as several ancillary datasets that DataQuick provides to its customers, see FTC, FTC Puts Conditions on CoreLogic, Inc.'s Proposed Acquisition of DataQuick Information Systems, 2014. For further cases see Jeffrey A. Eisenach & Ilene Knable Gotts, *Looking Ahead – The FTC's Role in Information Technology Markets*, 83 Geo. Wash. L. Rev. 1876, 1881–1885 (2015); Stanley M. Besen, *Competition, Privacy, and Big Data*, 28 JLT 63 (2020).

[626] U.S. v. Thomson Reuters Corp., Case No.: 1:08-cv-00262 (D.C.C. 2008).

[627] U.S. Department of Justice, Justice Department requires Thomson to sell financial data and related assets in order to acquire Reuters, 2008.

[628] Decision and order, Nielsen Holdings N.V., FTC Docket No. C-4439 (Feb. 24, 2014).

[629] FTC, Analysis of Agreement Containing Consent Order to Aid Public Comment, Nielsen Holdings N.V., FTC Docket No. C-4439, 2013.

[630] See Complaint, Nielsen Holdings N.V., FTC Docket No. C-4439 (Feb. 24, 2014), p. 3.

to an approved buyer. This concerned television, radio and calibration panel data in such form and at such frequency as reasonably requested by the buyer.[631] This should enable the buyer to successfully develop a cross-platform service to compete with Nielsen/Arbitron.[632] In fact, certain assets were licensed to competitor comScore.[633]

bb) Data concentration as advantage in advertising markets

The 2008 acquisition of DoubleClick by Google was also subject to merger review in the U.S.[634] Amongst other, the FTC inquired into conglomerate effects[635] the potential effects of foreclosure based on the combination of Google's and DoubleClick's data. However, the FTC approved the acquisition and argued that neither the data available to Google, nor the data available to DoubleClick would constitute an essential input to a successful online advertising product.[636] It also noted that Google's competitors have at their disposal valuable stores of data not available to Google.[637]

Also, with regard to Microsoft's acquisition of search engine Yahoo! in 2010, the FTC has found that the transaction would increase competition in the market and stressed that access to a larger data pool may enable more rapid innovation of potential new search-related products and algorithms.[638]

The WhatsApp acquisition by Facebook was also approved by the FTC in 2014 some weeks before the European Commission cleared the merger. The FTC followed the premise that Facebook will not use WhatsApp's user information for advertising purposes or sell to a third party for commercial or marketing use without the users' consent. Also, Facebook guaranteed that it continues to operate as a separate company[639] – which ultimately was not the case. In 2020, however, the FTC – as well as a number of U.S. State Attorneys General – sued Facebook for a violation of Section 2 Sherman Act.[640] One of the allegations is that Facebook has harmed

---

[631] See Decision and order, Nielsen Holdings N.V., FTC Docket No. C-4439 (Feb. 24, 2014), p. 6.

[632] See Greg Sivinski, Alex Okuliar & Lars Kjolbye, *Is big data a big deal? – A competition law approach to big data*, 13 ECJ 199, 212 (2017).

[633] See FTC, FTC Approves Nielsen Holdings N.V. and Nielsen Audio, Inc.'s Application to Sell its LinkMeter Technology and Related Assets to comScore, Inc., 2014.

[634] See FTC Statement, Google/DoubleClick, File No. 071-0170 (Dec. 20, 2007), p. 12–13.

[635] See Witt, *op. cit.*, 224, who remarks that this enquiry into conglomerate effects remained the exception in the U.S.

[636] See FTC Statement, Google/DoubleClick, File No. 071-0170 (Dec. 20, 2007).

[637] See FTC Statement, Google/DoubleClick, File No. 071-0170 (Dec. 20, 2007).

[638] See U.S. Department of Justice, Press Release of 18.02.2010, Statement of the Department of Justice Antitrust Division on Its Decision to Close Its Investigation of the Internet Search and Paid Search Advertising Agreement Between Microsoft Corporation and Yahoo! Inc.

[639] See Rich, Letter to Erin Egan, Chief Privacy Officer, Facebook, and to Anne Hoge, General Counsel, WhatsApp Inc., 10.4.2014.

[640] Complaint for Injunctive and Other Equitable Relief, FTC v. Facebook, Inc., Case No. 1:20-cv-03590 (D.D.C., Dec. 9, 2020).

competition and maintained its monopoly power in the social networking market through its acquisitions of Instagram and WhatsApp.

A notable case in the U.S. that also concerned data advantages with regard to digital advertising markets took place in 2012, when Bazaarvoice acquired PowerReviews, its primary competitor in the market for online product ratings and review platforms. The DoJ successfully opposed the acquisition two years later.[641] The court found that the acquisition would amplify Bazaarvoice's access to 'consumer behaviour data and brings significant opportunities for syndication, advertising, and data'.[642] It held that there were typically no available substitutes for such dynamic data so that the new entity would control enough such data to foreclose rivals.[643] The court ordered that Bazaarvoice must divest all acquired assets of PowerReviews, including the data.[644]

cc) Data advantage as market entry barrier

In 2010, and therefore early as compared to the EU, the DoJ enquired into merger-induced data advantages which are key for reaching incontestable positions in other markets. In the acquisition of Live Nation by Ticketmaster Entertainment in 2010, the DoJ required data access as behavioural remedy, which has been designed as portability right. Ticketmaster is the world's largest ticketing company. Live Nation is the world's largest promoter of live concerts, but has also started to enter the market for ticketing. The DoJ raised horizontal and vertical concerns about the competitive effects of the acquisition and required structural and behavioural remedies.[645] The DoJ identified data to play a critical role for other ticketing services being able to compete with Ticketmaster.

To prevent the anticompetitive abuse of Ticketmaster's unique ticketing data,[646] the DoJ required the merged entity to provide clients with their 'ticketing data'. This includes financial data relating to a ticketing client's events, number of sold tickets, proceeds from those sales for a specific event, ticket inventory, number and location of tickets that are sold, amount for which the tickets are sold, pricing, marketing and promotions run for the event, the sales as a result of the marketing or promotions, and the status of the ticket inventory.[647] This also includes 'ticket buyer data', meaning non-public identifying information for ticket buyers (including, name, phone number, e-mail address, and mailing address), but not data that is collected through other means (e.g., website tracking, user group surveys, public sources).[648] In particular, if clients

[641] U.S. v. Bazaarvoice, Inc., Case No. 13-cv-00133-WHO.

[642] U.S. v. Bazaarvoice, Inc., Case No. 13-cv-00133-WHO, 2014 WL 203966 (N.D. Cal., Jan. 8, 2014), para. 83.

[643] See Sivinski/Okuliar/Kjolbye, *op. cit.*, 212.

[644] See U.S. v. Bazaarvoice, Inc., No. 13-cv-00133 WHO (N.D. Cal. Dec. 2, 2014), p. 2.

[645] In detail see Mary T. Coleman & David A. Weiskopf, *Non-Self-Enforcing Remedies and the Recent Modification to the Ticketmaster/Live Nation Merger Consent Decree*, CPI Antitrust Chronicle April 2020.

[646] See Id., p. 5.

[647] See U.S. v. Ticketmaster Entertainment, Inc., Case No: 1:10-cv-00139 (D.D.C., Jul. 30, 2010).

[648] See Ibid.

choose to use another ticketing service, the merged entity is required to provide the client 'with a complete copy of all Client Ticketing Data and all Ticket Buyer Data historically maintained by Defendants for such venue(s) in the ordinary course of business, in a form that is reasonably usable by the client' within 45 days.[649] In 2020, the consent decree was modified and extended until 2025, because some conduct remedies – albeit not with regards to the data access commitment – have been proven as ineffective against anti-competitive conduct.[650] Also, the amendments of 2020 prescribed the appointment of an independent monitoring trustee.[651]

dd) Data and input foreclosure

Also comparably early, the DoJ dealt with data and input foreclosure. In 2011, Google acquired airfare pricing and shopping software developer ITA.[652] ITA supplied an airline schedule database and seat availability to various online travel intermediaries as an input for their own products.[653] ITA delivered accurate and almost instant results to its customers because it was able to access, aggregate, and reconfigure the data and use cached outcome data.[654] The DoJ was concerned that by acquiring ITA, Google would be able to foreclose rivals (other flight search services) from some important input data. Therefore, the DoJ requested a behavioural commitment by Google. For five years, Google must continue to license the database, including updates, to third parties on FRAND terms.[655] To this day, this case remains the only formal challenge of an acquisition by the 'Big Five' by U.S. authorities.[656]

Currently, the DoJ is still reviewing the acquisition of Fitbit by Google, which has been completed in January 2021 (see above).[657]

V. Special data access obligations for 'gatekeepers' (DMA) or undertakings of paramount cross-market relevance for competition (§ 19a GWB)

1. Data access obligations and other data-related rules in the DMA

[649] See Ibid.

[650] See U.S. v. Ticketmaster Entertainment, Inc., Case No: 1:10-cv-00139-RMC, Doc. 22 (D.D.C., Jan. 28, 2020).

[651] See U.S. v. Ticketmaster Entertainment, Inc., Case: 1:10-cv-00139-RMC, Doc. 29 (D.D.C, Jan. 28, 2020), p. 14–16.

[652] U.S. v. Google Inc. and ITA Software, Inc., Case: 1:11-cv-00688 (RLW).

[653] See Sivinski/Okuliar/Kjolbye, *op. cit.*, 212.

[654] See Sivinski/Okuliar/Kjolbye, *op. cit.*, 213.

[655] See U.S. v. Google Inc., Case: 1:11-cv-00688 (RLW), (D.D.C, Apr. 8, 2011), p. 13–14.

[656] See Witt, *op. cit.*, 223.

[657] See Feiner, FTC, DOJ seek to rewrite merger guidelines, signaling a tougher look at large deals, 2022.

For the largest digital platforms, an additional layer of data-related obligations is emerging. In the EU, the DMA[658] will be formally adopted over the summer of 2022.[659] Pursuant to Article 46 DMA, the European Commission will then adopt a procedural regulation. Undertakings potentially falling under the definition of a gatekeeper under Article 3 DMA will have to notify the European Commission by the summer of 2023. Based on this notification, the European Commission will designate the gatekeepers who will then have to comply with the obligations listed in Articles 5, 6 and 7 DMA by the beginning of 2024. These obligations apply automatically to each of the core platform services[660] identified in the European Commission's designation decision.

a) Data access obligations in the DMA

The DMA lists three data access obligations:

- Firstly, an obligation to offer effective data portability – continuous, real-time and free of charge – to end users and third parties authorised by them (Article 6 No. 9 DMA). Article 6 No. 9 DMA shall make sure that gatekeepers do not restrict the switching or multi-homing of end users and thereby undermine the contestability of core platform services and restrict the innovation potential of digital services (Recital 59).
- Secondly, an obligation to grant business users, as well as third parties authorised by them, access to the data provided by them or generated in the context of their business offers on the platform – again continuous, real-time and free of charge (Article 6 No. 10 DMA). Access and use must be granted to aggregated and non-aggregated data. Where the data includes personal data, in particular of end users who engaged with the products and services offered by the business user, access and use of the data presuppose the consent of the end user. But the gatekeeper must enable business users to obtain such consent (Recital 60).[661]
- Thirdly, an obligation for gatekeepers that run online search engines to provide any third party undertaking that also offers online search engines with access to ranking, query, click and view data generated by end users in relation to free and paid search. Access must be granted on fair, reasonable and non-discriminatory terms (Article 6 No. 11 DMA).

Beyond Article 6 No. 11, the DMA does not foresee any obligation of gatekeepers to grant access to data to third parties in 'scenario 2'-settings, i.e. to undertakings that had no role of

[658] Regulation 2022/XXX of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act). For a discussion of the initial European Commission's proposal for a DMA see Schweitzer ZEuP 2021, 503.

[659] It is expected to be published in the OJ in September 2022.

[660] Article 2(2) DMA sets out a conclusive list of all the services to be considered core platform services for the purposes of the DMA, namely: online intermediation services, online search engines, online social networking services, video sharing platform services, number-independent interpersonal communication services, operating systems, cloud computing services and online advertising services. Web browsers, virtual assistants were added to the initial proposal.

[661] For the importance of an effective implementation of this obligation see Baschenhof, The Digital Markets Act (DMA): A Procompetitive Recalibration of Data Relations?, 2021, https://ssrn.com/abstract=3970101 (last visited 4.7.2022), p. 23: There is a risk that gatekeepers ultimately refuse data access referring to the end users' rights under the GDPR.

their own in the generation of those data, or are authorised by a platform user who has had such a role.

b) Other data-related obligations in the DMA

This list of data access obligations is complemented by a list of restrictions regarding the combination of data and data processing and field of use: firstly, unless the end user has been presented with specific choice and provided valid consent in compliance with Articles 4(11) and 7 of the GDPR, a gatekeeper must not process personal data from end users that result from the use of services of third parties for the purpose of providing advertising services; they must not combine personal data from the relevant core platform service with personal data from any other service – whether offered by themselves or by third parties; they must not cross-use personal data from the relevant core platform service in other services they offer separately – and vice versa; and they must not sign in end users to other services of the gatekeeper in order to combine personal data (Article 5 No. 2 DMA). This provision reacts to concerns that all these practices tend to advantage gatekeepers in accumulating more data and thereby raising barriers to entry (Recital 36). Leaving end users a free choice between a 'data intense' version of the service and a less personalised, but otherwise equivalent alternative is thought to promote contestability.[662]

Secondly, a gatekeeper must refrain from using any data not publicly available that is generated or provided by business users in the context of the use of a relevant core platform service in competition with those business users (Article 6 No. 2 DMA).[663] Otherwise, gatekeepers with a dual role as platform providers and competitors on the platform could take advantage of the privileged access to data that they enjoy as platform providers when they compete with the businesses to which the data pertain (Recitals 46-48).[664]

c) Rationales of the data-related obligations in the DMA

This package of data-related obligations does not follow a unitary logic. Rather, it responds to different concerns. The recitals to the DMA highlight that 'data-driven advantages' – together with strong network effects and extreme economies of scale – figure among those characteristics of core platform services that tend to lead to very high barriers to entry and undermine the contestability of the entrenched positions of gatekeepers in the provision of the relevant core platform services (Recitals 2 et seq., 32), and that a gatekeeper's access to large

[662] It remains an open question whether the hopes that consumers, when presented with free choice, will opt for the more data-sensitive alternatives will materialize.

[663] Article 6 No. 2 DMA specifies that "data that is not publicly available' shall include 'any aggregated and non-aggregated data generated by business users that can be inferred from, or collected through, the commercial activities of business users or their customers, including click, search, view and voice data …".

[664] Baschenhof, The Digital Markets Act (DMA): A Procompetitive Recalibration of Data Relations?, 2021, https://ssrn.com/abstract=3970101 (last visited 4.7.2022), p. 28 raises the question whether this limitation on the use of data is limited to the use for activities that would place the gatekeeper in actual competition with the business user, or whether it would extend to uses that are in potential competition with a business user.

amounts of data may allow it to leverage advantages from one area of activity to another (Recital 3).

Some of the data-related obligations – the restrictions on the combination and field of use – have been inspired by competition law proceedings.[665] The data access obligations in Article 6 No. 9, Article 6 No. 10 and Article 6 No. 11 DMA reach significantly beyond existing competition case law, however. Yet, they are not entirely new: in principle, a right to the portability of personal data already follows from Article 20 GDPR. Article 6 No. 9 DMA just makes it significantly more effective.[666] The obligation to ensure the access of business users to the data provided by them or generated on the basis of their offers (Article 6 No. 10 DMA) seems to be related to the data porting and access rights proposed in the Draft Data Act – only that the latter relates to machine-generated data, whereas the DMA relates to data linked to online services (and its scope of application is limited to gatekeepers). Across the different regulations, there seems to be a shared assumption that data co-generators should have access to the data they co-generate, even though the data access and portability obligations under Article 6 No. 9 and Article 6 No. 10 DMA apply only to gatekeepers.

So in a broader perspective, the data portability and data access obligations of the DMA appear to be relatively cautious. Both Article 6 No. 9 and Article 6 No. 10 relate exclusively to 'scenario 1'-settings (on the categorization of different data access scenarios see above, part E(III)(2)(b)(aa)(1)), i.e. to the porting of data or the access to data that was co-generated by the end user or business user who requests access. While both provisions may promote competition – by facilitating switching and multi-homing (Article 6 No. 9 DMA), and by allowing business users to compete more effectively on the platform and adjusting their offers to consumer preferences more swiftly – neither of them will enable undertakings to challenge the gatekeeper's position head-on. The gatekeeper's data advantages, which essentially results from the access to the whole bundle of data, remains unaffected.

Only Article 6 No. 11 DMA refers to a 'scenario 2'-case. In this one area of activity – online search engines – the European legislator has apparently presumed that access to data is *the* core barrier to the success and expansion of competing search engines, and that contestability can only be – but can also be expected to be – re-established by granting access to ranking, query, click and view data (Recital 61). Being limited to search engine data, Article 6 No. 11 DMA is, however, a sector-specific rather than a horizontal data access rule.

---

[665] Article 5 No. 2 DMA, for example, is inspired by the Bundeskartellamt's Facebook decision – Bundeskartellamt, 6.2.2019, B6-22/16 – *Facebook* (for a detailed analysis of the Facebook case, in particular of the BGH's Facebook decision of 23.06.2020, see Schweitzer JZ 2022, 16). Article 5 No. 2 DMA significantly expands the basic idea of the Facebook case, however. Also, whereas the Bundeskartellamt's decision had heavily relied on consumer exploitation, the recitals of the DMA emphasize the potential foreclosure effects of extensively accessing, processing, combining and cross-using personal data. Article 6 No. 2 DMA is related to the European Commission's Article 102 TFEU proceeding against Amazon – see Case AT.40462 – *Amazon Marketplace* (pending).

[666] See also Borgogno/Colangelo, Platform and Device Neutrality Regime: The Transatlantic New Competition Rulebook for App Stores?, TTLF Working Papers No. 83.

2. Data access obligations and other data-related rules in § 19a GWB

In Germany, a special regime of abuse control for undertakings of paramount cross-market significance for competition is already in operation: with the 10th amendment of the GWB, which entered into force in January 2021, a new § 19a GWB has been passed. Its goal is to empower the Bundeskartellamt to – firstly – designate undertakings that hold a special position of cross-market power that comes with the control of broad digital 'ecosystems' (§ 19a(1) GWB); and then to impose tailored obligations upon the designated norm addressees in a second step. The obligations can be selected from a conclusive list of seven possible obligations/prohibitions set out in § 19a(2) GWB. While there is a significant overlap between the rules of conduct in Articles 5 and 6 DMA and the obligations that the Bundeskartellamt may impose under § 19a(2) GWB, the latter are formulated more broadly. In five of the seven obligations/prohibitions, a more general description of the type of conduct that can be prohibited is combined with more specific examples that shall illustrate the type of conduct to be addressed. But these examples are not conclusive. So far, the Bundeskartellamt has initiated proceedings under § 19a(1) GWB (designation of norm addressees) against Meta (Facebook),[667] Amazon,[668] Google (Alphabet)[669] and Apple.[670] Google (Alphabet) was the first undertaking to be designated an undertaking of paramount cross-market significance for competition under § 19a(1) GWB.[671] The designations of Meta (Facebook)[672] and Amazon[673] have followed. No decision under § 19a(2) GWB has been taken so far.

a) Data portability and access obligations in § 19a GWB

In many respects, § 19a(2) GWB allows for the imposition of obligations upon norm addressees that may reach beyond the DMA. However, this is not the case when it comes to data access: In this regard, § 19a(2) GWB appears to be significantly less ambitious than the DMA. § 19a(2), 1st sentence, No. 5 GWB empowers the Bundeskartellamt to impose data portability obligations: according to this provision, the Bundeskartellamt may prohibit a norm addressee from "refusing the interoperability of products or services or data portability, or making such interoperability or data portability more difficult, and thereby impeding competition". A denial of, or

[667] Bundeskartellamt, First proceeding based on new rules for digital companies – Bundeskartellamt also assesses new Sec. 19a GWB in its Facebook/Oculus case (Press release of 28.1.2021).

[668] Bundeskartellamt, Proceedings against Amazon based on new rules for large digital companies (Sec. 19a GWB) (Press release of 18.5.2021).

[669] Bundeskartellamt, Proceeding against Google based on new rules for large digital players (Sec. 19a GWB) – Bundeskartellamt examines Google's significance for competition across markets and its data processing terms (Press release of 25.5.2021).

[670] Bundeskartellamt, Proceedings against Apple based on new rules for large digital companies (Section 19a (1) GWB) - Bundeskartellamt examines Apple's significance for competition across markets' (Press release of 21.6.2021).

[671] Bundeskartellamt 30.12.2021, B7-61/21 – *Google/Alphabet*.

[672] Bundeskartellamt 2.5.2022, B6-27/21 – *Meta (vormals Facebook)*, case report.

[673] Bundeskartellamt 5.7.2022, B2-55/21 – *Amazon.com, Inc.*, case report.

restrictions on data portability will frequently hamper multihoming or the switching of users to competing services.[674] Whether § 19a(2), 1st sentence, No. 5 GWB empowers the Bundeskartellamt to require a norm addressee to provide business users with full access and use of the data generated by their offer (similar to Article 6 No. 10 DMA) is less clear. However, § 19a(2), 1st sentence, No. 5 GWB may, by implication, enable the Bundeskartellamt to impose data access obligations upon a norm addressee to the extent that such data access is necessary to ensure the (vertical or horizontal) interoperability of products or services, where competition would be hampered in the absence of such interoperability.

Clearly, § 19a(2) GWB lacks a provision analogous to Article 6 No. 11 DMA, i.e. a provision that would empower the Bundeskartellamt to mandate a search engine to grant access to ranking, query, click and view data generated by end users. Nor does § 19a(2) GWB foresee a possibility to impose access obligations upon norm addressees in other potential 'scenario 2' settings – i.e. in situations where third parties request access to bundled individual or aggregate data in order to compete with the norm addressee on a primary or a complementary market.

b) Other data-related obligations in § 19a GWB

While § 19a GWB is more restrictive than the DMA as regards data access obligations, it goes beyond the DMA in empowering the Bundeskartellamt to impose limitations to the collection, combination and use of data. According to § 19a(2), 1st sentence, No. 4 GWB, the Bundeskartellamt may prohibit a norm addressee from "creating or appreciably raising barriers to market entry or otherwise impeding other undertakings by processing data relevant for competition that have been collected by the undertaking, or demanding terms and conditions that permit such processing". This rather broad catch-all provision is illustrated by two more specific examples. In particular, the Bundeskartellamt may prohibit a norm addressee from

> "a) making the use of services conditional on the user agreeing to the processing of data from other services of the undertaking or a third-party provider without giving the user sufficient choice as to whether, how and for what purpose such data are processed;" or from
>
> "b) processing data relevant for competition received from other undertakings for purposes other than those necessary for the provision of its own services to these undertakings without giving these undertakings sufficient choice as to whether, how and for what purpose such data are processed".

§ 19a(2), 1st sentence, No. 4 lit. a GWB resembles Article 5 No. 2 DMA and is based on the Bundeskartellamt's experience with the German Facebook case.[675] It goes beyond the Facebook case in that it is not limited to the combination of personal data, but extends to the combination of non-personal data, and in that it does not only protect individual end users, but also business users.

---

[674] Bundestag publication 19/23492, p. 77.

[675] Bundeskartellamt 6.2.2019, B6-22/16 – *Facebook*.

Just like Article 5 No. 2 DMA, § 19a(2), 1st sentence, No. 4 lit. a GWB does not amount to an absolute prohibition of combining different data sources. Rather, the user must be offered a choice: s/he must have the possibility to opt for a 'basic' version of the service that is based on the 'on-service' data only, instead of contracting for a potentially more individualised service that is based on a combination of different data sources. The extent to which services are personalised on the basis of the combination of different datasets shall thus be determined by the users' free choice. The choice offered to users must then be a meaningful one. While the consent of the user required is to be distinguished from the consent requirement under Article 6(1) lit. a GDPR, a 'real' and informed consent is required. Default settings that nudge users to accept the combination of data sources will not be in compliance with § 19a(2), 1st sentence, No. 4 lit. a GWB.

§ 19a(2), 1st sentence, No. 4 lit. b GWB, on the other hand, empowers the Bundeskartellamt to prohibit a norm addressee from exploiting the business users' dependency for seizing more data from these business users, and thereby expanding its own data-related competitive advantages.

For example, a norm addressee providing analytical software to its business users which enable these users to evaluate user activities on their websites may be prohibited from automatically transferring all relevant data to the norm addressee; an app store provider may be prohibited from forcing app providers to agree that all app usage data is transferred to the app store provider; and a trading platform – like Amazon – may be prohibited from using the data generated through the activity of retailers active on that platform for competing with those retailers (see, for a similar prohibition, Article 6 No. 2 DMA).

The list of possible prohibitions is complemented by § 19a(2), 1st sentence, No. 7 GWB which empowers the Bundeskartellamt to prohibit a norm addressee from demanding disproportionate benefits for handling the offers of another undertaking, in particular from

> "a) demanding the transfer of data or rights that are not absolutely necessary for the purpose of presenting these offers" or from
>
> "b) making the quality in which these offers are presented conditional on the transfer of data or rights which are not reasonably required for this purpose."

§ 19a(2), 1st sentence, No. 7 GWB has been introduced with a view to protecting publishers against being pressured into accepting 'unfair' conditions in exchange for the access to or a favourable ranking of their content on a norm addressee's platform. Its practical relevance in other settings is not yet clear.

3. Relationship between DMA and § 19a GWB

Given both the overlaps and the differences between the data-related obligations in the DMA and the possibilities for the Bundeskartellamt to impose data-related obligations, the

relationship between the DMA and § 19a GWB comes into view. This relationship has been highly contentious during the DMA trilogue proceeding.[676] With a view to avoid a fragmentation of the internal market, the EP Committee on the Internal Market and Consumer Protection proposed to exclude a parallel application of § 19a GWB and similar national norms.[677] Ultimately, Article 1 No. 6 DMA strikes a different balance: while the Member States must refrain from imposing regulatory obligations upon gatekeepers (Article 1 No. 5 DMA), EU competition rules and the corresponding national competition rules remain applicable alongside the DMA. Also, national competition rules may also impose *additional obligations* on gatekeepers within the meaning of Article 3 DMA.[678] Such rules shall qualify as competition rules if they are "based on an individualised assessment of market positions and behaviour, including its actual or likely effects and the precise scope of the prohibited behaviour, and which provide for the possibility of undertakings to make efficiency and objective justification arguments for the behaviour in question". § 19a GWB clearly qualifies as 'national competition law' according to this definition.

Nonetheless, national competition authorities must not take decisions that run counter to the DMA, or to a decision adopted by the European Commission under the DMA (Article 1 No. 7). Once the DMA has entered into force and the gatekeepers have been designated, the obligation to enable data portability for end users (Article 6 No. 9 DMA) and to ensure effective access to data for business users (Article 6 No. 10 DMA) will apply automatically, and it will be for the European Commission to decide on the precise specifications for data portability and data access. Given that § 19a(2) GWB – as it now stands – rather stays behind the DMA when it comes to data access, the room for additional action by the Bundeskartellamt under § 19a GWB appears to be small. However, the obligations under Articles 5 and 6 DMA apply to gatekeepers under the DMA only, and only to the 'core platform services' identified in the relevant designation decision pursuant to Article 3 No. 7 DMA. Under § 19a GWB, the Bundeskartellamt, on the other hand, is empowered to impose § 19a(2) GWB-obligations on the norm addressees with respect to any part of their activity if this is appropriate to address a relevant competitive risk. In this regard, some room for additional data portability requirements may remain. Also – as set out above – § 19a(2) GWB empowers the Bundeskartellamt to impose more far-reaching limitations to the collection, combination and use of data. In these regards, § 19a GWB may, in the future, complement the gatekeeper obligations that follow from the DMA. Where considering the imposition of such obligations, the Bundeskartellamt has to comply with the obligations to cooperate with the European Commission and the ECN as set out in Articles 37 and 38 DMA.

---

[676] For a more detailed discussion see Zimmer/Göhsl ZWeR 2021, 29 (56 et seq.).

[677] European Parliament, Report on the proposal for a regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act) (30.11.2021), A9-0332/2021, Amendment 6. In favour of a continued parallel application of § 19a GWB on the other hand: Bundestag publication. 19/25868, p. 9 et seq. and the Protocol Declaration of the acting Government of the Federal Republic of Germany on the DMA, issued in advance of the Competitiveness Council of 25.11.2021. See also: Zimmer/Göhsl ZWeR 2021, 29 (59 et seq.); Kühling, Tackling Big Tech, Verfassungsblog of 14.5.2021, https://verfassungsblog.de/tackling-big-tech/ (last visited 4.7.2022).

[678] See also Schweitzer in Immenga/Mestmäcker, GWB, 7. ed. 2022, § 19a paras. 64 et seq.

4. Open policy issues

Although data-driven advantages are considered to be (1) among the core reasons for the difficulty to contest gatekeepers/digital ecosystem providers; (2) important drivers of platform envelopment strategies; and (3) the core of the extremely successful advertisement-driven business models of Google (Alphabet) and Meta (Facebook), the data-related obligations remain quite cautious.

This is particularly true for § 19a GWB, which empowers the Bundeskartellamt to impose data portability obligations, but no further reaching obligations to grant access to and use of data to business users.

The DMA strives to establish rights of end users and business users to access and use those data which is generated based on their own platform activity. In this focus on – according to our categorisation – data access according to scenario 1, the DMA is akin to the Draft Data Act[679] (see below, part F(I)): both Acts seem to be driven by the idea that the users of products or services should have a privileged right to access the data they co-generate, and that this will enhance the ability for businesses to compete on the platform, or possibly in complementary markets, and to develop their digital and (partly) data-driven business models. But arguably, this right will not level the huge data-driven advantages that gatekeepers enjoy vis-à-vis smaller business users of their core platform services.[680] The data-driven barriers to entry into the markets dominated by gatekeepers will remain high.

A gatekeeper's engagement in data-driven platform envelopment strategies will be somewhat complicated by the necessity to obtain the consent of end users for the combination and the cross-use of personal data, both under the DMA (Article 5 No. 2 DMA and (possibly) under § 19a(2), 1st sentence, No. 4 lit. a GWB). But where the gatekeepers can show that the bundled services come with increased convenience or other benefits for end users, this may ultimately not be a severe hurdle.

Neither the DMA nor § 19a GWB address concerns that the norm addressees may have built up a form of 'data power' that may provide them with huge competitive advantages in the field

---

[679] The scope of the Draft Data Act is limited to 'data generated by the use of a product or related service'. In this regard, the DMA – with its focus on data generated in the use of digital services – and the Draft Data Act appear to be complementary.

[680] Some consider that the rules on data portability and access will primarily benefit competing gatekeepers who are in a position to realize the full potential of such data access – see Baschenhof, The Digital Markets Act (DMA): A Procompetitive Recalibration of Data Relations?, 2021, https://ssrn.com/abstract=3970101 (last visited 4.7.2022), p. 60 et seq. See, in particular, p. 62, with a view to Article 6 No. 11 DMA: "... many gatekeepers have business models that are similar in that they rely on the monetization of 'insights from user data", so that the data collected by search service providers using a similar business model may be more useful to them than to smaller search service providers with a 'radically different service'. Furthermore, gatekeepers are more likely to have the funds and scale to be able to incorporate the data provided to them by other gatekeepers than smaller providers'.

of AI as a fundamental multi-purpose technology of the future. Our data access scenario 3 – which arguably falls outside the scope of traditional competition law – remains unaddressed also by the DMA and § 19a GWB.

Finally, the implementation of data-related obligations may be a challenge to competition authorities. This is particularly true for data portability and data access obligations. Their effectiveness will, *inter alia*, depend on the availability of technical specifications and standards. Ways need to be found to ensure their practicability and usefulness for competitors – but their flexibility at the same time.

F. Policy options and discussion

Based on the weaknesses and deficiencies of the existing legal framework identified in part E, we now explore potential policy options and possible needs for reform: Should the German legislator support the new data access rights as proposed in the Draft Data Act with a view to promoting competition and innovation? Do we need changes in substantive competition law and/or procedural law to promote voluntary data sharing and pooling? Is there a need to go further in mandating access to data under European and German competition law, and if so in which settings and in which manner? Or do we rather need more sector-specific regulation? Are changes needed in the realm of merger control? And which role can data intermediaries play in enabling or promoting data access, and which legal framework is appropriate for them?

We will first discuss the Draft Data Act, asking whether the data access rights it proposes and the legal framework it will establish are likely to contribute, or can be made to contribute, to a well-functioning data economy (I). We will then focus on possible reforms in the realm of competition law, including merger control (II), before turning to the role of contract law (III). Finally, we will look at the potentials of data intermediaries in promoting data access and data sharing (IV).

I. The Draft Data Act

1. Main features and aims of the Draft Data Act

a) 'Horizontal' data access right and supplementary tools

The existing legal framework provides for limited data access rights only. This is true, also, with regard to eventual rights of a product user to access, port and process data that is generated in the course of this user's use of a product (our data access scenario 1). To the extent that the data qualifies as personal data within the meaning of Article 4 No. 1 GDPR, Article 20 GDPR grants a right to data portability with limited effectiveness (see above, part E(I)(4)). Beyond Article 20 GDPR, neither European nor German law provide for a general portability or access right. Rather, under contract law and competition law, portability and access rights will exist only under specific conditions. In some sectors, specific regulatory regimes will apply.

The Draft Data Act now proposes to introduce a 'horizontal' data access[681] right both B2C and B2B, i.e. a right that is not confined to specific sectors. It is not designed as an all-embracing data access regime. Rather, data holders shall be obliged to grant product users access to the "data generated by the use of the product or related service" (Article 4(1)) and, upon request by the product user, to share those data it with third parties acting on behalf of the user (Article 5(1)). Hence, the scope of the access right is limited to 'observed data' within the categorisation

[681] Draft Data Act, Explanatory Memorandum, 5.

of the OECD, and only to those kinds of 'observed data' that are generated by the use of a product directly or by a digital service that is "incorporated in or interconnected with a product in such a way that its absence would prevent the product from performing one of its functions" (Article 2(3) of the Draft Data Act). Other kinds of data which are not machine-generated in that sense, e.g. data collected by social media providers or other online services that lack a physical product component (like a search engine or a trading platform), are not included. Also, the Draft Data Act does not apply to information derived or inferred from this data.[682] In order to make the right to data access effective, the Draft Data Act combines different regulatory tools:

- It creates an obligations to design and manufacture products and related services with a view to ensuring the easy and secure accessibility of data, Article 3(1).
- It imposes a duty to provide information before the conclusion of a contract for the purchase, rent or lease of a product or a related service (including virtual assistant services – see Article 7(2)), on the nature and volume of the data likely to be generated from the use of the product or related service, how the user may access this data etc., Article 3(2).
- Upon the request of the user, the data holder must make the data available to third parties, Article 5. Third parties may process the data only for the purposes and under the conditions agreed with the user, and within the limitations as set out in Article 6(2).
- A special legal regime for data holders legally obliged to make data available specifies the conditions under which the data is to be made available (especially FRAND requirements), limits for any possible compensation of the data holder, access to a dispute settlement regime and rights of the data holder to apply appropriate technical protection measures when sharing the data, Articles 8-12.
- Rules on unfair terms in B2B data access contracts are set out, Article 13.
- A special legal regime for B2G data access is provided, Articles 14-22.
- The European Commission is mandated to develop model contract terms, Article 34.

In addition to the rules directly concerned with B2C and B2B data access, the Draft Data Act includes various provisions that aim at fostering access to and use of data indirectly:

- Rules on the switching between providers of data processing services, Articles 23-26,
- Restrictions on international transfer or governmental access to non-personal data, Article 27,
- Rules on the interoperability requirements for data processing services, smart contracts and European data spaces, Articles 28-29,
- A limitation of the effect of sui generis data base rights, Article 35 (see supra part E(I)(2)).

b) Aims, legal nature and main features of the data access right

The aim of the Draft Data Act is set out in the Recitals[683] and the Explanatory Memorandum: It shall ensure that users of a product or related service have access to data they 'co-generate' by the use of the product or service and thereby avoid data-based 'lock-ins' and promote

[682] Recital 14 Draft Data Act.

[683] Recitals 5, 6.

aftermarket innovation; it shall prevent "the exploitation of contractual imbalances that hinder fair data access and use for micro-, small- or medium-sized enterprises" and thereby "ensure a fairer allocation of value in the data economy".[684] Furthermore, it shall enhance the "interoperability of data and data sharing mechanisms and services", and "facilitate switching between data processing services".[685] Overall, it shall promote data access with a view to "unlocking the value of data in Europe" and enhance opportunities of innovation.[686] The consistent reference of these aims to the Internal Market goal are reflected in the choice of Article 114 TFEU as the legal basis.

By granting a right to access the data generated by the use of an Internet of Things (IoT) object, the Draft Data Act enhances consumer choice.[687] However, the access right in Article 4 is not limited to consumers but extends to all users of a product. Quite in a competition policy spirit, the Draft Data Act is to enhance user choice, broadly understood. By contrast, the third party's rights to access to data as set out in Article 5 of the Draft Data Acts are derived rights only. The third party may process the data "only for the purposes and under the conditions agreed with the user" (Article 6(1) of the Draft Data Act). The specification that the data must not be used to "coerce, deceive or manipulate the user, by subverting or impairing the autonomy, decision-making or choices of the user" would seem to follow from the contract to be concluded between the user and the third party as a collateral duty of 'good faith'. Although the right to data access created by the Draft Data Act is therefore, primarily, a right of the product user, much of the Draft Data Act is concerned with framing the B2B relationship between the data holder and third party data recipients: frequently, they will be the entities to deal with the data holders directly.

While the aims of the Draft Data Act are set out in some detail, the legal nature of the newly created access right remains unspecified. It bears some relation to contract, (intellectual) property and competition law, but does not fall squarely into either of these basic categories. The explanatory memorandum and the Recitals do not take a position in this regard. It is clear nonetheless that a product user's access right under Article 4 is of a non-contractual nature: it does not presuppose a contractual relationship between that user and the data holder. The access right is irrespective of a pre-existing relationship with the data holder. Contracts do play an important role for the implementation of the access right, however. The need for a contractual implementation influences the legal regime before and after the claim for access to data. The seller or lesser of a product or related service is under an obligation to inform the user about the data generated by the product and service and about the access right. Also, once access is claimed, the details will be specified in a contract which must implement the (FRAND) terms set out in Article 8.

[684] Draft Data Act, Explanatory Memorandum, 15.

[685] Recital 5.

[686] Draft Data Act, Explanatory Memorandum, 1.

[687] Draft Data Act, Explanatory Memorandum, 13.

Nor does the Draft Data Act create a new (intellectual) property right or reinforce existing entitlements. According to Article 35, databases containing data obtained from or generated by the use of a product or related services are carved out from the scope of the data holder's 'sui generis' database rights. With regard to trade secrets, the Draft Data Act is neutral. Simultaneously, the Draft Data Act refrains from creating a novel exclusive legal position for the data holder or user. Economically, its basic idea of a "fair allocation of data value" may be conceptualised as reflecting the users 'partial ownership' (or 'co-ownership') of the data value. But this economic intuition has not resulted in the creation of an exclusive right owned or co-owned by the data holder and the user.

Finally, the data access right as set out in the Draft Data Act differs from a 'conventional' access remedy under competition law. While the proposed access right prevents the emergence of 'usage data monopolies' and facilitates the competitive provision of aftermarket and complementary services in IoT settings, it is granted irrespective of an analysis whether the data holder is dominant on a primary market and of whether a refusal to grant access would amount to an abuse of dominance. Rather, the right to FRAND access to 'co-generated' usage data is granted to product users 'across the board'. It has structural consequences for access to and competition in aftermarkets and complementary markets. But it is to be distinguished from a competition law remedy.

Simultaneously, the ambition to promote competition on complementary markets (and those only) drives the design of the new data access right and the legal regime surrounding it in various respects. The pro-competition goals show, *inter alia*, in the requirement that neither the user nor the third party shall be asked to provide any information to the data holder beyond what is necessary to verify the quality as a user or authorised third party (Articles 4(2) and 5(3) Draft Data Act) – a principle that shall ensure independent planning by the data holder and the user/third party, and thereby undistorted competition. The limitation of the pro-competition goals to complementary markets is reflected in the limitations to the right to share data with third parties in Article 5, as well as the constraints imposed on the data use both by the product user and by third parties in Articles 4 and 6 of the Draft Data Act. Neither the product user nor a third party acting on behalf of the user shall use the data "to develop a product or related service that competes with the product or related service from which the data originate" (see Articles 4(4) and 6(2) lit. e of the Draft Data Act). According to Recital 28, this limitation "aims to avoid undermining the investment incentives for the type of product from which the data are obtained". The Data Act shall stimulate innovation in aftermarkets and foster the development of entirely novel, innovative products and services. But it shall not promote the contestability of any given position of power on the primary market. The merits of this approach are controversial. Many commentators have argued that Articles 4(4) and 6(2) lit. e of the Draft Data Act are necessary to protect the legitimate interests of the data holder.[688] Competitors may

[688] See, *inter alia*, Drexl et al., Position Statement of the Max Planck Institute for Innovation and Competition of 25 May 2022 on the Commission's Proposal of 23 February 2022 for a Regulation on Harmonised Rules on Fair Access to and Use of Data (Data Act) (25.5.2022), https://ssrn.com/abstract=4136484 (last visited 4.7.2022),

compete on the primary product market, but they may not use the insights to be gained from the usage data stream to compete. However, in an economy that is increasingly characterised by individualised products, it may be exactly this stream of usage data that competitors need to tailor their product to the needs of the product user. It is unclear whether such a use would fall under the Article 4(4) prohibition, such that the data portability right of a product user under the Data Act – quite contrary to data portability under Article 20 GDPR – would not protect that user from a data-driven lock-in. It is unclear why, in this setting, the interests of the data holder would systematically outweigh the interests of the product user. Simultaneously, a situation in which access to the stream of usage data would allow a product user or third party to 'reverse engineer' the primary product would seem to be rare. It is doubtful whether Articles 4(4) and 6(2) lit. e of the Draft Data Act, as currently drafted, strike an appropriate balance.

Also, Article 5 requires the data holder to make available the co-generated usage data to a third party upon a user's request but excludes designated gatekeepers under Article 3 DMA as eligible third parties. What is more, such gatekeepers shall not solicit or commercially incentivise a user to supply to one of its services data that the user has obtained under the Data Act's access right or accept to receive such data (Article 5(2) of the Draft Data Act). For explanation, Recital 36 refers to the 'unrivalled ability' of gatekeepers to acquire data, such that access to product usage data would not be necessary to achieve the objectives of the Data Act – i.e. the goal to promote competition and innovation in aftermarkets or complementary markets. An obligation to grant access to gatekeepers upon the request of a user would "thus be disproportionate in relation to data holders". Even a gatekeeper may depend on access to individual level usage data in order to offer a tailored complementary service, however. Hence, the exclusion of gatekeepers from access to data cannot be read as following from some sort of in-built indispensability criterion (i.e. access is granted only if indispensable for the provision of complementary services) – a criterion which does not inform the Draft Data Act's access rights anyhow. Rather, it reacts to a concern that such data access could enable gatekeepers to engage in even more far-reaching envelopment strategies by which they would leverage their positions of power from core platform service markets to complementary data-driven product or services markets. While this is a risk indeed, the appropriate answer may be not to exclude gatekeepers from data access under Article 5 of the Draft Data Act, but to grant access only based on the gatekeeper's commitment to open up its own data troves for sharing (see on this: part F(II)(2)(c)). Ultimately, an exclusion of gatekeepers from data access under Article 5 of the Draft Data Act would not only amount to an implicit 'line of business restriction' for gatekeepers,[689] but it would severely restrict the rights of product users to freely choose how to make use of 'their' data.

---

para. 87. See also Picht, Caught in the Acts: Framing Mandatory Data Access Transactions under the Data Act, further EU Digital Regulation Acts, and Competition Law, Max Planck Institute for Innovation and Competition Research Paper No. 22-05, p. 20-21. Bomhard/Merkle,RDI 2022, 168, (172) point to some open questions but do not criticise the non-compete clause fundamentally.

[689] Recital 36 of the Draft Data Act states that the "exclusion of designated gatekeepers from the scope of the access right under this regulation does not prevent these companies from obtaining data through other lawful means". This somehow softens the restriction. For example, a gatekeeper may get access on the basis of Article

Article 7 introduces another exception to the otherwise horizontal applicability of the data access rights: The obligation to make data generated by the use of a product or related service accessible and the obligation to grant data access to product users or third parties authorised by them shall not apply to products manufactured or related services provided by small and medium-sized enterprises: with a view to incentivising innovation, they shall be protected from "excessive economic burdens" (Recital 44).

c) Critical evaluation of the general approach of the Draft Data Act

Overall, the Draft Data Act proposes to create a potentially strong right to data portability (broadly understood) for data generated in the use of a machine – including continuous and real-time access – that is independent of any position of market power of the data holder, or of dependence within the meaning of § 20(1a) GWB of the product user. In the Draft Data Act, the right to access to data is not conceptualised as a remedy to a market failure – namely market power – or an abuse of dominance. Rather, it is part of the legal infrastructure on which the relationships between market actors in the IoT context are to be based. The legislator reacts to a perceived need to take a basic decision on the allocation of rights in data as they gain novel economic importance in the emerging data economy. The fact that, in the IoT context, the product user, too, contributes to the generation of the data, and the economic intuition that, given the non-rivalry of data in its use, this justifies an attribution of 'co-ownership', is translated into a legal regime of access rights. Indeed, the multiplication of rights of use in data seems desirable as it may avoid the emergence of monopoly positions regarding what may be an important input in innovation and a key factor for competition.

However, there may be cases in which efficiency grounds may argue for an exclusive use of data. For example, an exclusive use of the data may allow the data holder to undertake long-term investments which it may otherwise not be willing to do. The Draft Data Act raises the question whether room remains to capture these potential efficiencies of exclusivity – at least in settings where there is no imbalance of power between the parties. This translates into the question if and under which conditions the data access rights under the Draft Data Act can be waived contractually. We turn to this question below (2(c)(bb)).

While striving to establish a new allocation of rights in data, the Draft Data Act has its limits. Firstly, the focus is on access rights of data 'co-generators' – and thereby on the allocation of rights in response to our access scenario 1: the Draft Data Act creates a right to data portability, broadly understood. It has nothing to say on our data access scenario 2 (which, consequently, remains the domain of competition law) and on our data access scenario 3 (which remains to be resolved as a matter of innovation policy). Secondly, the right to data access is limited to the data generated by the use of a product or related service (including virtual assistants). Data

20 GDPR. But Article 20 GDPR does not grant a right to continuous, real-time access. And it this may not suffice for offering a fully functional complementary service.

generated by the 'mere' use of a service remains outside the scope of the Draft Data Act. However, Article 6 No. 9 and No. 10 DMA now establish relatively broad data portability rights of consumers and business users – albeit vis-à-vis gatekeepers only.

2. Allocation of rights under the Draft Data Act

a) Manufacturer and distributor of products

According to Article 3(1) "products shall be designed and manufactured, and related services shall be provided, in such a manner that data generated by their use are, by default, easily, securely and, where relevant and appropriate, directly accessible to the user." This approach to make data accessibility part of the product design deserves support.[690] However, it should be stipulated who can initiate which private enforcement measures in case of non-performance.

Article 3(2) complements the product design approach by an information duty with regard to the data generated by the product or related service. Before concluding a contract for the purchase, rent, or lease of a product or the provision of a related service, clear and sufficient information should be provided to the user on how the data generated may be accessed. This obligation does not affect the obligation for the controller to provide information to the data subject pursuant to Articles 12, 13 and 14 GDPR.[691] A comparable information duty – with a different field of application – has already been enacted in Article 9(1) and (2) P2B Regulation,[692] according to which 'online intermediation services' shall include in their terms and conditions a description of any personal data or other data which business users or consumers provide for the use of services concerned and of the technical and contractual access to such data.

Information duties of this kind, especially Article 3(2), are of major importance for the effectivity of the envisaged access rights. Users typically do not know what data is collected by the manufacturer or other data holder. This may prevent users from requesting access to data. The absence of information on what kind of data is available may be one of the reasons why data access requests have remained relatively rare so far. Therefore, the information duty in Article 3(2) deserves support even if it may lead to again another layer of small print information that may not be read by all users. What is more: it may be indicative of a need to impose a similar information duty on dominant undertakings under Article 102 TFEU and/or § 19 GWB where these may be subject to data sharing obligations (see below II(2)(d)).

However, the Draft Data Act should clarify who precisely is the addressee of this obligation. This will not be an issue where the manufacturer and seller (or lessor) are identical. In the more

---

[690] Drexl et al., Position Statement of the Max Planck Institute for Innovation and Competition of 25 May 2022 on the Commission's Proposal of 23 February 2022 for a Regulation on Harmonised Rules on Fair Access to and Use of Data (Data Act) (25.5.2022), https://ssrn.com/abstract=4136484 (last visited 4.7.2022), paras. 73-74.

[691] Recital 23 Draft Data Act.

[692] OJ 2019 L 186, 57.

typical scenario, where the manufacturer does not sell its products directly to its users, only the manufacturer should be subject to the obligation – and not the seller (or lesser) who may not know exactly what data is collected by the product.[693] For the seller, an analogous obligation may result from Article 7(1)(d) Sales of Goods Directive[694] or Article 8(1)(b) Digital Content Directive[695] ("possess the qualities and performance features, including in relation to functionality, compatibility, accessibility, continuity and security, normal for digital content or digital services of the same type and which the consumer may reasonably expect").[696]

b) Legal position of the data holder

The Draft Data Act does not create new intellectual property rights, nor does it recognise any other kind of property or exclusive ownership right of the data holder which could be enforced against users or third parties.[697] Still, in economic terms, the proposal may be read as an indirect recognition of a technical, de facto exclusive position of the data holder.[698] Where the requirements of the access rights of Articles 4 and 5 are not met, the data holder remains free to technically exclude others from accessing machine-generated data. Article 11 of the Draft Data Act even recognises explicitly that the data holder may use technical protection measures. Nonetheless, this indirect recognition does not amount to a legal property or ownership right. Rather, the gist of the Draft Data Act is to enact broad horizontal access rights for users and (derivatively) for third parties.

Simultaneously, the data holder shall be constrained in his or her use of the data: according to Article 4(6), the data holder shall only use any non-personal data generated by the use of a product or related service on the basis of a contractual agreement with the user. This proposal has been criticised by commentators: if Article 4(6) were to be taken literally, every use of the covered data would depend on the user's contractual consent. A simple consent would not suffice; applying 'implied terms' theories from national contract law would entail the risk of a violation of the principle of effectiveness of EU law.[699] The result of such a regime would be that data holders, in order to make use of the collected data, would need to enter into contracts

---

[693] Drexl et al., Position Statement of the Max Planck Institute for Innovation and Competition of 25 May 2022 on the Commission's Proposal of 23 February 2022 for a Regulation on Harmonised Rules on Fair Access to and Use of Data (Data Act) (25.5.2022), https://ssrn.com/abstract=4136484 (last visited 4.7.2022), para. 74.

[694] OJ 2019 L 136, 28.

[695] OJ 2019 L 136, 1.

[696] See Metzger in MüKBGB, 9th ed. 2022, § 327e para. 34. See also Drexl et al., Position Statement of the Max Planck Institute for Innovation and Competition of 25 May 2022 on the Commission's Proposal of 23 February 2022 for a Regulation on Harmonised Rules on Fair Access to and Use of Data (Data Act) (25.5.2022), https://ssrn.com/abstract=4136484 (last visited 4.7.2022), para. 74.

[697] Recital 6 Draft Data Act; COM SWD(2022) 34 final, 154.

[698] See Kerber, Governance of IoT Data: Why the EU Data Act will not fulfill its objectives (8.4.2022), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4080436 (last visited 4.6.2022), p. 1.

[699] But see Leistner/Antoine, IPR and the use of open data and data sharing initiatives by public and private actors (Evaluation of the proposed Data Act), Study for the European Parliament Committee on Legal Affairs (JURI), 2022, p. 92.

with every user.[700] Such a regime would create a hold-up position for users and go far beyond their legitimate interests.[701] With regard to non-personal, machine-generated data, users would be in a much stronger legal position than data subjects are with regard to personal data under the GDPR.[702]

The aim of the Draft Data Act – to enable independent innovation and competition in aftermarkets and complementary markets – would suggest a different approach: both co-generators, the data holder and the product user, should be granted an independent right to use the data without the approval of the other party.[703] The rights of use and their limits should be symmetrical: the data holder should not depend on the consent of the user to use co-generated data as long as the legitimate interests of the user are not concerned. This idea is reflected in the second sentence of Article 4(6) of the Draft Data Act but should be drafted in clearer and more general terms.[704] Inversely, the product user, having requested access to data, does not need to ask the data holder for consent with regard to the intended use of the data (see Article 4(1)-(4)). Simultaneously, the Draft Data Act provides for a number of safeguards for the interest of the data holder. These safeguards are not without doubt when it comes to restrictions for the development of competing products in Article 4(4), see supra at 1(c). However, they also reflect the more general idea that the user should be free to use the data as long as the data holder's interests are not concerned. The legislature should further specify what a legitimate interest is that may justify restrictions of use of the data. Any attempts of industrial espionage which goes beyond the use of machine-generated data and any use to the detriment of the other party affects its legitimate interests and requires consent. The mere use of machine-generated data for the development of competing products is not really a likely case; and it should not as such be considered to affect the legitimate interests of the other party. Both parties should have an opportunity to use the co-generated data for the development of competing products.

c) Access right of user

aa) Conditions for data access by user

As sketched above, the core of the Draft Data Act is the creation of a right of a product user to access the data generated by the use of the product or related service (Article 4(1) Draft Data

[700] The mere collection seems to be allowed without a contract.

[701] Drexl et al., Position Statement of the Max Planck Institute for Innovation and Competition of 25 May 2022 on the Commission's Proposal of 23 February 2022 for a Regulation on Harmonised Rules on Fair Access to and Use of Data (Data Act) (25.5.2022), https://ssrn.com/abstract=4136484 (last visited 4.7.2022), paras. 45-46.

[702] Bomhard/Merkle RDi 2022, 168 (174).

[703] But see Leistner/Antoine, IPR and the use of open data and data sharing initiatives by public and private actors (Evaluation of the proposed Data Act), Study for the European Parliament Committee on Legal Affairs (JURI), 2022, p. 93-94.

[704] Drexl et al., Position Statement of the Max Planck Institute for Innovation and Competition of 25 May 2022 on the Commission's Proposal of 23 February 2022 for a Regulation on Harmonised Rules on Fair Access to and Use of Data (Data Act) (25.5.2022), https://ssrn.com/abstract=4136484 (last visited 4.7.2022), para. 54, therefore suggest to delete Article 4(6) first sentence.

Act). Access must be granted "without undue delay, free of charge, and, where applicable, continuously and in real-time". A simple request through electronic means shall suffice to get access. The right of a product user to access the data generated by his/her use of a product encompasses a right to share the data with third parties (Article 5(1) Draft Data Act). Consequently, upon the request of a user or a third party acting on behalf of the user, the data holder is obliged to also grant access to that third party, again without undue delay, free of charge to the user, continuously and in real-time, and "of the same quality as is available to the data holder" (for more detail, see below, at d).

In principle, the right of access is conceived of as a right of an independent use of the data: the user is not required to inform the data holder of what use is intended (Article 4(2) Draft Data Act). In the light of the competition law on information exchange (see above, part E(III)(1)), this is essential to comply with the requirement of independent planning. Given that usage data is a competitively relevant input, the user as well as third parties must be able to compete and innovate without the data holder being informed of their business plans. Simultaneously, the Draft Data Act imposes limits on the use of the data by the product user in order to protect the data holder's legitimate interests. The legitimate interests pertain, firstly, to the protection of trade secrets: the data holder and the user can agree on measures to preserve the confidentiality of the shard data (Article 4(3)). Secondly, and controversially (see above), Article 4(4) of the Draft Data Act considers that the data holder has a legitimate interest in that the data is not used to develop a product that competes with the product from which the data originates.

bb) Waiver of access right

The parties may conclude a contract before any data access request is submitted. This begs the question if they can exclude the product user's access right from the outset. A first contract to be considered is the contract between the product user and the distributor of the product which collects data, e.g. a contract concluded between a car manufacturer and a car rental company that buys or leases a car fleet; a contract between the producer of an airplane and the airline that acquires it; or a contract between the land machine dealer and the farmer who buys a land machine. Such contracts may be concluded between the (later) data holder and product user within the meaning of the Draft Data Act, but this need not always be the case. Distribution chains may have multiple levels. Also for leasing or rental contracts, the party actually letting the product to a user, the manufacturer and the later data holder need not be identical. This is also reflected in Article 3(2)(e). But the parties may also agree on the waiver of the access right at a later stage.

The Draft Data Act seems to be based on the premise that the statutory allocation of the user's access right is of a mandatory nature, see Recital 40 and Article 12(2). However, this premise is not made explicit, and Article 12(2), which declares any deviating contractual terms to be non-binding, formally only applies to Articles 8-11 of the Draft Data Act. As mentioned above (see 1(c)), and with a view to the goals of the Draft Data Act, a justification for making the

access rights mandatory is difficult to find in the absence of a market failure.[705] A waiving of data access rights may sometimes be efficient for the parties and facilitate long-term investments of the data holder.

A market failure is plausible, however, if a manufacturer is given the full freedom to have users sign an unlimited waiver of all future access rights when the sale, rental or lease agreement is concluded. This is certainly true if the user is a consumer. But it may also be true vis-à-vis business users – even in the absence of market power – if the agreement is signed in a situation of asymmetric information. Typically, the data holder will know more about the nature of the collected data and its possible uses. While this asymmetry is meant to be addressed by the information duty in Article 3(2), the asymmetries are more profound and not fully offset by this provision. Frequently, neither party will be able to fully oversee the possible future uses of the collected data. Many companies with large collections of usage data continuously expand their 'data lakes' without full knowledge of what the exact use of this data will look like in the future. But the product user will often be in an inferior position when accepting a waiver pro futuro. The law should then provide means to ensure that both parties have a chance to participate in possible future business opportunities once they come visible.

This risk of being cut-off from all future business opportunities on aftermarkets does not occur in all practical scenarios, however. Users of products who accept a waiver of their access right and regret this decision later on when they discover the economic value of new business models, may decide to choose a different manufacturer when they acquire new products. Given that many everyday IoT devices have a rather short lifespan, users will have several opportunities to decide on a possible waiver. Yet, in other settings, the contract may concern durable industrial machinery. In such a case, the user may be bound by a contractual waiver of data access rights for many years if the contract does not foresee any revocation rights. Moreover, it cannot be expected that users will always find manufacturers offering products without a waiver requirement, especially on tightly oligopolistic markets. The potential imbalances caused by such long-term waivers may concern both SMEs and larger market actors.

Admittedly, the issue of overbroad assignments or waivers of future business opportunities is of a general nature. In principle, the owner of an asset, be it a property, a stock or a company, must live with the fact that the transferred asset may turn out to be of much higher value than expected at the moment of a sale or other transfer. But such a liberal approach would be inconsistent with the goal of the Draft Data Act to enable competition on aftermarkets based on user data, and would risk to undermine the whole idea of a new, more pro-competitive and innovation-friendly allocation of access rights. This is true even more in a setting in which the potential uses of data are not yet fully understood by many market actors and are bound to dynamically change in unforeseeable ways.

[705] Critical Leistner/Antoine, IPR and the use of open data and data sharing initiatives by public and private actors (Evaluation of the proposed Data Act), Study for the European Parliament Committee on Legal Affairs (JURI), 2022, p. 79-80.

Given this situation, a comparison with copyright law might be used as a source of inspiration. Statutory limits for broad assignments or waivers of future uses of works are of main importance in copyright law where the parties to a license contract oftentimes do not know whether the work can be exploited in new and profitable ways in the future, especially if parties conclude full buy-out agreements without knowledge of later possible modes of exploitation by new media channels. Under the traditional approach of German copyright law, such possible future modes of exploitation of works could not been waived or licensed. Recital 40 and Article 12(2) of the Draft Data Act may follow a similar rationale. In the case of copyright law, however, the legislator turned away from a mere invalidation of waivers in 2007 and instead implemented a right of revocation of such licenses on future uses in § 31a(1)(3) UrhG.[706]

The legislature would be well advised to reconsider whether the broad brushed mandatory nature of the access right should not be replaced by a more fine-lined approach under which – absent an imbalance of power – a waiver would be possible as long as the user retains a right of revocation after some period of time (2-3 years). The revocation of the waiver should only have effect ex nunc, i.e. concern data collected after the revocation. For products with a shorter average lifespan, the right of revocation could be dispensable. Such an approach would safeguard the user's chance to participate in the development of business models which are unforeseeable at the moment of the sale, rental or lease of the product. At the same time, manufacturers would have more flexibility to develop business models based on an exclusive exploitation of the collected data. The suggested restrictions on long-term waivers should apply irrespective of the size and market power of the user. For SMEs, a revision of unfair standard terms in accordance with Article 13 would still apply.

d) Third parties

The Draft Data Act is based on the general idea that product users – like the data holder – should have a right to access data they co-generate. It does not create access rights for previously unrelated third parties – i.e. access rights in what we call our scenario 2 settings. However, the Draft Data Act is not blind to the fact that the user may not be the most interested or competent party to develop services on aftermarkets. This is evident if the user is a consumer. But it may also be the case if a business user is not active on the relevant market. The Draft Data Act addressees this triangle of interests in Article 5. Third parties may benefit from the new access rights regime by receiving data either from users or directly from the data holders at the request of the user, Article 5(1). In any case, the use of data by third parties presupposes the involvement of a user and is bound to several limits and conditions provided for in Articles 5 and 6.

Regarding the relationship of users and third parties, Article 6(1) seems to presuppose that the parties conclude a contract under which the third party may use the data ("under the conditions agreed with the user"). The conclusion of such a contract is not a necessary precondition for the

[706] Spindler in Schricker/Loewenheim, Urheberrecht, 6. ed. 2020, § 31a paras. 1-5.

use of the data by a third party, but its conclusion is indeed likely. The Draft Data Act should clarify whether the third party may pay money as consideration for the user's willingness to make a request. In the prototypical situation, a product user will empower a third party to act on his or her behalf because s/he is interested in the third party's complementary service. But there may be situations where this motivation is not sufficient – e.g. because the third party's service is still in an early stage of its development. At least when it comes to non-personal data, a decision of a product user to "monetise" his or her data in such a way should be accepted if the legislator wants to reach its goal of opening new opportunities for aftermarket services.

Article 6(1) and (2) provide a number of obligations to be respected by the third party. The way these requirements are drafted seems to express their mandatory character, the underlying assumption being a structural imbalance of bargaining power or an asymmetry of information. This is most obvious in Article 6(2)(a) ("coerce, deceive or manipulate the user"). However, this assumption may be challenged. Imbalances of power or information may occur in scenarios where private parties or SMEs as users enter into agreements with larger companies with expertise for data driven services or products as third parties. But the economic power and expertise may also be allocated differently. Large users may be engaged with start-ups as 'third parties' which want to provide services based on the accessed data. Also, one should keep in mind that the Draft Data Act excludes large platforms ('gatekeepers') from being third parties, see Article 5(2). This takes some of the potentially largest 'third parties' out of the game. In light of the diversity of actors of all sizes and the different scenarios at stake, the legislature should reconsider the mandatory nature of the requirements in Article 6(1) and (2) at least for scenario in which the user is not a consumer or SME.

Some of the provisions of Article 6(1) and (2) seem to reflect reasonable default rules for contracts, especially Article 6(1) ("shall delete the data when they are no longer necessary for the agreed purpose"), Article 6(2)(c) ("shall not make the data available it receives to another third party..."), Article 6(2)(e) ("shall not use the data it receives to develop a product that competes...") and Article 6(2)(f) ("shall not prevent the user, including through contractual commitments, from making the data it receives available to other parties..."). Those provisions may be used as defaults for contracts but they should not be mandatory.

Other provisions reflect legal standards of a non-contractual character and as such should remain mandatory, especially Article 6(2)(a) ("shall not coerce, deceive or manipulate the user"), Article 6(2)(b) ("shall not use the data it receives for the profiling of natural persons"), and Article 6(2)(d) ("shall not make the data available it receives to an undertaking providing core platform services").

3. Role of contracts in the implementation of data access under the Draft Data Act

Data access under the Draft Data Act is provided as a non-contractual right. Requests under Article 4 do not presuppose a contract between the data holder and the user. Still, data access requests will oftentimes (if not typically) occur between parties which have previously concluded a contract. Also, the parties may specify the details of data access requests in a

contract after such a request is submitted to the data holder. Contracts may be concluded between the data holder, the user and the third party under Article 5 Draft Data Act. The Draft Data Act addresses these contracts in different provisions which are discussed here in the order of a possible chronology of contacts between the parties.

a) Contract between user and distributor of the product

A first contract to be taken into account is the contract between the user and the distributor of the product which collects data. The requirements for these contracts have been discussed above at 2(c)(bb).

b) Contracts between user and data holder

The Draft Data Act is based on the premise that data holder and product user conclude a contract or even conclude several different contracts.

A first contract between data holder and product user is presupposed in Article 4(6) for any use of the data *by the data holder*. Whether the Draft Data Act should require such a contract in all possible scenarios has been discussed critically above at 2(b). It is remarkable that the Draft Data Act hardly foresees any mandatory or default rules for this contract, with the exception of Article 4(6) sentence 2, but leaves it entirely to the parties' contractual freedom and national contract law.[707] Obviously the European Commission does not see indications for a market failure here.

In the framework of the same contract or in a second contract, the parties may specify the details of data access requests and the following use of the data *by the product user*. This contract may be concluded in the context of the sales, rental or lease agreement of the product or at a later stage, before or after a request based on Article 4 has been submitted to the data holder. The parties should have an interest to come to such an agreement, given the many difficult technical aspects of a data access, starting with the exact scope and format of the data concerned and the time of delivery or access and extending to possible safeguards to keep the data secret etc. However, even though there may be good reasons to come to an agreement, the product user should not be obliged to enter into such a contract. The access right of Article 4 is a non-contractual right by nature. The product user has the right to go to court or lodge a complaint with the public authority under Article 31 even without a contract. It would then be up to the court to define the details of the product user's access to data, a task that courts will handle in parallel to the FRAND requirement of Article 8.[708] This puts the product user in a strong

[707] Leistner/Antoine, IPR and the use of open data and data sharing initiatives by public and private actors (Evaluation of the proposed Data Act), Study for the European Parliament Committee on Legal Affairs (JURI), 2022, p. 93.

[708] See Picht, Caught in the Acts: Framing Mandatory Data Access Transactions under the Data Act, further EU Digital Regulation Acts, and Competition Law, Max Planck Institute for Innovation and Competition Research Paper No. 22-05, p. 27-29.

bargaining position for the negotiation of a contract. The data holder needs to conclude a contract in accordance with Article 4(6), at least if one does not follow the more restrictive approach taken here, and has an interest to fix the details of the data access under Article 4. By contrast, the product user has all options in his hands.

In light of the strong bargaining position of the product user, it seems appropriate to rely on the principle of freedom of contract with regard to those contracts. Still, there may be arguments to review standard clauses unilaterally imposed by the data holder. Mere end users of products will typically not put much weight on the modalities of a later possible access to machine data, e.g. consumers buying IoT devices or farmers leasing land machines. If the modalities of data access are not appreciated on the market as a valuable feature of the product, competitors may not compete over them ('lemon market').[709] In this regard, a review of standard terms may be justified as suggested by Article 13 of the Draft Data Act. By contrast, for major users of machines, e.g. airlines, one can expect that the collected machine data is of enough relevance for consideration on the market.[710] Businesses should be in a position to consider the relevant clauses on data access carefully or take the risk of unfavourable conditions. A review of standard terms is therefore not appropriate in this case.

The review of standard terms under Article 13 is of general application; it is not restricted to situations, where a product user can claim data access according to the provisions of Article 4 Draft Data Act but will also apply if the parties conclude a contract on a voluntary basis. The provision combines a blanket clause ("grossly deviates from good commercial practice in data access and use, contrary to good faith and fair dealing") with a black and a grey list of unfair terms. The lists contain terms which have apparently used the Unfair Terms Directive 93/13[711] as a blueprint, e.g. on contractual limits of the liability of the party that unilaterally imposed the term or the remedies of the other party in case of non-performance or breach of contract. Other provisions on the grey list are more specific for data access contracts, e.g. the presumption that a term is unfair that "allows the party that unilaterally imposed the term to access and use data in a manner that is significantly detrimental to the legitimate interests of the other contracting party". The grey list should be amended by a provision on deviations from the technical requirements for data access (see below).

c) Contracts with third parties based on Article 5

aa) Contract between data holder and third party

[709] On the justification of a review of standard terms based on the „lemon markets" problem see Basedow in MüKoBGB, 9. ed. 2019, Vor § 305 paras. 4-8.

[710] But see Drexl et al., Position Statement of the Max Planck Institute for Innovation and Competition of 25 May 2022 on the Commission's Proposal of 23 February 2022 for a Regulation on Harmonised Rules on Fair Access to and Use of Data (Data Act) (25.5.2022), https://ssrn.com/abstract=4136484 (last visited 4.7.2022), para. 125, which pleads for a review of standard terms in case of non-SME users.

[711] OJ 1994 L 95, 29.

Finally, the data holder may enter into an agreement with the third party who is using the data based on the product user's request. As in the relationship between the data holder and the product user, Article 5 does not oblige the third party to enter into an agreement with the data holder. Access to data may be grounded on the product user's simple request under Article 4. Still, it will often be in the best interest of the data holder and the third party to specify the details of data access, namely the exact scope and format of the data concerned, the time of delivery or access, safeguards to keep the data secret etc.

For those agreements, the Draft Data Act seems to provide two legal means for courts to intervene. However, at closer scrutiny none of the two seems appropriate if taken as an instrument to review a contract freely negotiated between the data holder and the third party.

According to Article 8(1), the data holder shall provide access under "fair, reasonable and non-discriminatory terms and in a transparent manner" (FRAND). Given the fact that the data holder is the only entity that can grant access to the specific product user's data in question, it seems necessary to protect the third party from unfair or discriminatory access conditions. Without such a requirement, the data holder could dictate the terms of access to a third party without any bargaining position. Still, the FRAND requirements of Article 8(1) do not allow courts to review the conditions of a contract that has been concluded by the parties. What the FRAND requirement means instead in this context, is discussed below in more detail.

Still the standard terms used in a contract between data holder and third party could be reviewed in accordance with Article 13. But it is questionable whether a market failure justifies such a review. For the third party the access right will be of central interest which avoids the 'lemon market' problem described above. Therefore, imbalanced access terms are not comparable to standard clauses which are not read by SME parties – which would be the scenario for a possible review under Article 13 – but rather an issue of the possible abuse of the exclusive technical position of the data holder against bigger and smaller third parties.[712] For this problem, the FRAND mechanism in Article 8(1) is better suited.

bb) Contract between user and third party

The relationship of users and third parties has been discussed above at 2(d).

d) Lack of model contract terms or default rules

The analysis so far has addressed mandatory provisions for contracts between data holders, product users and third parties. For the well-functioning of markets, it will be equally important to develop model contract terms which the parties may apply as blueprints for their contracts

[712] But see Picht, Caught in the Acts: Framing Mandatory Data Access Transactions under the Data Act, further EU Digital Regulation Acts, and Competition Law, Max Planck Institute for Innovation and Competition Research Paper No. 22-05, p. 38 et seq.

or, at least, as starting point for negotiations. Once the market has developed business practices, those practices may be further developed into (majoritarian) default rules to be applied by courts in case of incomplete contracts. Up to date, both model terms and default rules suitable for mandatory access rights are not sufficiently developed.

The Draft Data Act addresses the issue of a lack of model terms or defaults. Article 34 allocates the task to the European Commission to "develop and recommend non-binding model contractual terms on data access and use". The European Commission has already published a tender for the appointment of experts for this task. The development of such terms will not be trivial and will take some years given the fact that markets are just emerging.

The most advanced soft-law instrument for data access contracts already available are the 'ALI/ELI Draft Principles for a Data Economy'. The Principles are not specifically tailored for data access contracts based on mandatory access rights. Still they may be useful as a source of inspiration. Principle 20 ('Access or porting with regard to co-generated data') provides a list of circumstances of a possible legitimate use of co-generated data. Principle 21 ('Desistance from data activities with regard to co-generated data') describes possible restrictions in the use of such data based on the legitimate interests of the data holder. The circumstances listed may be the basis for defaults in data access contracts since they describe what co-generator may expect. Principle 7 ('Contracts for the transfer of data') and Principle 8 ('Contracts for simple access to data') provide sets of contract law principles for data transfer or data access contracts. Even though drafted for voluntary data contracts, these principles may still be useful for a further specification of data access agreements concluded on the basis of Article 4 or Article 5 Draft Data Act.

4. Access to data under FRAND conditions

According to Article 8 of the Draft Data Act, a data holder, where obliged to make data available to a data recipient under Article 5 or "under other Union law or national legislation implementing Union law," shall do so "under fair, reasonable and non-discriminatory terms and in a transparent manner". Given the broad language, Article 8 of the Draft Data Act may have impact also for access rights based on the DMA and on competition law. Even though Article 12(3) makes clear that the Draft Data Act's provisions shall only be applicable to legislation entering into force after the Draft Data Act, Recital 87 still invites to use the provisions as template for further amendments of the already existing rules. The so-called FRAND requirement is not novel to EU market regulation law. It has been used in Article 102 TFEU competition cases where a refusal to license intellectual property rights was found to constitute an abuse of dominance. This approach has been applied to copyright in databases[713] and software[714] and more recently – with a broad legal practice and academic debate – with regard

[713] Case C-418/01, *IMS Health*, ECLI:EU:C:2004:257.

[714] Case T-201/04, *Microsoft*, ECLI:EU:T:2007:289.

to standard essential patents (SEPs) in the telecommunications market.[715] A simplified FRAND test is also applied in sector specific regulations.[716] Even though Article 8 is apparently drafted against this backdrop, experience from the older FRAND licensing schemes should only be used with some caution.

a) Addressees of the FRAND requirement

Article 8 seems to suggest that, within the framework of the Draft Data Act, only third parties that are granted data access under Article 5 should benefit from the FRAND requirement. However, such an interpretation would draw the circle of eligible addressees too narrow. If product users request data access under Article 4 Draft Data Act, courts will have to define the terms of such access as well. According to Article 4(1), access to data has to 'be free of charge'. But free of charge does not mean that the data holder may push through access conditions of an unfair, unreasonable or discriminatory nature. Therefore, the reference to Article 5 in Article 8 should be broadened and also encompass Article 4.[717] If the wording remains as it is, the proviso "or under other Union law" would have to serve as basis for including product users into the FRAND regime of Article 8.

b) What data is licensed under FRAND requirements?

Licensing of SEPs on FRAND terms may appear to be straightforward with regard to the licensed subject matter, which is a clearly defined registered right. However, the practical experience turned out to be different and raised complicated issues since patent holders, when asked for a non-discriminatory patent license, replied that they would only be willing to grant licenses for a given patent portfolio and on a worldwide basis whereas the potential licensees would only ask for a license for a specific patent for a specific state or region and therefore ask for a lower license fee.[718] Questions of this kind should not come up with regard to data accessed on the basis of a specific user request under Articles 4 and 5 of the Draft Data Act. Still, there may be issues with regard to the specific structure and format of the data and the technical means of access. These technical requirements should be further specified in Article 4, as explained below. Access based on FRAND terms in accordance with Article 8 Draft Data Act would then have to confirm and apply these technical specifications and requirements.

c) Who determines FRAND requirements?

---

[715] Case C-170/13, *Huawei*, ECLI:EU:C:2015:477.

[716] See e.g. Article 61 Regulation (EU) 2018/858 on the approval and market surveillance of motor vehicles, OJ 2018 L 151, 1.

[717] Picht, Caught in the Acts: Framing Mandatory Data Access Transactions under the Data Act, further EU Digital Regulation Acts, and Competition Law, Max Planck Institute for Innovation and Competition Research Paper No. 22-05, p. 27-28.

[718] See for the discussion of this issue Hauck/Kamlah GRUR Int. 2016, 420 (423-425).

The question of who should determine FRAND requirements and in what procedural setting is the subject of a broad debate with regard to SEPs. Yet, not all of the issues discussed with regard to SEPs are topical when it comes to data access. Potential licensees of SEPs are typically not depending on the patent holder's technical cooperation for the use of the protected standard. Usually, they know the technology from the standard setting organisation or from elsewhere and are merely in need for a license to use it. Therefore, in a typical procedural setting, it is not the potential licensee but the patent holder who initiates proceedings and sues the potential licensee for patent infringement.[719] In the framework of these proceedings, the patent holder is then confronted with the defence argument that an injunction should not be granted because of the patent holder's obligation to grant a FRAND license for the use of the SEP. This defence is the basis for the courts assessment of whether the license terms offered by the patent holder comply with the FRAND requirements. Actions of potential licensees with the aim to force holders of SEPs into FRAND license agreements have not been reported so far, at least in Germany.[720]

One can expect that court proceedings on data access claims under Article 4 or 5 of the Draft Data Act will follow a different pattern. In this setting, the user or the third party has no access to the data in question but depends on the data holder's technical cooperation. Therefore, one should rather expect the product user or third party on the claimant's side of a court case and the data holder on the defendant's bench. Such a scenario, though different from the typical SEP case, is not new in the case law on Article 102 TFEU. It resembles the setting in the *Microsoft* case where the General Court confirmed a decision by the European Commission which obliged Microsoft to make interoperability information available to other undertakings having an interest in developing and distributing work group server products and to provide such information on the basis of FRAND terms.[721] A similar setting could occur if, as provided for in Article 31 Draft Data Act, public authorities of Member States would enforce the access rights of Articles 4 and 5 and the data holder would then lodge a complaint at the competent courts. In addition, users or third parties could bring suits before the regular courts which would then have to decide directly on the existence of an access right and on the applicable FRAND conditions under which the data holder would have to grant access. It can be expected that public authorities or courts would not have to be very creative in the drafting of such FRAND conditions since both the data holder and the product user or third party would arguably suggest such conditions in their pleadings. It would then be up to the public authority or court to decide which of the suggested terms complies with the requirements of the FRAND test.

[719] See also Drexl et al., Position Statement of the Max Planck Institute for Innovation and Competition of 25 May 2022 on the Commission's Proposal of 23 February 2022 for a Regulation on Harmonised Rules on Fair Access to and Use of Data (Data Act) (25.5.2022), https://ssrn.com/abstract=4136484 (last visited 4.7.2022), para. 102.

[720] Walz/Benz/Pichelmayer GRUR 2022, 446 (447).

[721] Case T-201/04, *Microsoft*, ECLI:EU:T:2007:289, at para. 48.

The handling of SEP patent license cases by regular courts has been criticised in the legal literature. Courts may indeed not be best suited to negotiate contract terms with parties.[722] Also, one may have doubts whether an infringement procedure on a specific patent allows the court and the parties to come to a decision on FRAND terms for broader international patent portfolios.[723] Therefore, it has been suggested to advice parties to refer their disputes to arbitration[724] or to prescribe a mandatory dispute settlement procedure before the parties can bring their case before a court.[725] It may indeed be assumed that such alternative dispute resolution bodies may be better equipped to gear the parties into constructive contract negotiations. They are not bound by the tight corset of civil procedural rules, may be chosen by the parties and may therefore have special expertise in the area. Article 11 of the Draft Data Act takes up these ideas and provides that data holders and data recipients shall have access to certified dispute settlement bodies. The availability of such a dispute settlement mechanism is mandatory according to Article 12(2). However, such settlement procedure does not affect the right of the parties to seek an effective remedy before a court or tribunal of a Member State, see Article 10(9). It may therefore still occur that a party directly enters the courtroom.

d) Royalties

The Draft Data Act offers no guidance as to how royalties for FRAND licenses based on Article 8(1) should be determined. Here, experience from the SEP patent cases may be helpful. Different approaches for the determination of FRAND royalties have been developed. For data access licenses, the so called 'comparable licenses approach' may often be appropriate where previous licenses in the given market are used as starting point before the relevant differences between the previous transactions and the license at issue are taken into account.[726] It presupposes that a prior licensing practice under somewhat comparable conditions exist. In addition, other criteria such as data generation responsibility, refinement status, and business model-relevance may be considered.

e) Relationship of FRAND requirements and review of (standard) contract terms

What remains to be clarified is the relationship of a contract concluded between the data holder and the third party and the FRAND requirements of Article 8(1). The FRAND requirements of Article 8(1) are designed as a yardstick for public authorities, courts or dispute settlement

[722] See from the abundant literature Picht GRUR 2019, 11; Schaefer/Czychowski GRUR 2018, 582; Walz/Benz/Pichelmayer GRUR 2022, 446 (448).

[723] Hauck/Kamlah GRUR Int. 2016, 420 (423-425).

[724] Picht GRUR 2019, 11 (24-25).

[725] Walz/Benz/Pichelmayer GRUR 2022, 513.

[726] Picht, Caught in the Acts: Framing Mandatory Data Access Transactions under the Data Act, further EU Digital Regulation Acts, and Competition Law, Max Planck Institute for Innovation and Competition Research Paper No. 22-05, p. 31-33. See also Nestler/Ordosch GRUR-Prax 2012, 372 (373).

bodies which have to decide about a claim for access.[727] They are not meant as a standard of review for contracts concluded between the parties.[728] One should not allow the third party to set aside a contract with the argument that its terms are not fair and reasonable or discriminate between third parties. Otherwise, a review would result that would apply both to standard terms and individually negotiated contract and as such be more far-reaching than the review foreseen under Article 13. It should be borne in mind that the third party is under no obligation to conclude a contract with the data holder. Also, the European Commission has not presented any evidence for a systemic structural imbalance of power or other market failure between data holders and third parties that would justify such a far-reaching review across the board. Rather, it seems appropriate to leave the parties with the two possible, but independent ways to specify the conditions of data access: Firstly, the parties can come to an agreement, whereby the third party may use Article 8(1) as a bargaining chip. The agreement may also be reached as part of a settlement in proceedings. Such contracts should then be respected and not reviewed. As explained above, the legislature should also refrain from introducing a control of standard terms under Article 13 for this case. Secondly, the parties may not agree on a contract. In this case, the third party may initiate proceedings before public authorities, courts or dispute settlement bodies and apply for access on FRAND terms. Admittedly, a third party who wants to offer services for which it depends on user data may be under pressure to rather conclude an unfavourable contract than to wait for a public authority or court to issue a FRAND decision. But in this regard, procedural means, like preliminary measures, are the tool of choice to protect the third party. A generalised substantive review of contracts between businesses, including individually negotiated terms, would be overly intrusive. If, on the other hand, an imbalance of power exists, due to a position of dominance of the data holder or a dependence of the third party on the data holder, competition law – including § 20(1a) GWB – remain applicable and would provide the substantive standard to be applied to the contractual conditions. General civil law doctrines like ordre public or ‘gute Sitten’, e.g. § 138 BGB, may be invoked as last resort.

5. Technical requirements of data access

The Draft Data Act does not specify how data access rights are to be made operational technically. Article 3(1) obliges the manufacturer – who need not be the later data holder – to design products and related services in such a manner that data generated by their use are, by default, easily, securely and, where relevant and appropriate, directly accessible to the product user. But the provision does not specify any technical requirements to be respected by data holders which are under an obligation to grant access under Articles 4 and 5. The same holds true for the information duties in Article 3(2) which address the purchase, sale or lease contract for the product.

[727] See also Drexl et al., Position Statement of the Max Planck Institute for Innovation and Competition of 25 May 2022 on the Commission's Proposal of 23 February 2022 for a Regulation on Harmonised Rules on Fair Access to and Use of Data (Data Act) (25.5.2022), https://ssrn.com/abstract=4136484 (last visited 4.7.2022), para. 101.

[728] This is also expressed at the end of Recital 38 Draft Data Act: “Voluntary data sharing remains unaffected by these rules.”

Another provision of relevance in this regard is Article 11 which allows the data holder "to apply appropriate technical protection measures, including smart contracts, to prevent unauthorised access to the data and to ensure compliance with Articles 5, 6, 9 and 10, as well as with the agreed contractual terms for making data available." The provision permits technical restrictions regarding the access and use of the data, but it does not further specify the technical requirements necessary to enable a legally compliant access and use in accordance with Articles 4 and 5.

This gap is even more striking in light of the detailed provision on the technical requirements for interoperability in Article 28. Article 28 applies to operators of data spaces, but it does not apply to data holders under an obligation to grant access under Articles 4 and 5. The legislature should reconsider whether the technical requirements of Article 28, which address important points, should be generalised such as to make them suitable also for data access requests, or whether a similar but independent provision should be introduced in Chapter III for that purpose.

A provision on the 'technicalities' of access requests should include the technical requirements which are essential to facilitate access and a further use of the data. It should include the following aspects:

- the data shall not be compressed, reduced or otherwise altered, if not explicitly requested by the data user or third party; data held in different qualities or resolutions shall be provided in the highest available quality or resolution, if not explicitly requested otherwise by the product user or third party;
- the data shall contain all metadata that is present in its original unaltered form;
- the data set content, data collection methodology and data quality shall be sufficiently described to allow the recipient to find, access and use the data;
- the data structures, data formats, vocabularies, classification schemes, taxonomies and code lists shall comply with technical standards and shall be described in a publicly available and consistent manner;
- the technical means to access the data, such as application programming interfaces, and their terms of use and quality of service shall be sufficiently described to enable automatic access and transmission of data between parties, including continuously or in real-time in a machine-readable format;
- access to the data set shall normally not be restricted to an 'in situ'-use on the server or other technical infrastructure of the data holder. The data holder may permit an 'in situ'-use,[729] but it shall not normally technically restrict access to usages on its own servers or infrastructures.[730] A restriction of access to an 'in situ'-use would need to be specifically justified by the data holder. Technical protection measures used for preventing 'ex situ'-use shall not be covered by Article 11.

[729] Recital 21 Draft Data Act.

[730] See Kerber, Governance of IoT Data: Why the EU Data Act will not fulfill its objectives (8.4.2022), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4080436 (last visited 4.6.2022), p. 8-9, 15-16.

The legislator should either adopt a detailed provision which specifies the technical requirements for data access requests or use a more general wording following the example of Article 20 GDPR ("structured, commonly used and machine-readable format") and authorise the Commission, as in Article 28(2), to adopt delegated acts to supplement the Draft Data Act by further specifying the requirements.

Deviations from the technical requirements by contract should be possible in principle. However, deviations in contractual terms unilaterally imposed on a micro, small or medium-sized enterprise, should be reviewed in accordance with Article 13 Draft Data Act. Given the importance of the technical feasibility of data access, the legislature should consider dedicating a new provision to such deviations in the "grey list" of Article 13(3).

6. Database rights, trade secrets, personal data

a) Database rights

As shown above, sets of machine-generated data may be protected by 'sui generis' database rights. However, it is unclear which data collections meet the requirements of Directive 96/9. Also, the allocation of rights in case of co-generation of data is not clearly defined. 'Sui generis' rights are a source of legal uncertainties and may increase the risk for hold-ups. At the same time, protection with the 'sui generis' right seems unnecessary since the incentives to collect data are strong enough even without such rights. Article 35 Draft Data Act addresses this problem, but the current drafting raises several questions to be clarified in the legislative procedure.

According to Article 35, second half sentence, "the sui generis right provided for in Article 7 of Directive 96/9/EC does not apply to databases containing data obtained from or generated by the use of a product or a related service." This proviso seems to exclude sets of machine-generated data altogether from the protection under Article 7 of Directive 96/9/EC, irrespective of whether the data is subject to an access request under the Draft Data Act or not. Simultaneously, Article 35, first half sentence, may be read to imply that only access requests under the Draft Data Act should be privileged ("In order not to hinder the exercise of the right of users to access and use such data in accordance with Article 4 of this Regulation or of the right to share such data with third parties in accordance with Article 5 of this Regulation…"). This would mean that the 'sui generis' right could still be used to deny requests for access to machine generated data if they are based on other legal grounds, e.g. competition law or sector-specific rules. In light of the further explication given at the end of Recital 84, the first interpretation seems to be more convincing: "… this Regulation should clarify that the sui generis right does not apply to such databases as the requirements for protection would not be fulfilled." Obviously, the drafters wanted to exclude those datasets more generally from the 'sui generis' right. Such an approach seems preferable given that the arguments for a limitation of the 'sui generis' rights are the same when access is requested on competition law grounds or

sector specific regulation.[731] This should even apply if such access rights are based on provisions that have entered into force before the Draft Data Act, since Article 12(3) does not apply in this regard.[732]

Also, either Article 35 or a recital should further specify which datasets are covered. It should not suffice for the exclusion to be triggered that a data set 'contains' machine-generated data. Otherwise, Article 35 would amount to an indirect abrogation of the 'sui generis' right. Rather, Article 35 should be confined to datasets that comprise machine-generated data only or predominantly, with no substantial other data included and no further investments and efforts in the obtaining, verification or presentation of the data being made.[733]

Finally, Article 35 or a recital should clarify that Member States are precluded from the creation of national protection regimes that could replace the 'sui generis' right. The exclusion under Article 35 should not be understood as opening room for manoeuvre for Member States, especially for claims based on unfair competition.[734]

b) Trade secrets

Sets of machine-generated data covered by the access rights of Article 4(1) and Article 5(1) Draft Data Act may be protected as trade secrets under the provisions of the Trade Secret Directive 2016/943/EU and the implementing provisions in the German Trade Secret Act (GeschGehG). This has been analysed in more detail in Part E of this study. Granting access to product users and third parties in accordance with the Draft Data Act comes with a risk for the data holder that the secrecy of the dataset may get lost. As a consequence, the relevant information contained in the dataset will no longer meet the requirements of a trade 'secret' and can be shared freely. The reactions of industry association to the Draft Data Act show that

[731] See also Leistner/Antoine, IPR and the use of open data and data sharing initiatives by public and private actors (Evaluation of the proposed Data Act), Study for the European Parliament Committee on Legal Affairs (JURI), 2022, p. 120.

[732] But see Drexl et al., Position Statement of the Max Planck Institute for Innovation and Competition of 25 May 2022 on the Commission's Proposal of 23 February 2022 for a Regulation on Harmonised Rules on Fair Access to and Use of Data (Data Act) (25.5.2022), https://ssrn.com/abstract=4136484 (last visited 4.7.2022), para. 264.

[733] Cf. Leistner/Antoine, IPR and the use of open data and data sharing initiatives by public and private actors (Evaluation of the proposed Data Act), Study for the European Parliament Committee on Legal Affairs (JURI), 2022, p. 119. See also European Commission, Study to Support an Impact Assessment for the Review of the Database Directive, Final Report, 2022, p. 66-67. For a broad exclusion Drexl et al., Position Statement of the Max Planck Institute for Innovation and Competition of 25 May 2022 on the Commission's Proposal of 23 February 2022 for a Regulation on Harmonised Rules on Fair Access to and Use of Data (Data Act) (25.5.2022), https://ssrn.com/abstract=4136484 (last visited 4.7.2022), para. 261.

[734] See Opinion of the European Copyright Society on selected aspects of the proposed Data Act (12.5.2022), https://europeancopyrightsocietydotorg.files.wordpress.com/2022/05/opinion-of-the-ecs-on-selected-aspects-of-the-data-act-1.pdf (last visited 4.7.2022); Husovec/Derclaye, Why the Sui Generis Database Clause in the Data Act Is Counter-Productive and How to Improve It? (8 March 2022), https://ssrn.com/abstract=4052390 (last visited 4.7.2022); Leistner/Antoine, IPR and the use of open data and data sharing initiatives by public and private actors (Evaluation of the proposed Data Act), Study for the European Parliament Committee on Legal Affairs (JURI), 2022, p. 120.

businesses worry about the potential risks for their trade secrets.[735] However, it is also clear that trade secret protection cannot shield data holders from access requests without undermining the main purpose of the Draft Data Act, which is to open data silos.

The Draft Data Act tries to balance the interests by a twofold approach. Articles 4(3) and 5(8) provide limitations to the data holder's trade secrets; in principle, trade secrets cannot be invoked to deny access requests under Articles 4(1) and 5(1). But the limitations of Articles 4(3) and 5(8) are limited in scope and subject to safeguards in the interest of the data holders. Trade secrets shall only be disclosed provided that all "specific necessary measures are taken to preserve the confidentiality of trade secrets in particular with respect to third parties". If the measures are not taken, any use or disclosure will be regarded as unlawful under Article 4(3) Trade Secrets Directive. The necessary measures can be specified in contracts between data holders and product users or, in case of Article 5(8), between data holders and third parties. In addition, the data holder is allowed to apply "appropriate technical protection measures" in accordance with Article 11.

The general approach taken by the Draft Data Act deserves support.[736] However, one should not expect that the provisions will immediately deliver legal certainty to the parties.[737] Courts will have to clarify the rights and duties of the parties involved in the years to come. It will not be trivial for data holders, product users and third parties to determine whether a given dataset qualifies as a trade secret. Parties may have different opinions about this qualification. Also, product users and third parties may face difficulties to determine the 'necessary measures' to be taken to preserve confidentiality. One obvious measure will be to conclude agreements with all third parties obliging them to keep secret information confidential. But it is not clear whether the conclusion of such agreements will suffice and what exactly they should look like.[738] Articles 4(3) and 5(8) suggest, that the data holder and the product user (or the third party) agree on these necessary measures. But the parties may have different understandings of what is necessary.[739] Additional uncertainties will arise in the three-partite scenario of Article 5(8). According to Article 5(8), disclosing a trade secret to a third party is required only if the information is "strictly necessary to fulfil the purpose agreed between a user and a third party". However, this limitation depends on an agreement to which the data holder is not a party.[740]

---

[735] See the position paper of BDI, p. 13 and VDMA, p.3., available at https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13045-Data-Act-amended-rules-on-the-legal-protection-of-databases/feedback_en?p_id=29086590 (last visited 4.7.2022).

[736] See also Leistner/Antoine, IPR and the use of open data and data sharing initiatives by public and private actors (Evaluation of the proposed Data Act), Study for the European Parliament Committee on Legal Affairs (JURI), 2022, p. 87.

[737] Also critical in this regard Drexl et al., Position Statement of the Max Planck Institute for Innovation and Competition of 25 May 2022 on the Commission's Proposal of 23 February 2022 for a Regulation on Harmonised Rules on Fair Access to and Use of Data (Data Act) (25.5.2022), https://ssrn.com/abstract=4136484 (last visited 4.7.2022), paras. 279-281.

[738] Bomhard/Merkle RDi 2022, 168 (171).

[739] Weizenbaum Institute for the Networked Society, Position paper regarding Data Act (11.5.2022), p. 12.

[740] Id., p. 13; Bomhard/Merkle, RDi 2022, 168 (172).

Finally, it is not clear which technical protection measures will be considered 'appropriate' under Article 11 and which measures will be found to be overly strict and excessive.

Despite these uncertainties, Articles 4(3) and 5(8) may pave the way for a balanced approach once these open questions are solved. Article 8(6), by contrast, should rather be deleted.[741] According to Article 8(6), an obligation to make data available to a data recipient shall not oblige the disclosure of trade secrets within the meaning of Directive (EU) 2016/943, "unless otherwise provided by Union law, including Article 6 of this Regulation, or by national legislation implementing Union law". This raises more questions than it may answer. Not only is the reference to Article 6 unclear. In more general terms, it is questionable if the provision will have any effect, given that it does not create an additional layer of protection for trade secrets, nor does it set out additional limitations.

c) Processing of personal data under the Draft Data Act

The Draft Data Act is based on the premise that much of the addressed machine-generated data will not qualify as personal data in the sense of Article 4(1) GDPR.[742] However, this assertion may be questioned in light of the strict standards of interpretation developed by the CJEU in its *Breyer* decision[743] and followed also by the European and national data supervisors. For much of the data covered by the Draft Data Act, data subjects will be identifiable for the data holder, the product user and/or the third party, at least if the data can be combined with other data, e.g. data of passengers or crew of aircrafts, drivers of vehicles, employees, or individuals in households where IoT products are used. This may lead to a legal responsibility as joint controller under Article 26 GDPR for product users, third parties and data holders, even if they cannot identify the individuals without the data held by the other parties, but only pass on machine-generated data.

The Draft Data Act does not provide a legal basis for the processing of data. Instead, it refers, in Article 1(3), to the GDPR which shall not be affect by the Draft Data Act. Data holders, product users and third parties therefore will have to justify their use of personal data under the existing legal framework of the GDPR. One can imagine scenarios where product users only request access to their own personal data and authorise a third party to use these data; in this case, consent may be used as legal ground if the requirements of Article 6(1)(a) are met. But of the product 'user' will not always be identical with the data subject.[744] Instead, business users and third parties will be interested in data which may either identify individuals as such or

[741] Drexl et al., Position Statement of the Max Planck Institute for Innovation and Competition of 25 May 2022 on the Commission's Proposal of 23 February 2022 for a Regulation on Harmonised Rules on Fair Access to and Use of Data (Data Act) (25.5.2022), https://ssrn.com/abstract=4136484 (last visited 4.7.2022), para. 284.

[742] COM SWD(2022) 34 final, 1.

[743] Case C-582/14, *Breyer*, ECLI:EU:C:2016:779.

[744] Drexl et al., Position Statement of the Max Planck Institute for Innovation and Competition of 25 May 2022 on the Commission's Proposal of 23 February 2022 for a Regulation on Harmonised Rules on Fair Access to and Use of Data (Data Act) (25.5.2022), https://ssrn.com/abstract=4136484 (last visited 4.7.2022), para. 306.

which can be linked to other data and then be used to identify customers, employees or other individuals – like, for example, if the car rental service requests vehicle data from the manufacturer or the airline requests flight data from the aircraft producers. In these scenarios, the processing of data will only be justified if one of the legal grounds of Article 6 GDPR applies. Either all data subjects have given their consent to the processing, Article 6(1)(a), or one of the other grounds for lawful processing in Article 6(1)(b)-(f) is fulfilled, especially if the data processing is necessary for purposes of the legitimate interests pursued by the controller or by a third party. Such a right clearance may be burdensome if not impossible in scenarios with many data subjects.

As a result, data holders might be trapped in situations where a request for data access under Article 4 cannot be processed without a possible violation of the requirements of the GDPR.[745] Since Article 1(3) Draft Data Act gives priority to the GDPR, such a denial of access would most likely be justified and would not lead to fines or other enforcement measures under the Draft Data Act. Data holders have a legitimate interest to act carefully and to take all necessary measures to comply with the GDPR. But data holders may also use the argument of GDPR-compliance strategically to block access requests. Given that the assessment of possible GDPR violations is highly uncertain and that data holders have no genuine interest to share data, it will be a natural choice to act risk-averse.

In light of this tension, Leistner/Antoine suggest to amend the Draft Data Act and to recognise Articles 4(1) and 5(1) Draft Data Act as relevant obligations of Union law, to which the data holder is subject, and which should thus be a legitimate ground for lawful data processing according to Article 6(1)(c) GDPR. For sensitive data, Article 9 GDPR would still prevail and require the consent of the data subject.[746] Such a solution would have the advantage of providing a relatively clear-cut solution, but it would imply that large amounts of potentially identifiable data would be dispersed among product users and third parties, with all the associated risks. As the authors admit, such a solution is "properly difficult to agree upon politically".[747]

A pragmatic way out of the dilemma could be to clarify the requirements of anonymisation of datasets and to oblige data holders, product users and third parties to use all available and economically reasonable means to anonymise data sets before they are shared, especially if the consent of the data subjects cannot be obtained.[748] Data requests should not be rejected with the argument of privacy if anonymisation is possible. Such anonymisation efforts should not only be encouraged with regard to datasets which immediately allow the identification of

[745] Bomhard/Merkle RDi 2022, 168 (172).

[746] Leistner/Antoine, IPR and the use of open data and data sharing initiatives by public and private actors (Evaluation of the proposed Data Act), Study for the European Parliament Committee on Legal Affairs (JURI), 2022, p. 91.

[747] Id., 92.

[748] See also Drexl et al., Position Statement of the Max Planck Institute for Innovation and Competition of 25 May 2022 on the Commission's Proposal of 23 February 2022 for a Regulation on Harmonised Rules on Fair Access to and Use of Data (Data Act) (25.5.2022), https://ssrn.com/abstract=4136484 (last visited 4.7.2022), para. 307.

individuals, but also for those which allow for an identification only after a combination with other data held by the product user or by the third party. Anonymisation of data requires that neither the data holder, e.g. the manufacturer of a vehicle, nor the product user under Article 4(1) Draft Data Act, e.g. the car rental service, can identify individual costumers. However, based on the risk-based approach, reasonable anonymisation efforts should be taken into account when the legitimate interests of the data holder, product user and third party are assessed in accordance with Article 6(1)(f) GDPR.[749] A clarification of these requirements in the Draft Data Act would mitigate the risks for privacy and, at the same time, increase the number of successful data access requests under Articles 4(1) and 5(1). The Draft Data Act should also clarify who has to bear the costs of anonymisation. If the parties cooperate and conclude agreements, they can negotiate the allocation of costs. If they do not come to an agreement, and the data request is enforced by public authorities or courts, the data holder can take that the costs of anonymisation into account as part of the compensation under Article 9.

7. Interoperability and switching

The Draft Data Act intends to enable interoperability for data sharing across sectors, which are not within the scope of a specific European data space, through essential requirements set out in Article 28 (see also Recitals 79, 86). While the development of such an interoperability regime is of great importance, we do not dive into the technicalities of this regime here.

8. Enforcement

The legal nature of the data access right is not just of academic interest, but has consequences for legal practice, especially for the enforcement of data access claims. Article 31 Draft Data Act obliges EU Member States to designate one or more competent authorities as responsible for the application and enforcement of the regulation. These authorities are competent to handle complaints arising from alleged violations of the Draft Data Act, conduct investigations into matters that concern the application of the Draft Data Act and impose fines in cases of violations. In addition, data holders and data recipients shall have access to dispute settlement bodies in accordance with Article 10.

The Draft Data Act neither provides nor excludes private enforcement actions brought before national courts.[750] This raises the question if private enforcement can complement the administrative enforcement of the Draft Data Act and, if yes, what kind of private enforcement actions will be available. Obviously, both the product user and the data holder may invoke remedies for breach of contract if the other party fails to comply with conditions laid down in the data access contract concluded on the basis of the data access right; such remedies are indirectly recognised by the provisions on unfair terms in Article 13 which emphasise that an exclusion of remedies may be subject to review.

[749] Id., para. 307.

[750] See Article 10(9) Draft Data Act.

What is less clear is whether a product user can request data access directly from the data holder and, in case of denial, bring an action before the regular civil courts. While Article 4 is drafted as an individual right of the product user against the data holder, the Draft Data Act does not specify whether such claims may be enforced by the Member States' courts. This may be attractive for users if, e.g., the Member States' courts would issue effective preliminary measures. The Draft Data Act should clarify that private enforcement by the product user is permitted. Moreover, it should specify whether competitors (e.g. other manufacturers of IoT products) can bring claims against data holders or manufacturers who do not comply with their obligations under the Draft Data Act. Under German law, such claims of competitors – as well as cease and desist letters paid for by the data holder – could be justified on the basis of the Act against Unfair Competition (UWG), § 3a ('Breach of law') if not excluded by the Draft Data Act.

9. The role of data intermediaries

The Draft Data Act does not make use of the opportunity to specify which role data intermediaries could have in the context of the new regime. For further discussion of the potential role of data intermediaries, we point to part F(IV) of this study.

II. Competition policy

1. The application of Article 101 TFFU/§ 1 GWB to data sharing and pooling arrangements

a) Greater legal clarity for data cooperations: Guidelines/a new Block Exemption Regulation for data access and data sharing?

As pertinent surveys have consistently shown (see part D(III)), the absence of legal certainty regarding the legality of voluntary data sharing arrangements can be a relevant disincentive for market participants to engage in data cooperations. Simultaneously, a growing number of rules mandates data access and sharing. Both trends argue for the identification of clear legal principles on when and under which conditions data sharing is in line with Article 101 TFEU/§ 1 GWB.

However, creating legal certainty in this field is not an easy task. The competition law on information exchange has always been complex and highly context-sensitive. Many grey zones remain. When these rules are applied to data access and sharing agreements, the complexities multiply.[751] As discussed above, much will depend on the type of data that are shared, with pricing data marking one extreme, and pure machine-sensor-data possibly another extreme; on the level of individualisation or aggregation of the data shared; on how data sharing is organised

[751] For the complexities of the assessment see Schallbruch/Schweitzer/Wambach, Ein neuer Wettbewerbsrahmen für die Digitalwirtschaft, Bericht der Kommission Wettbewerbsrecht 4.0, 2019, p. 59 et seq.

– as in situ access on the servers of the original data holder, with the full dataset being passed on to a competitor, or with the involvement of a data intermediary; and on many additional aspects of the precise data governance regime. In its Draft Horizontal Guidelines (2022), the European Commission has tried to summarise the relevant criteria.[752] A complex and context-sensitive assessment will frequently remain necessary. This will be true, in particular, as data access and sharing agreements emerge which no longer limit the use of the data to a specific sector – as they currently mostly do. Where data are used across sector boundaries, such sharing may have different competitive effects in different markets and settings[753] – a fact which will further add to the complexity of the assessment.

Hence, the prospects for finding rules on data sharing agreements that are both general, clear and easy to apply to the broad variety of possible data sharing agreements are rather slim. This is true all the more as the experience with data access and sharing agreements is still at an early stage. The pool of relevant competition law cases is small. While it is true that data access and sharing arrangements may come with a significant pro-competitive and innovative potential, they also come with real risks to competition. The public encouragement of data sharing notwithstanding, competition authorities are well advised not to give it a 'free pass' at a time, where data sharing arrangements are in the process of being formed. Rather, competition law and competition authorities should make sure that the emerging arrangements are in line with competition law standards.

There are, therefore, good reasons to caution against a sweeping privilege for data access and sharing agreements. A number of authors has argued in favour of the passing of a tailored Block Exemption Regulation (BER) for data access and sharing agreements, however.[754]

The advisability of such a project depends on whether criteria can be identified that justify the granting of a safe harbour for a relevant category of data access and sharing agreements. It is doubtful whether the practice of data access and sharing agreements in the market is already sufficiently consolidated. Also, the more data access and sharing agreements become cross-sectorial, the less it may make sense to rely on market share thresholds for constraining the scope of the safe harbour. Different limiting principles may need to be developed. For the time being, sector-specific rules and specifications for data access and sharing agreements may be more useful than a broad 'Data-BER'.[755] Cross-sectorial data access and sharing agreements may continue to require a case-by-case analysis.

[752] C(2022) 1159 final, paras. 423 et seq.

[753] Examples in Lundqvist EuCML 2018, 146 (149).

[754] See, in particular, Podszun, Handwerk in der digitalen Ökonomie, 2021, p. 187; Podszun, Empfiehlt sich eine stärkere Regulierung von Online-Plattformen und anderen Digitalunternehmen? Gutachten F zum 73. Deutschen Juristentag, Hamburg 2020/Bonn 2022, F-91 – F-94.

[755] For a similar conclusion see Picht, Caught in the Acts: Framing Mandatory Data Access Transactions under the Data Act, further EU Digital Regulation Acts, and Competition Law, Max Planck Institute for Innovation and Competition Research Paper No. 22-05, p. 16.

In order to contribute to the emergence of a coherent framework, it is nonetheless useful to search for some general principles.[756] Some have suggested that they may follow from an analogy between 'data pools' and patent pools, such that the TT-Guidelines[757] could provide a useful starting point.[758] However, data pools and patent pools arguably have different functions: patent pools are defined by reference to a specific technology and function as a device for collecting royalties in this context. Data pools may be a mechanism for accumulating a database that allows for a more targeted interaction between certain market actors. Or they may function as a 'data lake' that may be used as a base to run data analytics for a broad variety of purposes.[759] In addition, data pools may – and possibly will typically – collect relatively unorganised data that is not covered by intellectual property rights. Frequently, parts of the data pooled may not be unique, but available elsewhere, too.[760] Some of the categories that are relevant for evaluating the competitive effects of patent pools – namely the distinction between substitutable/non-substitutable patents[761] and essential/non-essential patents[762] – will be notoriously difficult to apply to data, at least when observed data is being pooled.[763] Nor is it obvious that only such data should be allowed to be included in the pool which is 'essential' for its objective.[764] The broader the purpose of the data pool, the less useful such a criterion may be. Nonetheless, some of the general principles developed in the context of patent pools may also proof useful for data pools. Most obviously, this is the case for those rules that are meant to prevent foreclosure effects where the pool represents a significant share of the market and the data pooled affects the ability to compete. In such cases, the pool must grant fair, transparent and non-discriminatory access to all third parties who request access, as is already mentioned in the European Commission's Draft Horizontal Guidelines (see above, part E(III)(1)(b)). In such settings, the pool must also make sure that the data formats, standards for data transfer and data storage do not become a barrier for access to the relevant data. Beyond this most fundamental principle, a requirement that pool members should be allowed to license their data individually outside the pool[765] may be an important pro-competitive safeguard. Picht has plausibly suggested an analogous application of Article 5(1)(a) TT-BER[766] which restricts exclusive cross-licensing or assignment obligations regarding the data recipient's follow-on innovations.[767] It is less clear whether a requirement that any party to the pool should be allowed

[756] For such an endeavour see Id., p. 12 et seq.

[757] OJ 2014 C 89, 3; See in particular on patent pools, paras. 244 et seq.

[758] Lundqvist EuCML 2018, 146 (152).

[759] Lundqvist EuCML 2018, 146 (151).

[760] Id., 149.

[761] OJ 2014 C 89, 3 para. 251.

[762] Id., para. 252.

[763] Crémer/de Montjoye/Schweitzer, Competition Policy for the digital era, Final report, 2019, p. 96.

[764] This is proposed as a criterion for a 'safe harbour' for data pools by Lundqvist EuCML 2018, 146 (153 et seq.).

[765] For this proposition see Lundqvist EuCML 2018, 146 (153 et seq.).

[766] OJ 2014 L 93, 17.

[767] See Picht, Caught in the Acts: Framing Mandatory Data Access Transactions under the Data Act, further EU Digital Regulation Acts, and Competition Law, Max Planck Institute for Innovation and Competition Research Paper No. 22-05, p. 15.

to exit the pool, with his or her essential dataset, at any given point in time,[768] is useful with a view to protecting competition in all circumstances.

A field to be further explored is the role of restrictions on data use for the competitive assessment of data collaborations. Such restrictions on data use can be an important element of a data collaboration – at times a legally necessary one, to ensure conformity with the GDPR, with the competition law principles for the legality of information exchanges or with the law on trade secrets. Other restrictions on data use may raise the risk of anti-competitive effects and limit the innovative potential of data access and data sharing.[769] We suggest that, for the time being, the effects and possible justifications of data use restrictions must be analysed case-by-case.

b) The contribution of data governance rules on the legality of data sharing

In the search for possible safe harbours for data sharing agreements, it is plausible to turn to the possibility of institutional and organisational safeguards against both collusion and foreclosure. Starting with collusion, it is true that many types of data can be put to a broad range of uses and that a multitude of possibilities exists to combine different datasets with one another. But the risk that competitively sensitive information can be drawn from a specific dataset may be significantly reduced if the dataset remains on the server of the original 'data controller' and a competitor is given access to those data on the basis of queries and for specified purposes only. According to para. 440 of the European Commission's Draft Horizontal Guidelines (2022), the governance regime of a given data pool may contain safeguards that participants to that pool have access only to the data provided by themselves and to the aggregated data of the other participants for a pre-defined, limited and legitimate set of purposes, for example. Where data is pooled, it may matter for the legality of the data sharing arrangement whether data access is organised through a data intermediary – in the Draft Horizontal Guidelines the European Commission speaks of a 'trustee' (para. 411) – who may be charged with the task to ensure, among other things,[770] that no competitively sensitive information is derived from the relevant dataset. Such a data intermediary may also address the risk of foreclosure if s/he is mandated to ensure FRAND access of third parties to the pooled data. Decisions regarding the standardisation of data formats and interfaces, which are in general competition-enhancing, would still need to be reviewed for anti-competitive effects (see above).[771] These hints to the

[768] For this proposition see, again, Lundqvist EuCML 2018, 146 (153 et seq.).

[769] See Lundqvist EuCML 2018, 146 (153), who likens data pooling to open and transparent standard-setting procedures and suggests that the same privilege could apply under Article 101(1) TFEU – provided that access to the data is provided on FRAND terms and that there is no agreement on what to do with the data: 'The data from the pool must be free to use when competing downstream'.

[770] E.g. to ensure compliance with the GDPR.

[771] For the idea that data intermediaries that manage data pools could play a role in ensuring compliance of data sharing with Article 101 TFEU and an analogy between data intermediaries and independent experts in the frame of TT-agreements (OJ 2014 C 89, 3 para. 256) in this respect also see Botnari, EU Competition Law and Data Pooling, Master Thesis Tilburg Law School, 2020, https://arno.uvt.nl/show.cgi?fid=151932 (last visited 4.7.2022).

relevance of the data governance regime for the assessment of the legality of data access and/or sharing agreements may be further developed and expanded as the experience with data access and sharing agreements grows. Already now, a consolidation of the various 'data governance' principles established in the different data regulations as they currently seem to mushroom would be helpful – although it would need to pay attention to the different contexts and functions or the relevant regulations.

While data intermediaries may be helpful tools to ensure competition law compliance in some instances, they are neither the only possible option to do so, nor may it be easy for them to ensure that no exchange of competitively relevant data takes place between the cooperating parties. There has been some discussion in the literature, for example, to what extent GAIA-X could prevent the exchange of competitively sensitive information in the individual sector data spaces. In any case, its members must accept codes of conduct, which require compliance with competition rules; non-compliance can lead to exclusion from the association.[772] Possibly, GAIA-X could also implement technology which would continuously monitor whether GAIA-X members comply with the requirements of the GAIA-X platform, including (but so far not implemented) competition law.[773] Given the uncertainties surrounding the legality of data sharing, such a technology may not be easily available, however. It may be due to these difficulties that the requirement in Article 11(9) of the European Commission's DGA proposal that DIS "shall have procedures in place to ensure compliance with the European Union and national rules on competition" was deleted in the course of the trialogue.[774] What remains is the general obligation – also of data intermediaries – to comply with competition law in providing their services (see Article 1(4) and Recital 37 DGA).

Ultimately, the effectiveness of data intermediaries in ensuring compliance with Article 101 TFEU may depend on the circumstances of the case. They may be particularly effective in implementing non-discriminatory data access regimes that protect against the risk of anti-competitive foreclosure. In this regard, a certain legal standard appears to emerge in the (still limited) practice of the Bundeskartellamt – which seems to require some degree of independence of the data access manager, but not the involvement of a data intermediary regulated under the DGA.

c) Improved procedures for providing guidance case-by-case?

[772] Falkhofen EuZW2021, 787 (794).

[773] Falkhofen EuZW2021, 787 (794), referring to Catena-X, Die Mitgliedschaft auf einen Blick, https://catena-x.net/de/mitglied-werden (last visited 4.7.2022).

[774] Nevertheless, and surprisingly, the corresponding Recital 29 DGA remained in the final version of the DGA and states that DIS 'should also take measures to ensure compliance with competition law and have procedures in place to this effect. This applies in particular in situations where data sharing enables businesses to become aware of market strategies of their actual or potential competitors. Competitively sensitive information typically includes information on customer data, future prices, production costs, quantities, turnovers, sales or capacities.' See further on this part F(IV) of this study on intermediaries.

Where legal certainty on the legality of a specific data access or sharing arrangement cannot be achieved on a general level, a well-functioning regime for case-by-case guidance is needed.

The Bundeskartellamt is well-known for its readiness to provide undertakings with informal advice with a view to the possibilities and limits of cooperation, including data access and sharing agreements where a relevant legal and economic interest exists. With the 10th amendment to the GWB, the German legislator has complemented the regime of informal advise by a right for cooperating companies to obtain a decision from the Bundeskartellamt under § 32c(1) GWB: if the preconditions for a prohibition according to Article 101 TFEU/§ 1 GWB or Article 102 TFEU/§§ 19, 20 GWB are not fulfilled, and if the cooperating undertakings can show a significant legal and economic interest, the Bundeskartellamt has to issue a decision stating that there is no cause for action at the request of the undertakings (§ 32c(4), (1) GWB)).[775] The decision does not amount to an exemption under Article 101(3) TFEU/§ 2 GWB. But with a § 32c(1)-decision, the Bundeskartellamt commits not to make use of its competences under §§ 32, 32a GWB subject to new insights arising. It will protect the collaborators against prohibitions and fines by the Bundeskartellamt.

To our knowledge, there has only been one – 'non-digital' – request under § 32c(4) GWB so far.[776] The Bundeskartellamt may issue guidance on what needs to be shown to demonstrate a 'legal and economic interest' under § 32c(4) GWB to further increase legal certainty. However, overall the Bundeskartellamt's regime of providing – mostly informal – guidance seems to work well enough. For the Bundeskartellamt, it comes with the benefit that it is regularly confronted with relevant and novel cases and can build up experience in this emerging area of the law. To our understanding, there is no reason to reform the existing legal framework.

§ 32c(4) GWB-decisions will not protect against a prohibition by the European Commission, however. Even the imposition of a fine by the European Commission would remain legally possible, although unlikely in practice. At the European level, the European Commission can, in principle, provide guidance through 'no infringement' decisions under Article 10 Regulation No. 1/2003[777] or, alternatively, through so-called 'comfort' or 'guidance letters' (see Recital 38 Regulation No. 1/2003 and the European Commission Notice on guidance letters[778]). To this date, no Article 10 decision has yet been published, however.[779] Also, DG Competition has been reluctant in the past to provide informal guidance or to issue guidance letters. In order to

[775] Cf. Klumpp/Seitz in Bien et al., Die 10. GWB-Novelle, 2021, Ch. 2, paras. 187-245.

[776] Bundeskartellamt, Bundeskartellamt provides preliminary assessment of DFL's 50+1 ownership rule (Press release of 31.4.2021), https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2021/31_05_2021_50plus1.html (last visited 4.7.2022).

[777] OJ 2003 L 1, 1.

[778] OJ 2004 C 101, 78. See also the European Commission's Draft of a Revised Commission Notice on Informal Guidance of 24.05.2022, https://ec.europa.eu/competition-policy/public-consultations/2022-informal-guidance-notice_en (last visited 4.7.2022). A consultation on this draft is still ongoing.

[779] Vgl. Ritter/Wirtz in Immenga/Mestmäcker, 6th ed. 2019, Article 10 VO 1/2003 para. 3.

ensure that the notification regime under Regulation 17[780] would not be re-introduced through a back door, the preconditions set out in the European Commission's 2004 Informal Guidance Notice for the European Commission to provide informal guidance have been very restrictive. For many years, no guidance letters were issued.

Recently, the European Commission's attitude towards informal guidance has changed, however, as the European Commission has recognised that, in some cases, genuine uncertainty exists and can be a disincentive for undertakings to move forward with collaborations that are overall beneficial. In October 2021, the European Commission has issued a guidance letter on the membership criteria and internal working rules of GAIA-X.[781] Also, the European Commission has published a draft of a revised Notice on Informal Guidance.[782] The public consultation has just ended.[783] Contrary to § 32c(4) GWB, it does not propose to create an individual right to informal guidance or a guidance letter. The European Commission shall provide case-by-case guidance only to the extent that this fits with its own enforcement priorities (Recital 6). Furthermore, in the context of a 'prima facie assessment' two cumulative criteria must be met that suggest that there are valid reasons for the European Commission to provide individual guidance:[784] firstly, the substantive assessment must raise novel or unresolved questions with regard to Articles 101 or 102 TFEU (Recital 7a). Secondly, a public clarification of these questions must provide significant added value. Such added value may be due to the actual or potential economic importance of the goods or services concerned and the consumers' interests;[785] to the fact that the objectives of the agreement (or unilateral practice) are relevant for the achievement of the European Commission's priorities or Union interest;[786] to the magnitude of the investments made which are linked to the agreement (or practice); and the extent to which the agreement (or practice) corresponds – or is liable to correspond – to more widely spread usage, such that the guidance will have precedential value (Recital 7b). No guidance will be given where the legal questions raised are identical or similar to issues raised in a case pending before the CJEU, or where the case is subject to a proceeding before the European Commission or a national competition authority or court (Recital 8). Hypothetical questions will not be considered. Requests for guidance must relate to an agreement (or unilateral practice) that is either ongoing or at an advanced state of planning (Recital 9).

[780] OJ 1962 13, 204.

[781] See European Commission, Letter to Gaia-X (19.10.2021), https://gaia-x.eu/sites/default/files/2021-11/Letter%20to%20Gaia-X_update.pdf (last visited 4.7.2022).

[782] European Commission's Draft of a Revised Commission Notice on Informal Guidance of 24.05.2022, https://ec.europa.eu/competition-policy/public-consultations/2022-informal-guidance-notice_en (last visited 4.7.2022).

[783] The consultation period ends on 21.06.2022.

[784] Under the 2004 Notice on Informal Guidance, only the second criterion is subject to a 'prima facie evaluation' – see OJ 2004 C 101, 78 para. 8b.

[785] According to the 2004 guidance, the economic importance from the consumer's point of view was to be taken into account.

[786] This would be a new criterion compared to the 2004 guidance.

The draft notice certainly has the potential to somewhat 'upgrade' the informal guidance mechanism to a more regularly used mechanism. Indeed, this is in the best interest of both DG Competition and undertakings: for DG Competition, it provides an opportunity to take a closer look at novel arrangements or arrangements of high practical relevance and develop an (informal) line of precedents as the practice of data access and sharing agreements emerges. Informal guidance may allow for the 'agility' that is needed to develop legal principles as the data economy dynamically evolves, and for a setting that is geared towards cooperation instead of confrontation, as infringement proceedings will typically be. In cooperation with the undertakings requesting guidance, measures can be developed and agreed that mitigate potential risks to competition.[787]

However, the draft of a revised European Commission Notice on Informal Guidance falls short of providing a procedural framework that would fully realise this potential. Frequently, measures that may mitigate the risks of data cooperations to competition will themselves be new and partly experimental. In such settings, a new framework for informal guidance should provide for the possibility to test such measures. More than 'one-off' advice in the form of a guidance letter is needed in such a case. Rather, a framework for a monitored temporary experiment is required. For example, the susceptibility of a specific data access or sharing regime to produce collusive outcomes may need to be tested for a specified period of time. In other cases, the governance rules for a data access or sharing agreement may need to be adjusted where it becomes clear that they do not sufficiently guarantee for non-discriminatory access. Where the framework proposed in the draft Notice on Informal Guidance appears to focus on novel legal issues, legal and technological issues will frequently be intertwined in complex ways when it comes to assessing data access and sharing agreements, and much will depend on the sometimes unpredictable effects of novel technical or organisational arrangements.

While it is true that such a regime may absorb a significant amount of resources, it seems that a pro-active strategy to encourage and develop data access and sharing will need such a special framework to accompany the emerging practices in a sufficiently quick and flexible manner. Providing guidance to undertakings in this context would require mixed teams of economists, lawyers and data scientists. In order to keep such a regime manageable and share the burden, an expansion of the cooperation within the European Competition Network (ECN) may be advisable. The ECN may, for example, entrust a national competition authority with the task to monitor a certain data access or sharing agreement and report to the ECN in due time.

A notification mechanism for National Competition Authorities' 'decisions not to take action' could be created. Firstly, such a regime could be used to establish a common line within the ECN. Secondly, if the European Commission does not intervene within a certain period of time, the European Commission could be barred from imposing a fine, and its interventions could be limited to an *ex nunc* effect.

[787] The Draft Notice on Informal Guidance thereby suggests that the Commission is willing to move from an adversarial style of competition law enforcement towards a more cooperative style – described as 'participative antitrust' by Tirole, Economics for the Common Good, 2017, p. 355 et seq.

2. Data-related abuses of dominance – Article 102 TFEU/§ 19 GWB

a) Need for reform?

As shown in part E, Article 102 TFEU and §§ 19, 20 GWB are, in principle, flexible enough to address anti-competitive strategies based on refusals to grant data portability (with regard to individual level, co-generated data) or access to bundled individual level or aggregate usage data or to other types of competitively relevant data. With § 19(2) No. 4 GWB and § 20(1a) GWB, the German legislator has already updated its data-related abuse regime.[788]

However, the gap between § 19(2) No. 4 GWB and § 20(1a) GWB is somewhat puzzling and hints to some unresolved issues regarding the analytical framework for determining a potential anti-competitiveness of refusals to grant access to data.[789] § 19(2) No. 4 GWB seems to suggest that for dominant undertakings, the legal test to determine the unlawfulness of refusals to grant access is the EFD. In relationships of bilateral dependency, § 20(1a) GWB seems to impose an increased responsibility to grant access to data. However, the scope of this responsibility will need to be determined case by case, and § 20(1a) GWB provides little guidance on the principles that should guide the interest balancing. We therefore suggest that a clarification is needed as to when the EFD is the right framework of analysis and when further-reaching obligations to grant access to data are justified (see under b).

An acknowledgment of more far-reaching data access obligations in specific settings – e.g. in ecosystem settings – comes with the question whether all undertakings shall benefit symmetrically, or whether gatekeepers within the meaning of the DMA or undertakings of paramount cross-market significance for competition according to § 19a GWB should be excluded (for such a suggestion see Article 5(2) of the Draft Data Act) (on this: see below, c).

In order to turn data access into an effective competition law remedy, cross-cutting principles must be developed on how to ensure sufficient transparency for access petitioners regarding the type and structure of data held, as well as FRAND access to data (d). The complexity of establishing a regime of effective FRAND access suggests that frequently, sector-specific regulation may be preferable.

Furthermore, guidelines on how to ensure that data access complies with the GDPR will need to be established to make data access regimes work smoothly (e).

---

[788] For a positive reception of this reform see, *inter alia*, Schmidt, Zugang zu Daten nach europäischen Kartellrecht, 2020, p. 549 et seq.; Kerber WuW 2020, 249 (256): "from an economic perspective overall well-designed" and Weber WRP 2020, 559 (565) (important to foster innovation and competition and preferable to an ex ante regulation).

[789] For concerns regarding a continued legal uncertainty with a view to data access issues see, for example, Mäger NZKart 2020, 101 (102); Huerkamp/Nuys NZKart 2021, 327.

b) Towards differentiated analytical frameworks for data access

aa) The role of the EFD as applied to data

So far, the question of when a refusal to grant access to data will amount to an abuse of dominance has mainly been discussed within the framework of the EFD, or with a view to possible adjustments of the EFD to the specificities of data (see above, part E(III)(2)(b)(aa)(3)).

Indeed, depending on the context and the type of data, the EFD may provide an appropriate test for establishing when a refusal to grant access is anti-competitive. The legislative revision of § 19(2) No. 4 GWB confirms as much.

It does not suggest that § 19(2) No. 4 GWB is the adequate analytical framework in all settings, however. This has been corroborated by the integration of a new § 20(1a) GWB. However, the legislator has failed to explain which settings vindicate relatively broad obligations to provide access to data and in which settings obligations to share are to be handled rather restrictively.

Meanwhile, two possible reasonings have emerged that may justify the imposition of further-reaching obligations to share data. Firstly, an orchestrator of an ecosystem in which data functions as an important link between the various segments or markets may be under a special obligation to grant access to data to those users of the ecosystem that contribute to the generation of the data and to the success of the ecosystem (bb). Secondly, special data-sharing obligations may be justified in data-driven markets (cc).

bb) Special data access obligations for ecosystem orchestrators

For some time, the debate on competition law-based access to data obligations has been led in a rather generic fashion. More recently, the specificities of digital ecosystems have come into view. While different types of ecosystems exist,[790] data will frequently play an important role: user and usage data may be cross-used in different segments of the ecosystem; it may connect core products with complementary services; and it may drive innovation within the ecosystem.

With § 19a GWB, the German legislator has already recognised the specificities of digital ecosystems, including – to some extent – the role of data (see § 19a(2), 1st sentence, No. 4 GWB). But the scope of application of § 19a GWB is limited to the largest players, namely those of "paramount cross-market significance for competition".

Yet, a refusal of an ecosystem orchestrator to share data with the complementors may raise competition concerns below this threshold. In an open ecosystem, complementors contribute significantly to the overall value of the ecosystem. To the extent that it has become difficult for

[790] See, for example, Jacobides/Cennamo/Gawer Strateg. Manag. J. 2018, 2255; Jacobides/Lianos Ind. Corp. Change 2021, 1131; Jacobides/Lianos Ind. Corp. Change 2021, 1199.

complementors to switch to another ecosystem or to multi-home, the ecosystem orchestrator may, however, be able to exclusively control a large part of the data and, consequently, the data-driven business opportunities. It may, therefore, be appropriate to develop principles for data sharing in ecosystems – within the framework of § 19 GWB, and/or within the framework of § 20(1a) GWB. The sharing obligations may relate to individual level data – and hence amount to an obligation to ensure data portability. But depending on the precise setting and the competitive relevance of the data, they may also comprise an obligation to share bundled individual level or aggregate user data.[791] The sharing obligation will be limited to observed data: which insights can be inferred will be part of the competition to be expected and protected.[792] While data sharing obligations may follow already today from an open-ended interest balancing based on § 19(1) and (2) No. 1 or on § 20(1a) GWB, the practical relevance of these provisions may increase[793] if the legislator were to clarify that data sharing within ecosystems may be a special use case, and to develop a more structured test for this setting. Relevant criteria would include, *inter alia*, the question whether the access petitioners can still switch the ecosystem or multi-home; whether they contribute to the generation of the data, and to the value of the ecosystem; to what extent possibilities to compete and innovate within the ecosystem depend on data access; and to what extent the data is an important connecting factor between different segments of the ecosystem.

Data sharing principles within digital ecosystems may also include a rule that an ecosystem orchestrator, who simultaneously competes within the ecosystem will only be allowed to combine data generated by its own services with data generated by the offers of other business users of the ecosystem if, and to the extent to which, the ecosystem orchestrator ensures FRAND access to its 'own' data troves for these other users, too.

cc) Special rules on data sharing in data-driven markets?

Proposals for more far-reaching data access regimes have, so far, not been linked to data sharing in digital ecosystems, but rather to the sharing of user data in data-driven markets. Such a proposal has been presented, in particular, by Graef and Prüfer.[794] According to them, markets are data-driven "if a firm's marginal costs of innovation decrease with the amount of user information, that is, if it is subject to specific feedback effects ('data-driven' indirect network effects)".[795] A three-pronged test is proposed to determine whether these conditions are met: (i) there must be a positive relationship between demand and user information, (ii) user

[791] For a somewhat related proposal see Feasey/de Streel, Data sharing for digital markets contestability: towards a governance framework, CERRE Report September 2020, p. 55 et seq.

[792] Crémer/de Montjoye/Schweitzer, Competition Policy for the Digital Era, Final report, 2019, p. 101.

[793] Doubts regarding the practical relevance of the existing provisions have been expressed, *inter alia*, by Steinberg/Wirtz WuW 2019, 606 (607 et seq.); Lettl WRP 2020, I, Nr. 02; Körber MMR 2020, 290 (291 et seq.); Herrlinger WuW 2021, 325 (327 et seq.); Schweda/von Schreitter WUW 2021, 145.

[794] See Graef/Prüfer Research Policy 50 (2021) 104330.

[795] Graef/Prüfer Research Policy 50 (2021) 104330, p. 3. See also Argenton/Prüfer J. Compet. Law Econ. 2012, 73; Prüfer/Schottmüller J. Ind. Econ. 2022, 967.

information must be necessary to improve quality, (iii) quality must create more demand.[796] The search engine market has been presented as a paradigmatic example where all three conditions are met and a data sharing obligation should therefore be imposed.[797]

Together with Schottmüller, Prüfer has shown that in data-driven markets, user information may lead to market tipping (monopolization) and thus to lower incentives to innovate for both the dominant firm and (potential) competitors.[798] They have also shown that a dominant company can leverage its dominance to a connected market if user information is also valuable there as well, creating a 'domino effect'.[799]

Arguably, in data-driven markets, data sharing obligations can, already today, be imposed on dominant undertakings where a refusal to share data is found to be part of an exclusionary strategy.[800] Graef and Prüfer have proposed to introduce a data sharing obligation outside the realm of competition law, however, along the following lines:[801]

- Only user information shall be covered, i.e. "raw data about users' choices or characteristics, which can be logged automatically". In order to avoid interference with investment incentives, the sharing obligation would not extend to "processed data", where the data holder has invested in data analytics.
- Firms active in a data-driven market should be obliged to share their user data if their market share exceeds 30%.
- These firms shall make 'their' user data available to "every organization that is active in the respective industry or that can explain how it would serve users with the data". Consequently, the data sharing obligation would extend beyond our scenario 2 to the scenario 3 setting: it would not only impose an obligation to promote competition within the 'system' in which the firms are active, but a positive obligation to promote overall innovation.
- Gatekeepers under the DMA should be disqualified from data access.
- The appropriate access price to user information should equal the marginal cost of obtaining the user information, which is considered to be "(roughly) zero".
- For the implementation of the data sharing obligation, Graef and Prüfer have proposed a multi-level governance structure with national authorities and a yet to be established European Data Sharing Agency (EDSA) in charge.

---

[796] Prüfer, Competition Policy and Data Sharing on Data-driven Markets: Steps Towards Legal Implementation, http://library.fes.de/pdf-files/fes/15999.pdf (last visited 4.7.2022), p. 10 et seq. See also Klein et al., A Simple Test for Data-Drivenness of Markets, Tilburg University mimeo 2021.

[797] Argenton/Prüfer J. Compet. Law Econ. 2012, 73.

[798] Prüfer/Schottmüller J. Ind. Econ. 2022, 967.

[799] Prüfer/Schottmüller J. Ind. Econ. 2022, 967.

[800] See Crémer/de Montjoye/Schweitzer, Competition Policy for the Digital Era, Final report, 2019, p. 105 et seq. See, on the other hand, Casanova, Online Search Engine Competition with First-Mover Advantages, Potential Competition and a Competitive Fringe: Implications for Data Access Regulation and Antitrust (9.7.2020), https://ssrn.com/abstract=3647092 (last visited 4.7.2022): "We argue that when dominance is derived from first-mover advantages and innovation feedback loops, rather than high and non- transitory barriers to entry, competition policy and regulation should avoid undermining first-mover advantages through access regulation, as this is likely to result in trade-offs on innovation by all market players. We support instead a focus on prohibiting exclusionary behaviour by first movers to avoid leadership derived from anti-competitive foreclosing abuses rather than from competition on the merits."

[801] Graef/Prüfer Research Policy 50 (2021) 104330, p. 4 et seq.

A somewhat similar proposal has been presented by Krämer und Schnurr.[802] Like Graef and Prüfer, they want to address strong data-driven network effects[803] by way of an *ex ante* data sharing obligation[804] with a view to enabling niche entry and growth in data-driven markets.[805]

Indeed, next to data-sharing in digital ecosystems, data-driven markets appear to be a second setting, where specific rules on data sharing may need to be developed. Yet, it seems unclear whether this needs to be done outside the realm of competition law. Given the current dearth of data access requests, it is an open question whether the establishment of such a costly regulatory regime is justified at this point of time, and whether companies with a 30% market share in data-driven markets should systematically be subjected to such a regime. For the moment, it seems preferable to gain experience with data sharing based on competition law and sector-specific data sharing regimes.

c) Excluding gatekeepers from data access?

Interestingly, Graef and Prüfer have suggested to exclude gatekeepers from data access under their proposed data sharing regime. Similarly, Article 5(2) of the Draft Data Act proposes to exclude gatekeepers from data access. The obvious intuition is that – given the vast data resources they control and the competitive advantage that follows therefrom – gatekeepers should not be able to seize even more data and to further increase their competitive advantage.

Indeed, gatekeepers within the meaning of the DMA or undertakings of paramount cross-market significance for competition under § 19a GWB will frequently not be able to rely on the EFD to access data held by competitors that are dominant in a given market: in many cases, access to those data will not be indispensable for the gatekeepers to compete.[806] In some settings, the indispensability criterion may, however, be met with a view to competing in a specific market.

If gatekeepers were granted access to the relevant data in such a setting – or if they were granted access based on § 19(1) with (2) No. 1 GWB or on § 20(1a) GWB – they may, however, enjoy huge competitive advantages if they, and they alone, are able to combine those data with the data troves they already possess.

---

[802] Krämer/Schnurr J. Compet. Law Econ. 2022, 255.

[803] For a data-driven theory of harm three main arguments, comparable to Prüfer/Schottmüller J. Ind. Econ. 2022, 967, were made: (i) "in cases where data-driven network effects are strong, markets tend to monopolize (market tipping)", (ii) "this tipping effect does not stop in the very market where it started, but may spill over to related, data-intensive markets, which can already exist or may still emerge", and (iii) "this also has an effect on innovation, because high entry barriers stifle innovation activity in those areas and markets where entrants may set out to compete with the incumbent", Krämer/Schnurr J. Compet. Law Econ. 2022, 255, (258 et seq.).

[804] For the shortcoming of competition law and the need to establish some kind of *ex ante* regulation see Krämer/Schnurr J. Compet. Law Econ. 2022, 255 (268 et seq.).

[805] Id., 270 et seq.

[806] For this argument see Nothdurft in Bunte, Kartellrecht, 14th ed. 2022, § 20 GWB, at para. 99.

From a policy perspective, an obvious solution in such settings may be to make a gatekeeper's access to data conditional upon a commitment of the gatekeeper to open up its own data troves to competitors on FRAND terms. Given the existing legal framework, it is not obvious on which basis such a conditionality can be imposed, however. If the gatekeeper is regarded as a potential competitor from the start, the undertaking's position of dominance might be questioned from the start. Such a perspective may disregard the real absence of competitive discipline, absent a data sharing obligation.

The problem could be solved by amending § 19a GWB. The Bundeskartellamt would then be empowered to inhibit a norm addressee's access to data from undertakings which are – otherwise – subject to a data sharing obligation, or rather to make it conditional on a norm addressee's commitment to share their own data troves on FRAND terms.

d) Transparency requirements and FRAND access to data

As set out in part E(III)(4), it will often not be sufficient to oblige an undertaking to share data. Rather, the question of *how* the data shall be shared will need to be addressed. This may include a need to specify

- (common) data formats,
- easy-to-use technical interfaces (as APIs),
- fees and other conditions,
- safety/security requirements and preconditions for compliance with privacy laws (in the EU: the GDPR),
- additional interoperability requirements.[807]

Furthermore – and contrary to FRAND access to SEPs – FRAND access to data may presuppose the establishment of a transparency regime: access petitioners must, first of all, be enabled to discern what types of data are controlled by the data controller, how the data is structured etc.

Making data access effective may require the establishment of a highly complex regime.[808] The "access to account" regime that was established under the P2D2 Directive may serve as an illustration (see Box). Given that the precise structure and governance regime may be highly sector-specific, adopting sector-specific regulation may frequently be the preferred choice.[809] It may, however, be a task for competition law to help establish a set of horizontal legal principles that such regimes should follow.

---

[807] See Kerber in German Federal Ministry of Justice and Consumer Protection/Max Planck Institute for Innovation and Competition, Data Access, Consumer Interests and Public Welfare, 2021, p. 439 (450).

[808] See Id., 444. See also the high degree of detail in merger remedies that relate to data access in BMW/Daimler, Google/Fitbit and Meta/Kustomer (part E(IV)(2)(c)(bb)).

[809] Höppner/Weber K&R 2020, 24 (48); Schweitzer in Kühling/Zimmer, Neue Gemeinwohlherausforderungen – Konsequenzen für Wettbewerbsrecht und Regulierung, 2020, p. 44 (54).

Box: the implementation of the 'XS2A' regime under the PSD2-Directive

The implementation of the PSD2 Directives – which introduced a sector-specific access to account regime in the financial sector ('XS2A') – illustrates the complexity of implementing a data sharing obligation. Under this framework, member states shall ensure that account servicing payment service providers (ASPSP), such as banks, provide account information service providers (AISP) with real time access to bank account information (Article 67), and payment service providers (PISP) with access to the account of a customer and the ability to initiate payments directly from that account (Article 66) – both upon request of the account holder. The regulation also includes additional requirements, such as strong authentication of the bank, licensing of the financial service providers, and the liability of the bank for mistakes and fraud (see Article 66 et seq.).

Both forms of access depend on direct technical access to the bank account, so ASPSPs need to set up open interfaces for AISPs and PISPs.[810] Some degree of standardization may be required here.[811] The European Banking Authority (EBA) has been mandated to develop draft regulatory technical standards (RTS) on authentication and communication, which ASPSPs need to comply with, to ensure the successful functioning of XS2A (Article 98). In particular, the EBA should specify the requirements of common and open standards, which should ensure the interoperability of different technological communication solutions (Recital 93). The initial draft RTS of 2017 established, among other things, that customer data is provided through a dedicated interface provided by the bank.[812] This raised concerns among Fintechs, because such a system would have allowed banks to secretly interfere in the data transfer process.[813] The European Commission's reaction was to introduce an amended version of the EBA's draft RTS that includes a mechanism for direct account access in case of deficiencies in the dedicated interface.[814]

[810] See Kerber in German Federal Ministry of Justice and Consumer Protection/Max Planck Institute for Innovation and Competition, Data Access, Consumer Interests and Public Welfare, 2021, p. 439 (452).

[811] For the pros and cons of standardizing APIs in the context of XS2A see Borgogno/Colangelo, Data, Innovation and Transatlantic Competition in Finance: The Case of the Access to Account Rule (15.4.2020), https://ssrn.com/abstract=3251584 (last visited 4.7.2022), p. 14.

[812] European Banking Authority, Final Report on Draft Regulatory Technical Standards on Strong Customer Authentication and common and secure communication under Article 98 of Directive 2015/2366 (PSD2), https://www.eba.europa.eu/sites/default/documents/files/documents/10180/1761863/314bd4d5-ccad-47f8-bb11-84933e863944/Final%20draft%20RTS%20on%20SCA%20and%20CSC%20under%20PSD2%20%28EBA-RTS-2017-02%29.pdf (last visited 4.7.2022).

[813] For a comprehensive account of the "RTS saga" see Borgogno/Colangelo, Data, Innovation and Transatlantic Competition in Finance: The Case of the Access to Account Rule (15.4.2020), https://ssrn.com/abstract=3251584 (last visited 4.7.2022), p. 12 et seq.

[814] C(2017) 3459 final.

Finally, after further intense discussions between the European Commission, the European Parliament and the European Council,[815] the European Commission published the final version of the RTS in March 2018, which provides requirements to be complied with by payment service providers – including specifications for the establishment of common and secure open standards for the communication between ASPSPs, PISPs, AISPs, payers, payees and other payment service providers (see Article 1 lit. d, 28 et seq.).[816] In order to provide clarity on the interpretation of the RTS requirements, the EBA has issued an opinion to help and coordinate private standardization entities operating across the EU.[817] A number of private standardization initiatives developed market solutions, such as the Berlin Group, which has developed the NextGenPSD2 XS2A framework – the main standard used in Germany.[818]

Within the framework of the RTS, it is up to the payment service providers how they implement the XS2A requirements under the PSD2 directive. From a strategic perspective, they can decide to choose a passive 'compliance-only' approach ensuring that other companies can access a customer's account data and execute transactions via PSD2 APIs, or they can decide to be proactive and develop a 'bank ecosystem' where bank processes in all segments are supported with integrated FinTech partner products.[819]

Also on a more technical note, banks have to consider a wide range of implementation options:[820] besides deciding to adopt a market standard for APIs or to develop their own interfaces, they need to consider whether to combine several interface standards, to (voluntarily) implement additional functions (e.g. forward transfers, mass payments, standing orders), to include certificates at the application layer for more security (PSD2 only requires using certificates at the transport layer). Furthermore, they need to choose an option for customer authorization and access management, consent management, strong customer authentication (PSD2 requires two-factor authentication) and exceptions as well as transaction monitoring mechanisms.

e) Compliance with the GDPR

[815] See Borgogno/Colangelo, Data, Innovation and Transatlantic Competition in Finance: The Case of the Access to Account Rule (15.4.2020), https://ssrn.com/abstract=3251584 (last visited 4.7.2022), p. 13 et seq.

[816] OJ 2018 L 69, 23. For a list of the main requirements of the RTS see European Banking Authority, Opinion on the implementation of the RTS on SCA and CSC, 2018, p. 3 et seq.

[817] Ibid.

[818] See NDGIT, Guidelines for PSD2 Implementation: Helping banks explore API strategies and options, https://ndgit.com/wp-content/uploads/2019/04/NDGIT-PSD2-Whitepaper-en.pdf (last visited 4.7.2022), p. 5. For further information see also The Berlin Group, PSD2 Access to Bank Accounts, https://www.berlin-group.org/psd2-access-to-bank-accounts (last visited 4.7.2022).

[819] NDGIT, Guidelines for PSD2 Implementation: Helping banks explore API strategies and options, https://ndgit.com/wp-content/uploads/2019/04/NDGIT-PSD2-Whitepaper-en.pdf (last visited 4.7.2022), p. 3.

[820] Id., p. 5 et seq. See also Open Banking Europe, Third Party Provider User Management for PSD2 Access to Account (XS2A) https://www.openbankingeurope.eu/media/1176/preta-obe-mg-001-002-psd2-xs2a-tpp-user-management-guide.pdf (last visited 4.7.2022).

As the empirical survey[821] has demonstrated, uncertainty about the legality of data access and data sharing under the GDPR is widely perceived as an impediment to data sharing. This may also be true for dominant undertakings: when it comes to personal data, the GDPR may indeed constrain the ability of data controllers to provide access to bundled individual or aggregate data.[822] Relevant uncertainty may also exist with regard to compliance with Article 101 TFEU.[823] In order to facilitate data sharing and data access and to lower compliance risk and cost also for dominant undertakings, they should be provided with guidance as to how to effectively comply with these regimes.

3. Merger Policy

a) Overview

Merger policy with regard to data-driven business models is subject of ongoing policy reform in the context of the larger debate around mergers in digital markets and killer acquisitions. Currently options are already considered in different European countries and the EU, ranging from preliminary consultations to legislative proposals before the parliaments. The variety of proposals and priorities for reform will be outlined in section b), particularly the policies in the U.K., France, Germany, the EU, and the U.S. Taking these proposals into account and considering the analysis of data-driven mergers that was conducted in part E(IV), further policy options are discussed in section c). In general, it appears advisable that the German legislature strengthens merger review to accommodate the particular effects of data-related mergers to competition. One means would be to modify merger review at least within the scope of § 19a GWB. At the same time, reforms of EU merger review should be considered.

As a general caveat, proposals have not yet reached a satisfying level of conceptual refinement that would eliminate doubts about their effective applicability by competition authorities. There is increasing economic evidence for adequately conceptualising the legal framework for mergers, but a recalibration of the merger review framework would still need further, more targeted inquiry and consultation. Nevertheless, already in light of the current evidence, this study supports the general direction of considering strengthening merger review with particular regards to data-driven markets and ecosystems.

b) Policy debate

aa) Debate across Europe

[821] IEDS, Anreizsysteme und Ökonomie des Data Sharings: Handlungsfelder des unternehmensübergreifenden Datenaustausches und Status quo der deutschen Wirtschaft, 2022, p. 52.

[822] These constraints may be avoided through anonymization. For an overview about anonymization techniques and the 'differential privacy' approach towards anonymization, see Hölzel EDPL 2019, 184.

[823] Cf. Schallbruch/Schweitzer/Wambach, Ein neuer Wettbewerbsrahmen für die Digitalwirtschaft, Bericht der Kommission Wettbewerbsrecht 4.0, p. 56-59.

(1) EU level

On the EU level, the Article 22 EUMR Guidance and Article 14 DMA (see part E(IV)(2)(a)) were notable measures which concern an update of merger review. Currently ongoing is the European Commission's revision of the Implementing Regulation and the European Commission Notice on Simplified Procedure.[824] This aims to lower administrative burdens. However, neither does this specifically affect competition in digital markets nor does the European Commission generally plan to change the substantial rules of the EUMR as such. In this regard, the European Parliament has lately reaffirmed that data is key when it comes to digital markets,[825] and calls on the European Commission to consider revising the merger guidelines[826] as well as taking "a broader view when evaluating digital mergers and to assess the impact of data concentration".[827]

Furthermore, the European Commission has gathered evidence on the revision and updating of its market definition notice.[828] It aims to revise the Market Definition Notice of 1997,[829] not the least to consider the peculiarities of "digital markets, in particular with respect to products or services marketed at zero monetary price and to digital 'ecosystems'" as well as 'non-price competition (including innovation)'[830]. Such update appears overdue.

(2) United Kingdom

The U.K. has expressed on various occasions to tighten merger review. Quite influentially, the U.K. Furman report of March 2019 suggested that "merger assessment in digital markets needs a reset" and has given comprehensive advice.[831] The Lear report of May 2019[832] has extensively assessed merger practice in digital markets in the U.K. The findings of both reports are reflected in the revised merger guidelines, which the CMA adopted in March 2021.[833] The revisions aim

---

[824] See European Commission, Merger policy package of 26 May: Evaluation and follow-up actions, https://ec.europa.eu/competition-policy/public-consultations/2021-merger-control_en (last visited 4.7.2022). In a first public consultation the European Commission gathered information about the simplification of merger control procedures, see https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12957-Revision-of-certain-procedural-aspects-of-EU-merger-control/public-consultation_en (last visited 4.7.2022). The European Commission launched a new public consultation open from May 6, 2022 until June 3, 2022, regarding a further simplification of the procedures, see https://ec.europa.eu/competition-policy/public-consultations/2022-merger-simplification_en (last visited 4.7.2022).

[825] See European Parliament, Competition Policy – annual report 2021, P9_TA(2022)0202, 05.05.2022, para. 63.

[826] See Id., para. 59.

[827] See Id., para. 65.

[828] See findings in COM SWD(2021) 199 final.

[829] OJ 1997 C 372, 5.

[830] See European Commission, Competition: Commission publishes findings of evaluation of Market Definition Notice (Press release of 12.07.2021), https://ec.europa.eu/commission/presscorner/detail/en/IP_21_3585 (last visited 4.7.2022).

[831] See Furman et al., Unlocking Digital Competition, 2019, p. 93.

[832] Argentesi et al., Ex-post Assessment of Merger Control Decisions in Digital Markets, 2019.

[833] See CMA, Merger Assessment Guidelines, 18.3.2021.

to prevent under-enforcement of merger review, especially in relation to digital markets, and to improve the CMA's tools to address situations in which buyers strategically buy up competitors (killer acquisitions). Amongst other, the guidelines stipulate a wide margin of appreciation and an increased focus when assessing evidence on the future development of competition, to explicitly consider non-price competition (e.g. level of privacy offered to users of digital services), and outline a more flexible approach of market definition.

Moreover, the Furman report was followed by the establishment of the Digital Markets Taskforce, which provided advice on a pro-competition regime for digital markets in December 2020.[834] It suggested a new regime for firms with 'strategic market status' (SMS), which would also include a mandatory notification system and reporting obligations as well as a lower standard of proof for finding a SLC at phase 2.[835] Subsequently, the Digital Markets Unit (DMU) within the CMA was formally set up in 2021. Amongst other things, the DMU develops a legislative framework for a new digital markets regime,[836] and it should enforce new rules on companies with SMS on digital markets. However, the U.K. legislator still needs to put such new regulatory regime in place and grant the DMU powers beyond the existing capabilities of the CMA. Legislation is not expected before 2023. In May 2022, the government further outlined possible monitoring and enforcement abilities this legal regime may take up.[837] It confirmed that companies who will get assigned an SMS have to report their most significant merger transactions to the CMA prior to their completion. At the same time, the government announced not to further pursue proposed changes to the Phase 2 merger review threshold.

(3) France

Also in France, reforming competition law and merger review with regard to digital markets is controversial for some time. Currently, the French legislator discusses an amendment to the national merger rules. Comparable to § 19a GWB, the proposal of the Senate[838] suggests designating undertakings with outstanding market position as 'entreprises structurantes'. Such undertakings should be obliged to report prior to transaction any merger that would impact the French market. In case the Autorité de la Concurrence decides to initiate an in-depth examination of such transaction, the proposal stipulates a reversal of the burden of proof: entreprises structurantes must provide evidence that the transaction is not likely to harm competition. The chances of political consensus remain open. A similar proposal has been

[834] See https://www.gov.uk/cma-cases/digital-markets-taskforce (last visited 4.7.2022).

[835] See Furman et al., Unlocking Digital Competition, 2019, p. 89–102.

[836] See Levy et al., https://practiceguides.chambers.com/practice-guides/merger-control-2021/uk/trends-and-developments (last visited 4.7.2022).

[837] See Department for Digital, Culture, Media and Sport, Department for Business, Energy and Industrial Strategy: A new pro-competition regime for digital markets - government response to consultation – A consultation outcome, 2022.

[838] Version which was submitted to the Assemblée Nationale, the relevant proposals being: Proposition de loi Nr. 62, 19 février 2020 (Sénat: 48, 301 et 302 (2019-2020)).

rejected in the Assemblée Nationale in October 2020.[839] Besides criticism on the matter, the reform was also postponed with the motivation of achieving a uniform EU solution. However, after the 'small throw' of Article 14 DMA and the controversial referral mechanism under Article 22 EUMR, the debate on national reforms will continue. Moreover, the Autorité de la Concurrence has considered additional reform avenues, such as introducing alternative thresholds or empowering the Autorité de la Concurrence to require the parties to notify a concentration ex ante or ex post under specific conditions.[840]

(4) Germany

In Germany, the 'Kommission Wettbewerbsrecht 4.0' enquired into the thresholds and referral systems, the prospects of an ex-post control regime and proposed guidance for acquisitions of start-ups by dominant players.[841] Yet, the subsequent 10th Amendment to the GWB has not addressed killer acquisitions, instead it has been declared to pursue tighter rules on the EU level. In its joint statement with the CMA and ACC of April 2021,[842] the Bundeskartellamt has called for a more rigorous approach in blocking mergers and to prefer structural over behavioural remedies.[843] The statement also calls for questioning the presumption that mergers are generally efficiency-enhancing, pointing to the competition authorities' experience that merging firms tend to overstate the benefits while competitors, consumers and consumers are less engaged in the merger review procedure.[844] One month later, the German Government made clear its negotiating position for the DMA, considering the European Commission's proposal of Article 12 DMA (what then became Article 14 DMA) as a possibility to modify the merger control system under the EUMR by introducing value-based thresholds and adapting the substantive requirements to address killer acquisitions.[845]

bb) The U.S. Debate

In the U.S., there is a comprehensive policy discussion on the up-to-dateness of the merger guidelines. In January 2022, the FTC and DoJ announced the launch of their agencies' comprehensive joint review of the current horizontal and vertical merger guidelines.[846]

---

[839] Draft Legislation („projet de loi Ddadue') 2020, Initial Proposal of the Government: Projet de loi Nr. 314, 12 février 2020. Proposal for amendment of the Senate on Art. 4: Projet de loi Nr. 120, 8 juillet 2020 (Sénat: 314 rect. bis, 552, 553 et 548 (2019-2020)).

[840] See Autorité de la concurrence, Contribution au débat sur la politique de concurrence et les enjeux numériques, 19 February 2020.

[841] See Schallbruch/Schweitzer/Wambach, Ein neuer Wettbewerbsrahmen für die Digitalwirtschaft, Bericht der Kommission Wettbewerbsrecht 4.0, 2019, p. 65–71.

[842] CMA/ACCC/Bundeskartellamt, Joint statement on merger control enforcement, 2021.

[843] Id., para. 16.

[844] Id., paras. 9, 12, 14.

[845] See France/Germany/Netherlands, Strengthening the Digital Markets Act and Its Enforcement, non-paper, 2021.

[846] See U.S. Department of Justice, U.S. Federal Trade Commission: Request for Information on Merger Enforcement, 2022.

Amongst other, the agencies inquire into whether the agencies should analyse mergers involving digital markets and 'special characteristics markets' differently than other markets, including market definition, theory of harm, market tipping and network effects, zero-pricing, data-aggregation as motive or effect, interoperability and competition for attention.[847] After a 90-day period of public comments and the hosting of listening forums,[848] the FTC and DoJ are now considering to issue revised draft guidelines for public comment.[849] The outcome remains to be seen, but a clear policy trend towards tightening merger review is visible: DoJ Assistant Attorney General Jonathan Kanter has announced moving practice towards litigation rather than settlement negotiations.[850] Moreover, FTC Chair Lina Khan mentioned that the use of presumptions as well as nascent competition and how to update the conceptual framework of the guidelines to account for digital markets are issues to be considered.[851]

c) Discussion of Policy Options

aa) Towards Stricter Merger Review

The mentioned policy discussions reveal a clear trend across jurisdictions: merger review should be tightened to fill gaps and prevent systemic underenforcement.[852] Also in practice, the CMA's order to unwind Meta's acquisition of Giphy[853] as well as the controversial review outcomes and merger decisions in Meta/Kustomer and Google/Fitbit suggest that merger review needs some update. The debate on merger policies and enforcement goes hand in hand with a lively academic discourse regarding merger review in digital markets[854] and data-driven mergers in particular.[855] There is increasingly empirical evidence on troublesome competitive

[847] See Id., p. 7–8.

[848] Listening forums took place between March and May 2022, for details see FTC, FTC and Justice Department Launch Listening Forums on Firsthand Effects of Mergers and Acquisitions, 2022; the forum specifically dedicated to mergers in the technology sector was set for 12.05.2022, see FTC, FTC and Justice Department Listening Forum on Firsthand Effects of Mergers and Acquisitions: Technology, 2022.

[849] See FTC, Federal Trade Commission and Justice Department Seek to Strengthen Enforcement Against Illegal Mergers (Press release of 18.01.2022).

[850] See Jonathan Kanter, Opening Remarks at 2022 Spring Enforcement Summit *(April 4*, 2022) (transcript available https://www.justice.gov/opa/speech/assistant-attorney-general-makan-delrahim-delivers-remarks-university-haifa-israel (last visited 4.7.2022)).

[851] See FTC, Enforcers Summit Transcript of 04.04.2022.

[852] Overview in OECD, Start-ups, Killer Acquisitions and Merger Control, 2020; Sousa/Pike CLPD 2020, 26.

[853] See Killeen, https://www.euractiv.com/section/digital/news/meta-fined-1-5-million-for-breaching-giphy-acquisition-enforcement-order/ (last visited 4.7.2022),

[854] See Kwoka, Controlling Mergers and Market Power, 2020, p. 109–117, on mergers in the tech sector; questioning whether merger review is the right place see Cabral Inf. Econ. Policy 2021, 100866; regarding U.K., see Furman et al., Unlocking Digital Competition, 2019, paras. 3.32–3.108; Parker/Petropoulos/Van Alsytne Ind. Corp. Change 2021, 1307. See also Franck/Monti/de Streel, Article 114 TFEU as a Legal Basis for Strengthened Control of Acquisitions by Digital Gatekeepers, 2021, who evaluate options to strengthen control of acquisitions by digital gatekeepers before the background of the internal market competence under Article 114 TFEU.

[855] For a recent overview on the literature see Chen et al. RAND J. Econ. 2022, 3 (8–9).

effects and the gaps in current merger review regimes.[856] Much research has dealt with the legal framework for reviewing acquisitions by big tech and on killer acquisitions in particular.[857] However, identifying killer acquisitions in reality appears complex and evidence is still limited.[858] Another strand of academic discourse concerns the interrelation between data protection/privacy and competition law.[859] Particularly in the context of merger control, privacy can be a parameter of competition,[860] but also data protection rules can play a role for the competitive assessment,[861] as well as for designing effective data access remedies.[862]

The main argument for a more restrictive stand of merger review in digital markets refers to the higher social cost of an incorrect clearance in digital markets as compared to traditional markets, dues to high concentration/network effects and barriers to entry.[863] So even if there are efficiency gains in the short run, there is a risk of market tipping in the long run due to data externalities and network effects.[864]

Combining these rather general findings with the enquiry into data-driven mergers (see part E(IV)), the following analysis discusses possible policy options for the German legislature with regard to merger review. After looking at data-related remedies (under bb), more general aspects of the referral system (under cc) and notification thresholds (under dd) are discussed, before outlining means to advance the substantive criteria for merger review in Germany (under ee) and the implications for EU merger review (under ff).

bb) Remedies and data-related mergers in the EU

(1) The controversy on behavioural remedies and data-driven mergers

[856] See Affeldt/Kesle JECLAP 2021, 471, who find that half of he acquired apps by GAFAM are discontinued, continued apps become free of charge but request more private-sensitive permissions for use; Argentesi et al. JECLAP 2021, 95, analyze the characteristics of almost 300 mergers in the U.K. by Amazon, Facebook and Google; Motta/Peitz Inf. Econ. Policy 2021, 100868.

[857] See on 'killer acquisitions' Crémer/de Montjoye/Schweitzer, Competition Policy for the Digital Era, Final report, 2019, p. 111; Stuart ECJ 2021, 407; for numbers of acquisitions by GAFAM companies Witt Antitrust Bull. 2022, 208 (230); on post-merger break up Ducci/Trebilcock, CPI Antitrust Chronicles April 2020, p. 4.

[858] Gautier/Lamesch Inf. Econ. Policy 2021, 100890, identify one killer acquisition out of a sample of 175; however, questioning the sufficiency of evidence Wong-Ervin/Moore CLPD 2020, 51.

[859] Early on Lande, University of Baltimore School of Law Legal Studies Research Paper No. 2008-06.

[860] See e.g. Chirita in: Akseli/Linarelli, The Future of Commercial Law: Ways Forward for Change and Reform, 2019, p. 147, 40–42 (of the pre-published working paper); see Bitton/Overton, https://globalcompetitionreview.com/guide/e-commerce-competition-enforcement-guide/third-edition/article/united-states-e-commerce-and-big-data-merger-control (last visited 4.7.2022), with regards to the U.S. debate and practice.

[861] See Batchelor/Janssens Eur. Compet. Law Rev 2020, XI. (XV).

[862] See Kathuria/Globocnik J. Antitrust Enforc. 2020, 511.

[863] See Argentesi et al. JECLAP 2021, 95 (131).

[864] See Chen et al. RAND J. Econ. 2022, 3 (21).

As has been shown, it is highly controversial whether merger review does and should move from structural towards behavioural remedies. Especially, the recent remedy practice of the European Commission in BMW/Daimler, Google/Fitbit and Meta/Kustomer has stimulated the discussion.[865] Some regard the European Commission's recent decisions as a significant break with its previous practice to favour structural remedies.[866] In general, one cannot observe a general trend: there is still a strong preference for structural remedies in merger control.[867] Nevertheless, views are split on the benefits and risks of moving towards behavioural remedies with regard to data-related mergers.

(2) Towards a more structural approach

Proponents of a 'more flexible and differentiated approach to remedies' argue that behavioural remedies could fit better than structural remedies if future market and business model developments are difficult to foresee and especially the effects of structural remedies may be hard to predict.[868] In particular, access for third parties to data can be a suitable remedy, when the efficiencies are also gained through access of the merging entities to this data. Especially non-discriminatory access provisions can have far-reaching impact as the aim to protect a level playing field and the quality of access for third parties,[869] so that competitiveness of whole markets should be preserved or even created. By this means, data sharing can prevent monopolization and reverse short-run effects of the merger to mitigate the dynamic trade-off under certain circumstances – however, the effects considerably depend on policy and markets.[870] Before this background, Google/Fitbit may be regarded as a 'test case for future mergers and acquisitions'.[871]

Yet, such views face heavy criticism[872] and should indeed be regarded with caution. Ex-post evaluations in the U.K. have confirmed the superiority of structural over behavioural remedies, regarding the latter as more risky, complex and resource intensive to design and monitor, only being likely to work in a regulated environment, where aspects of monitoring can be delegated.[873] Moreover, the analysis does not indicate that behavioural remedies in the form of

---

[865] But at least in the U.S., no clear tendency can be observed, see Kwoka/Valetti Ind. Corp. Chang. 2021, 1286 (1289).

[866] See Witt Antitrust Bull. 2022, 208 (228), referring to Google/Fitbit and Microsoft/LinkedIn.

[867] See Maier-Rigaud/Loertscher, CPI Antitrust Chronicles April 2020, p. 7: in mergers between 2004-2018, structural remedies remained constantly on a high level (about 80%), while behavioral remedies have only slightly increased.

[868] For an overview see Wilson, http://competitionlawblog.kluwercompetitionlaw.com/2020/02/21/merger-remedies-is-it-time-to-go-more-behavioural/?output=pdf (last visited 4.7.2022), p. 3.

[869] See Van Gerven et al., https://globalcompetitionreview.com/guide/digital-markets-guide/first-edition/article/data-and-privacy-in-eu-merger-control (last visited 4.7.2022).

[870] See Chen et al. RAND J. Econ. 2022, 3 (28).

[871] See NewsDesk, https://exbulletin.com/tech/978201/ (last visited 4.7.2022); Feasey/de Streel, Data Sharing for Digital Markets Contestability, CERRE Report September 2020, p. 40, stating that 'the Commission may prefer data siloing over data sharing to remedy some competition concerns when two data-rich are merging'.

[872] Rather sceptic Kwoka/Valetti Ind. Corp. Chang. 2021, 1286.

[873] See CMA, Merger remedy evaluations, 2019, paras. 1.4 and 1.5.

access or data separation have yet proven to work in the case of data-driven mergers. Rather, the evidence stands at the beginning,[874] and rather suggests to not make use of them.[875]

Doubts already concern the design an effective remedy, considering that the behavioural control runs against the natural interest of the firm, but also taking into account that non-discrimination clauses and setting the price in the frame of access requirements are a complex task.[876] What became apparent in the analysed cases is that the accepted data-elated remedies were part of a larger bundle of commitments, all addressing specific concerns of harm. This poses the risk of 'remedy fragmentation', meaning that behavioural commitments address different concerns with separate obligations, while being uncertain about the respective implementation and their future holistic effect on competition in digital markets.[877] The commitment practice appears even more troublesome given the unforeseeable, dynamic developments of digital markets. Ten years as the initial period of commitments in Google/Fitbit and Meta/Kustomer appears overly long, given that even the BMW/Daimler case shows that even within three years, markets can develop unexpectedly. Moreover, this practice reveals how the competition authority takes over the role of a regulator when enforcing and updating the commitments, de facto regulating particular markets or even fine steering the companies.[878] This appears troublesome, not the least because data access should be subject to holistic sectoral regulation in case of market failure and not be introduced through the tempting backdoor of merger control on a case-by-case occasion.

As a strong argument against behavioural remedies or at least the biggest challenge is effective monitoring and enforcement. This is held to be a 'daunting task in complex digital industries', and the consequence of enforcement failures is high, given that a data-driven merger that was approved some years ago cannot be undone.[879] The Australian Competition rejected the Google/Fitbit commitments,[880] not the least because it saw significant difficulties in effectively monitoring and enforcing compliance them.[881] The EU appears more confident in the viability of effective enforcement, considering that the EU Remedies Notice requires that workability of

[874] Such as Google/Fitbit and Meta/Kustomer; The BMW/Daimler commitments should not be overinterpreted, as the concerned a very narrow case and commitment.

[875] Ticketmaster case also illustrates the ineffectiveness of conduct remedies – albeit not the data-related ones.

[876] See Pittman, CPI Antitrust Chronicles April 2020, p. 3.

[877] Not the least if monitoring of the remedies only assesses the remedies in an isolated manner.

[878] See Picht in BeckOK Kartellrecht, 4th ed. 2022, § 40 GWB para. 68; critical in this regard Prepared Statement of Federal Trade Commission Acting Chairwoman Rebecca Kelly Slaughter before the Subcommittee on Antitrust, Commercial and Administrative Law of the Judiciary Committee United States House of Representatives, 18.03.2021.

[879] See Chen et al. RAND J. Econ. 2022, 3 (7).

[880] See Van Gerven et al., https://globalcompetitionreview.com/guide/digital-markets-guide/first-edition/article/data-and-privacy-in-eu-merger-control (last visited 4.7.2022); ACCC, Statement of issues – Google LLC – proposed acquisition of Fitbit Inc, 18.06.2020.

[881] See Waters, Google's $3b deal to buy Fitbit given workout by ACCC, 2020; as the transaction had been completed meanwhile, the matter remains an ongoing enforcement investigation in Australia, see ACCC, Google LLC proposed acquisition of Fitbit Inc, https ://www.accc.gov.au/public-registers/mergers-registers/public-informal-merger-reviews/google-llc-proposed-acquisition-of-fitbit-inc (last visited 4.7.2022).

commitments must be fully assured by effective implementation and monitoring, and that they do not risk leading to distorting effects on competition.[882] This goes for the lifetime of the commitment.[883] As has been shown, the Google/Fitbit acquisition heavily relies on monitoring trustee as well as on Sentinel as technical expert. Involving technical experts is held to be well-suited for resolving technical issues or issues which require expert knowledge, which is especially the case in access remedies,[884] but it has been done rather rarely so far.[885] Depending on the functions assigned to the expert, this can also substitute arbitration.[886] Sentinel faces challenges for mastering the task, such as advancement of technical requirements, privacy and complaints.[887] Nevertheless, the information asymmetry between enforcers and companies provides high potential for circumvention and ineffective enforcement, while its negative consequences cannot be easily reversed.

For these reasons, competition authorities should treat data-related merger remedies in form of behavioural commitments with utter caution and rather abstain from 'experimenting' in this regard. This is especially true for data access and interoperability obligations, which naturally run against the interest of the merged entity. As for data separation commitments, it appears particularly troublesome that in Google/Fitbit indeed Google will remain as the holder of the data but commits to not using the data for particular purposes. Commissioner Vestager has expressed that such remedy would come closer to a structural than to a behavioural remedy, as she calls it a 'quasi-structural' remedy, which is guaranteed by technical solutions.[888] However, this view tends to overlook the problem of such data separation, which is that 'the dominant tech companies have the very properties that makes rules and remedies less likely to work'.[889] A separation commitment would only approximate structural remedies (and therefore worth being considered) if the data as such is held by an independent third party and made available to Google for specific designated purposes.[890] In this regard, fully separated data intermediaries[891] as data holders can mitigate some concerns, especially, if they are able to control that Google indeed only uses that data for the legitimate purposes. In this case, they could lower information asymmetries and discretion for anti-competitive conduct of the merging entities, and that transaction costs are lowered because technological solution and

[882] See OJ 2008 C 267, 1 para. 17.

[883] See Van Gerven et al., https://globalcompetitionreview.com/guide/digital-markets-guide/first-edition/article/data-and-privacy-in-eu-merger-control (last visited 4.7.2022).

[884] See Vande Walle, Remedies in EU Merger Control – An Essential Guide, Working Paper (12.05.2021), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3782333 (last visited 4.7.2022), p. 84–85.

[885] Overview in Id., p. 84–86.

[886] See Id., p. 85

[887] See NewsDesk, https://exbulletin.com/tech/978201/ (last visited 4.7.2022).

[888] Vestager, Defending competition in a digital age, Speech, Florence Competition Summer Conference, 24.06.2021.

[889] See Kwoka/Valetti Ind. Corp. Chang. 2021, 1286.

[890] See also Bourreau et al., Google/Fitbit will monetise health data and harm consumers, 2020, p. 9–10, who outline that more restrictions/more differentiated set of restrictions might be necessary. But they ultimately reject that remedies should be imposed at all.

[891] This would reach beyond the DGA's requirement of structural unbundling.

monitoring are put 'in the same hand'. However, it remains a case specific and open question to what extent this is viable in terms of technical governance and whether this would still incentivise the merger.

(3) Consequences for the legal framework

What are the implications for the advancement of the legal framework? In general, remedy practice lies within the discretion of the competition authorities within its mandate, and the European Commission would be free to abstain from such practice in future. In contrast, German merger legislation does explicitly prohibit the Bundeskartellamt to accept behavioural commitments which would subject the conduct of the undertakings concerned to continued control, such as in Meta/Kustomer and Google/Fitbit.[892] As for data separation, the hurdles should be high in a sense that a commitment to separate the data holding should only be regarded as a structural remedy, if the data itself is solely held by an independent third entity. In that case, such commitment could be considered as legitimate under German law, while it would be feasible under the current EU merger regime without doubts.

Nevertheless, the legislature should consider going a step further. In fact, the possibility and practice of accepting behavioural commitments can take away negotiating power from the competition authorities, as it has to be considered as a proportionate measure vis-à-vis blocking the merger as the 'safe' option. This is particularly problematic in case of acquisition by big tech players, where the risks of failing behavioural commitments are considerably high due to the systemic relevance of potential tipping and monopolization. Moreover, data access obligations aim to establish a level-playing field. However, this presumes that other companies would have capabilities to analyse the data compared to the big tech acquirer. This is often not true in reality,[893] but insufficiently taken into account when accepting the commitments.

For all these reasons, the legislature could demand that behavioural commitments may not be accepted in data-driven mergers that involve big tech players. Such prohibition could become a building block of a merger regime specifically designed for and linked to gatekeepers under the DMA and undertakings of paramount significance for competition across markets according to § 19a GWB (see ee(1)). This does not contradict the finding that behavioural commitments appear more likely to be accepted and successfully implemented in regulated industries where a government body can monitor market conditions.[894] While indeed the DMA and § 19a GWB are about to establish such regulatory environment for gatekeepers, which may also increase likelihood of successful monitoring of behavioural commitments, the context of merger review – as opposed to abuse of dominance scenarios – must not be overlooked: it is about the risk of enabling the strengthening of an already dominant market position or increasing the likelihood

[892] § 40(3) S. 2 GWB.

[893] See Bourreau et al., Google/Fitbit will monetise health data and harm consumers, 2020, p. 3.

[894] See Wilson, http://competitionlawblog.kluwercompetitionlaw.com/2020/02/21/merger-remedies-is-it-time-to-go-more-behavioural/?output=pdf (last visited 4.7.2022), p. 2.

of market tipping, while not being able to properly unwind the approved merger with all its negative consequences on competition and innovation. In such cases, the legal framework on merger review should not allow to risk underenforcement.

cc) Insufficiency of Notice and Referral under Article 22 EUMR/Article 14 DMA

It is doubtful whether national referrals to the European Commission under Article 22 EUMR are legitimate in cases where a transaction would not be notifiable under national and EU legislation. This question is currently pending before the General Court.[895] But regardless of the outcome, this approach seems not optimal because it ultimately leaves enforcement practice to the eagerness of the Member States to refer the case. The practice of the Bundeskartellamt to abstain from below-threshold referrals exemplifies that merger enforcement is then left with fragmentation and rather arbitrary outcomes. Moreover, the approach does not appear sufficient, because it does not change the legal standard of review but just broadens the scope of case that come under scrutiny.[896]

For a similar reason, the effect of Article 14 DMA should not be overestimated. On the one hand, it may provide relevant information on the transaction of gatekeepers to national authorities and increase transparency. Ideally, Article 14 DMA enables to control a merger and also increase the awareness for 'killer acquisitions' at an early stage. However, on the other hand Article 14 DMA presupposes the legitimacy and eagerness of national authorities to refer non-notifiable mergers under Article 22 EUMR. Moreover, it also demands all referral requirements of Article 22 EUMR to be met, while it eventually does not affect the substantive standard for review.[897]

dd) Limited potential of revising national thresholds for merger review

Not the least when considering the context of the referral procedure, (further) lowering the national merger thresholds would not only be a means to extend the scope of cases that would fall under national merger review, but it would also open up the possibility to refer the cases to the European Commission under Article 22 EUMR. The German legislator could pursue this way and enquire into decreasing the threshold e.g. down to EUR 200 Mio. transaction value,[898] which is already the case in Austria.[899] However, it remains open to what extent indeed critical transactions would be covered that have so far been under the radar of competition authorities.

---

[895] Case T-227/21 – *Illumina v Commission* (pending).

[896] Also the EP does not see it as sufficient and calls for clarification as to its applicability, see European Parliament, Competition Policy – annual report 2021, P9_TA(2022)0202, 05.05.2022, para. 64.

[897] There were valid concerns that the DMA would lack competence in doing so, for an assessment see Franck/Monti/de Streel, Article 114 TFEU as a Legal Basis for Strengthened Control of Acquisitions by Digital Gatekeepers, 2021.

[898] Alternatively, the transaction value threshold could be reduce to 100 Mio to collect more case evidence, and could then be raised again once the knowledge base has increased.

[899] See Podszun, Stellungnahme, „Digital Markets Act", Bundestag Wirtschaftsausschuss, 27.04.2022, p. 15.

The effects of the 9th amendment do not bear any indication: while they extended the scope of cases under scrutiny of German merger control,[900] only four of them concerned the tech sector from 2017-9/2020,[901] and there were neither phase-2 cases nor was any merger blocked or identified as 'killer acquisition'.[902] While further lowering the threshold could be a reasonable means to generate more evidence, it would not have an impact on the substantive criteria for merger review.

ee) Advancing substantive criteria for merger review in Germany

(1) § 19a GWB within the EU context

As the analysis revealed, such mergers are of particular interest in which the source of data is the interaction with existing and potential customers[903] and machine generated data such as location data.[904] Unlike rather clear-cut data-related cases which refer to dataset providers and information services,[905] these cases of data-driven mergers have been performed by undertakings which are highly likely to be covered by § 19a GWB, so that the relevant of § 19a GWB becomes apparent in this context. The common denominator are the economic criteria outlined in § 18(3a) GWB, which are relevant for designating undertakings as of paramount significance for competition across markets under § 19a(1) GWB. Therefore, this analysis enquires into the potential and means to advance substantive criteria for merger review in Germany within the scope of § 19a(1) GWB. The relationship to EU merger review and will be addressed subsequently (under ff).

(2) Substantial Aspects

Within the frame of § 19a GWB, the substantive test for a more effective merger enforcement could be adjusted and would therefore enable stricter and more targeted enforcement. It would follow a specified enquiry about the positive and negative effects on competition and innovation in data-related mergers.[906] In this regard, various aspects have been discussed, but for putting them into legislation, they would need more evidence and conceptual refinement. In addition to the harder stand on remedies as outlined above, the legislator could consider some of the following issues:

As for the theory of harm, it is important to enquire into the details of how data are and could be used by the merged entity and to understand the cross-market, meaning conglomerate effects

[900] See Bundestag publication 19/26136.

[901] See Id., p. 4.

[902] See Id., p. 5.

[903] Such as in Facebook/Whatsapp, Microsoft/LinkedIn, Apple/Shazam and Google/Fitbit.

[904] See Google/Fitbit.

[905] Such as Dun & Bradstreet and Thomson/Reuters.

[906] See Bourreau/de Streel, Big Tech Acquisitions – Competition & Innovation Effects and EU Merger Control, 2020, p. 8–13.

of data-driven mergers. Economic evidence stands just at the beginning[907] and appears very case specific.[908] For identifying potential harms and the loss of potential competitive restraints, an assessment is needed how the merger would change the incentives and abilities to compete of those companies who are left in market.[909] In this frame it is challenging to identify the strategy, e.g. whether the acquisition is undertaken to reinforce and increase market power by adding new functionalities to already existing products rather than generate synergies or enter new markets.[910] For understanding, which role data play in this respect,[911] an overarching view is needed, asking for the effects the merger would have on the whole 'ecosystem', while an overly segmented view on defined markets of conventional merger review runs the risk to overlook impediments of competition. Another issue is how the assessment treats alternative sources of the data and substitutability.[912] This was decisive for some of the analysed decisions on data-driven mergers as well as the question is pertinent whether data have already been traded prior to the merger.[913]

To take such broader view into account, the current application of the SIEC-test would need some modification. In particular the legislature would have to specify the standard that must be met for clearing or blocking the merger. As for the measure of prohibition, it is key to determine the circumstances under which a 'significant' impediment is presumed, and a dominant position is found to be strengthened. While the legal standard of the SIEC-test is generally controversial, the test within the frame of § 19a GWB would put more emphasis on the scale of potential harm of a merger in addition to the probability.[914] Regarding data access in particular, the legislature could consider two options. As first option, one could presume a merger to pose impediments to effective competition (and therefore to be blocked) if it enabled an undertaking under § 19a GWB to acquire more or new data, or if it would make data collection more efficient. This presumption could be based on the observation that for such undertakings data may function as 'general-purpose input', which generally increase their discriminating power.[915] It would also account for the observation that in many cases initial short-term consumer benefits that are visible (e.g. lower prices) are driven by the undertaking's pricing strategy to increase the data

[907] See Chen et al. RAND J. Econ., 2022, 3 (9).

[908] See Motta/Peitz Inf. Econ. Policy 2021, 100868, p. 30 (of the pre-published working paper), on the theory of harm with regards to conglomerate mergers and the collection of data.

[909] See Sousa/Pike CLPD 2020, 26 (29).

[910] See Gautier/Lamesch Inf. Econ. Policy 2021, 100890, p. 29–30 (of the pre-published working paper), who identify this in the majority of cases, however also pointing to limitations of their empirical analysis.

[911] See also Graef in: Moore/Tambini, Digital Dominance – The Power of Google, Amazon, Facebook, and Apple, 2018, p. 71, 85–88, pointing to the relevance of the value sort of data involved, availability, the role and scale in machine learning.

[912] On the closeness of substitution between big datasets, which requires an extended assessment, MaierJECLAP 2019, 246; Graef in Moore/Tambini, Digital Dominance – The Power of Google, Amazon, Facebook, and Apple, 2018, p. 71, 85.

[913] See De Corniére/Taylor, CEPR Discussion Paper No. DP14446, p. 24–25, arguing that a key determinant of the effect of the merger on consumer surplus is whether data can be traded in absence of the merger.

[914] See Furman et al., Unlocking Digital Competition, 2019, p. 100–101; on the discussion of the expected harm test, see OECD, Start-ups, Killer Acquisitions and Merger Control, 2020, p. 42–43.

[915] See Bourreau et al., Google/Fitbit will monetise health data and harm consumers, 2020, p. 2.

scale of the acquirer rather than passing on efficiency gains onto consumers.[916] A second, more differentiated presumption would be particularly sceptic to acquisitions that involve services/products that complement each other. It has been argued that especially if the consumption synergy is high between using the product from one market and the other market (now both under the umbrella of the merged entity), the likelihood of monopolization of both markets (by foreclosure) is higher, so that blocking the merger would be reasonable.[917]

Corresponding with the modified substantive test, the burden of proof would need adjustment. Several commentators have suggested to shift the burden of proof in the context of tech mergers[918] to mitigate the information asymmetries between competition authorities and merging entities and ultimately making it easier for competition authorities to block a merger.[919] Especially in cases one of the merging parties has an entrenched dominant position (and therefore § 19a-cases), it would require the merging parties to provide evidence that the merger does not raise any significant competition issue or that expected efficiency gains are sufficiently large.[920] The legislature should take up on this, but for making it operable, a more differentiated approach is worth being considered to be applied in practice.[921] The concrete design would depend on the substantive changes to merger review that would have to be made regarding undertakings under § 19a GWB.

(3) The § 19a GWB nexus

Introducing modified merger review for undertakings covered by § 19a GWB requires thorough legislative integration into the fabrics of the GWB. New sections that would modify the standard of merger review could be introduced in §§ 35 et seq. GWB, e.g. a provision as new § 35(1b) GWB on the local nexus and threshold, modifications of the SIEC test as new § 36(4) GWB (also addressing the standard and burden of proof and the de minimis clause), possible modifications to the notification procedure under § 39 GWB, etc.

These amendments should correspond with a general clause added to § 19a GWB, which refers to these modifications. In this frame, the legislature has to decide, whether the modified merger review would need an additional decision of the Bundeskartellamt under § 19a(2) GWB to be 'activated' or whether the modified rules would directly apply to all mergers of undertakings declared as of paramount significance for competition across markets under § 19a(1) GWB. The latter seems preferable, because the merger review procedure itself gives the competition

---

[916] See Chen et al. RAND J. Econ., 2022, 3 (28).

[917] See Id., 23.

[918] Or also more general with particular respect to killer acquisitions.

[919] See e.g. proposals to shift the burden of proof by Parker/Petropoulos/Van Alsytne Ind. Corp. Change 2021, 1307 (1328–1330); Valletti, https://www.promarket.org/2021/06/28/tech-block-merger-review-enforcement-regulators (last visited 4.7.2022); Stigler Committee on Digital Platforms, Final Report, 2019, p. 111.

[920] See Motta/Peitz CLPD 2020, 19 (24); Stigler Committee on Digital Platforms, Final Report, 2019, p. 111; with regards to the reform in Germany Podszun, Stellungnahme, „Digital Markets Act", Bundestag Wirtschaftsausschuss, 27.04.2022, p. 15.

[921] Proposed by Sousa/Pike CLPD 2020, 26 (32–35).

authority the opportunity to examine the proposed merger, while the company can assert its rights and take legal action if needed within this procedure.

The challenge is to make it operable for the competition authority, while providing sufficient legal certainty to the undertakings.[922] While the legislature would have to address the substantial aspects, it is advisable that the Bundeskartellamt provides guidance to the affected undertakings.[923]

ff) Merger Review in the EU

A tightening of the German merger review standard would not be a substitute for needed reform of EU Merger Review. Such ambitious endeavour should be pursued at the same time, not the least considering that the U.S. has taken up on the policy debate with full fledge. The diverging approaches and practices between European make cooperation and the quest for EU-wide solutions a necessity. This is even more the case for data-driven mergers, because given the possible cross-market relevance of data, allowing the merger in one jurisdiction can also have an effect on markets in other jurisdictions on which the merger has been blocked. It can be agreed with the European Parliament, which has urged the European Commission 'to take a broader view when evaluating digital mergers and to assess the impact of data concentration'.[924] However, it is not supplemented by suggestions, how to do that.

An open question is the nexus to gatekeepers under the DMA. The agreed solution on the DMA does not affect substantial merger review. Therefore, new solutions could now be found without the pressure to accommodate it within the framework of the DMA under a questionable legal basis.[925] The EU legislature still has the possibility to design rules on merger review which particular refer to gatekeepers under the DMA. In substance, Article 14(1) DMA has already recognised the significance for mergers if they 'enable the collection of data'. This would need further elaboration. Ideally, merger reform in the EU would address substantial review as such, including the relationship with national rules and notification thresholds,[926] and it would also require an update of the Merger Guidelines. However, such reform would reach far beyond the questions of data-driven mergers and digital markets, and take considerably more time, critical analysis and consultation before implementation. In this respect, tightening merger review in

[922] On approaches see Nazzini/Carovano CLPD 2020, 44.

[923] Such as on merger thresholds, see Bundeskartellamt/BWB, Leitfaden Transaktionswert-Schwellen für die Anmeldepflicht von Zusammenschlussvorhaben (§ 35 Abs. 1a GWB und § 9 Abs. 4 KartG), 2022.

[924] See European Parliament, Competition Policy – annual report 2021, P9_TA(2022)0202, 05.05.2022, para. 65.

[925] The question is the also not burdened with the question about the right legal competence under Article 114 AEUV, see Franck/Monti/de Streel, Article 114 TFEU as a Legal Basis for Strengthened Control of Acquisitions by Digital Gatekeepers, 2021.

[926] See also Crémer/de Montjoye/Schweitzer, Competition Policy for the Digital Era, Final report, 2019, p. 113–116; Gautier/Lamesch Inf. Econ. Policy 2021, 100890; European Parliament, Competition Policy – annual report 2021, P9_TA(2022)0202, 05.05.2022, para. 67; Bourreau/de Streel, Big Tech Acquisitions – Competition & Innovation Effects and EU Merger Control, 2020, p. 15; Motta/Peitz Inf. Econ. Policy 2021, 100868, p. 34 (of the pre-published working paper).

the Member States within the well and narrowly defined scope of § 19a GWB could also generate more evidence that is ultimately valuable for a major reform of merger review on the EU level.

4. DMA/§ 19a GWB

a) DMA

The DMA is about to be passed. In the months and years to come, much will depend on its effective implementation. While this is true for many of the Articles 5-7 DMA-obligations, questions regarding an effective implementation of the data-related obligations figure prominently. What is more: apart from Article 5 No. 2 DMA (restrictions on data use and combinations in the absence of user consent), all the data-related obligations are set out in Article 6 DMA and are therefore 'susceptible' – and arguably in need – of being further specified.[927] This is true, in particular, for the data portability and data access obligations in Articles 6 No. 9 and 6 No. 10 DMA. Both provisions call for an effective implementation of the relevant obligations: when it comes to data portability (Article 6 No. 9 DMA), the data shall be made available "in a format that can be immediately and effectively accessed by the end user or the third party authorised by the end user", and measures must be taken such that continuous and real time data portability is provided in high quality (Recital 59). As far as the business users' access to 'their' data is concerned (Article 6 No. 10 DMA), gatekeepers must "ensure the continuous and real time access to these data by means of appropriate technical measures, such as for example putting in place high quality application programming interfaces (APIs) or integrated tools for small volume business users" (Recital 60). Also, they must enable business users to obtain consent from their end users for data access and data retrieval. Both provisions thereby require gatekeepers to act pro-actively and to consider and integrate data portability and data access in the design of the platform service (data portability and data access 'by design' – see also Recital 65: 'compliance by design'). But neither of these norms specifies the format in which and the interface through which data portability or data access are to be provided.

The same applies to Article 6 No. 11 DMA, which requires that gatekeepers who have been designated as providing online search engines as a core platform service provide fair, reasonable and non-discriminatory access to ranking, query, click and view data: what exactly FRAND access to data may mean in the context of the DMA remains an open question.[928] Further, the recitals to the DMA explain that the gatekeeper must anonymise the data "without substantially degrading the quality or usefulness of the data" (Recital 61), but with no further specification of how this is to be done. A difficult balancing exercise may be required in this regard to the

[927] Article 5 DMA sets out those obligations which the European Commission considers to be sufficiently clear such that they can be implemented without further guidance. By contrast, Article 6 DMA lists those obligations which are 'susceptible of being further specified'.

[928] On this see: Picht/Richter GRUR Int. 2022, 395 (397 et seq.) who call for best practice guidance for a procedural approach towards FRAND cutting across the various recent EU data regulations and for the development of a 'FRAND-supportive institutional structure'.

extent that anonymization affects the usefulness of the data to draw relevant information from the dataset.

In a first phase, the designated gatekeepers themselves will have to define conditions of access, including technical specifications that they consider effective in achieving the twin goals of the DMA – contestability and fairness – and must report these specifications to the European Commission (Article 11 DMA and Recital 68). In any case, data portability and data access will need to be fair, reasonable and non-discriminatory (FRAND) (Recital 62), and these fundamental principles of access will need to be integrated, as much as possible, into the technological design of the service (Recital 65). Gatekeepers must not try to circumvent their obligations, including by technical restrictions of access or by manipulative designs when it comes to consumer choice (see also: Article 13 DMA and Recital 70). As disputes between gatekeepers and platform users about compliance with the DMA obligations are foreseeable, gatekeepers shall provide for "a Union based alternative dispute settlement mechanism that should be easily accessible, impartial, independent and free of charge for the business users" in their general conditions (Recital 62).

Arguably, fundamental decisions on the specifications and terms of data portability and data access cannot be left to private enforcement alone, however. They are inextricably linked to the overarching goals of the DMA which must be achieved effectively, and, at the same time, in a proportionate manner (Article 8(7) DMA). With a view to the obligation of online search engine providers to grant access to ranking, query, click and view data, the European Commission shall assess, in particular, whether the measures intended or implemented by the gatekeeper are fair and do not confer an advantage on the gatekeeper (Article 8(8) DMA).

According to Article 8(2) DMA, the European Commission may, on its own initiative or upon request by a gatekeeper, open proceedings to specify the measures that gatekeepers have to implement in order to effectively comply with an obligation under Article 6 DMA, including the obligations to grant data portability and data access. Such proceedings will involve a dialogue with the gatekeeper (see Article 8(5) DMA), but also a consultation with third parties (Article 8(6) DMA and Recital 65). Simultaneously, Article 46(1) lit. b DMA empowers the European Commission to adopt implementing acts that lay down the "form, content and other details of the technical measures that gatekeepers shall implement" in order to comply with Articles 5, 6 or 7 DMA. While it remains at the discretion of the European Commission whether specifications shall be provided under Article 8(2) or under Article 46(1) DMA (Recital 65), the recitals to the DMA highlight that the implementation of 'some of the gatekeepers' obligations such as those related to data access, data portability or interoperability could be facilitated by the use of technical standards, and that the European Commission may request European standardisation bodies to develop them (Article 48 DMA and Recital 96).[929] Indeed, the involvement of the European standardisation bodies may be called for: ultimately, the data-

[929] Baschenhof, The Digital Markets Act (DMA): A Procompetitive Recalibration of Data Relations?, 2021, https://ssrn.com/abstract=3970101 (last visited 4.7.2022), p. 20 argues in favour of a standardization of the data format and mechanism.

access related DMA obligations are geared towards developing and rolling out fundamental technical infrastructures, including appropriate data formats and standards for data transfer, including the relevant interfaces. This endeavour is closely intertwined with the EU's broader data strategy. The data formats and standards for data transfer that will be established as part of the implementation of the DMA are bound to affect technical choices made elsewhere. Developing data portability and data access standards in particular should therefore be part of a broader endeavour that cuts across the various data-related regulations that have recently been passed or are currently being considered.[930]

While it is important for the European Commission to be involved and to make sure that the relevant decisions are taken with the goals of the DMA in mind – ensuring contestability in particular – there are reasons to believe that the relevant standards should not be set by the European Commission itself. Rather, they should be developed in an open process that involves all the relevant stakeholders.[931] The European Commission will have to ensure that the process remains open and fair, and is not dominated by the interests of the gatekeepers. Also, it is essential to ensure that the standards remain open to adaptations over time. The data economy is still in an early phase. There is a real risk of it becoming locked into inferior and even inefficient standards.[932]

Another important risk of the DMA regime is that it will overstrain the enforcement resources of the European Commission. The DMA tries to address this concern by requiring changes to the internal corporate governance of the gatekeepers, namely the establishment of an internal compliance function that is separate from the operational functions of the gatekeeper and cooperates with the European Commission (see Article 28 DMA).

These different dimensions of the DMA's enforcement regime point to one core question: what regulatory style should the European Commission adopt when enforcing the DMA? Since the entry into force of Reg. 1/2003, EU competition law enforcement has followed an adversarial model.[933] When it comes to the European Commission's enforcement powers, the DMA adopts and partly expands the core provisions of Reg. 1/2003. On the other hand, it includes a number of provisions that point towards a more cooperative and conversational model. Each regulatory model comes with its own strengths, weaknesses and risks. A conversational – instead of a 'legalistic' – model may be essential in order to soften some of the potentially inefficient and counter-productive inflexibilities inherent in the DMA. As Julia Black has highlighted, it

[930] For a similar thought see Picht/Richter GRUR Int. 2022, 395 (396).

[931] See also: Picht/Richter GRUR Int. 2022, 395 (397) who call for an 'inclusive bottom-up approach which is targeted to the relevant stakeholders and conducted with an overarching view on a variety of actual and potential cases'.

[932] See also Picht/Richter GRUR Int. 2022, 395 (396) who emphasize the need for a 'balance between flexibility and specification'.

[933] For the hypothesis that Europe has moved towards a model of 'adversarial legalism' that was initially a distinctive feature of the American legal and regulatory style, see: Kagan Oxf. J. Leg. Stud. 1997, 165; Kagan Regul. Gov. 2007, 99.

requires significant regulatory resources of time, information and expertise on the other hand.[934] When it comes to information, gatekeepers will have a natural advantage.[935] Also, the risk of regulatory captures may increase. Much attention will therefore need to be given to design the regulatory structure – beyond the provisions that the DMA entails.

Finally, the potential role of data intermediaries in the implementation of the DMA should be considered. Both in the context of Article 6 No. 9 DMA (data portability) and of Article 6 No. 10 DMA (data access for business users), they may come to play a relevant role[936] and have a potential to bundle and defend the interests of end and business users in an effective enforcement (for a more detailed discussion of the role of data intermediaries see part F(IV)).

Beyond the issues relating to the implementation of the data-related obligations of the DMA, the question remains to what extent these obligations will contribute to increasing the contestability of the market position of the gatekeepers, to 'levelling the playing field' when it comes to competition on neighbouring markets or to addressing the concerns related to advertisement-driven platform business models. There are reasons to believe that the contribution will be real, but modest. End users (Article 6 No. 9 DMA) and business users (Article 6 No. 10 DMA) will have access only to those data generated based on their own activity. The gatekeeper, on the other hand, will have access to the whole of the data trove. Given the economies of scale and scope in data analytics, this may amount to a huge competitive advantage. The competitive advantages increase with the ability to experiment with data analytics, including AI.

Also, while the DMA starts to tackle competition problems in online advertising markets, this can only be a start. The requirement in Article 5 No. 2 DMA to obtain consent from end users when combining different data from different sources may even create additional incentives to cross-market services that come with some sort of benefit for end users and induce them to consent. A more far-reaching requirement – e.g. to combine different datasets and to cross-use data in different markets only if the gatekeeper agrees to grant access to those data on equal terms also to competitors – may be needed.

It is not to be expected that the DMA will be amended along those lines soon, however. Possibly, the European Commission will test some more pro-active approaches based on EU competition law. In some sectors, more far-reaching sector-specific rules may be forthcoming and provide a useful testing ground.

---

[934] Black, Rules and Regulators, 1997, p. 42.

[935] The DMA partly tries to counter these by endowing the Commission with broad powers of inspection, including a right to 'require the undertaking … to provide access to and explanations on its organisation, functioning, IT system, algorithms, data-handling and to record or document the explanations given' – see Article 23(4) DMA. The duty of the compliance officer to cooperate with the Commission (Article 28 DMA) may be another one.

[936] See also Picht/Richter GRUR Int. 2022, 395 (398, 399-400): Data intermediaries could 'provide technical infrastructure, organize data pooling and interoperability as well as negotiate and implement FRAND transaction conditions'.

In some respects, national competition law may usefully 'experiment' with new horizontal solutions.

b) § 19a GWB

The questions raised by § 19a GWB somewhat differ from the question of how to ensure an effective implementation of the DMA. This is due, in particular, to the different design and goals of the § 19a GWB-regime. Under § 19a GWB, the Bundeskartellamt retains a significant degree of flexibility to tailor remedies to the specific competition problems that any norm addressee and any given service provided by it may raise. Given that § 19a GWB – contrary to the DMA – remains competition law proper, the Bundeskartellamt will therefore have to define and substantiate a specific risk to competition before it imposes a specific obligation. § 19a GWB does lower the threshold of intervention, but the Bundeskartellamt remains obliged to show a clear link between a plausible risk to competition and the remedy imposed.[937]

As far as the imposition of the data-related obligations foreseen in § 19a(2) GWB is concerned, this requirement will arguably be met easily, however. This is true for the imposition of a data portability obligation according to § 19a(2), 1st sentence, No. 5 GWB, as the absence of data portability is bound to impede multi-homing or the switching of end users to competing services[938] or of business users to competing platforms. But it is also true for the imposition of the data combination and use restrictions provided for in § 19a(2), 1st sentence, No. 4 GWB, which are meant to ensure end user choice (§ 19a(2), 1st sentence, No. 4 lit. a GWB) and to protect business users from appropriating business opportunities that they have developed (§ 19a(2), 1st sentence, No. 4 lit. b GWB).

In addition, the Bundeskartellamt will have to define the terms on which data portability must be granted. Whereas the data portability obligations under the DMA would seem to be geared towards the goal to establish a coherent, overarching data portability infrastructure for all gatekeepers, a Bundeskartellamt's decision under § 19a(2), 1st sentence, No. 5 GWB would need to react to specific competition concerns in a given context. Obviously, the constitutional law principle of equal treatment (Article 3 GG) applies, and the Bundeskartellamt should strive to develop a coherent set of principles. Nonetheless, § 19a(2) GWB-decisions are to react to context-specific risks to competition which may differ and require differentiated reactions. Whereas Article 6 No. 9 and Article 6 No. 10 DMA require continuous and real-time data portability across the board, a competition law analysis may suggest differentiated requirements service by service.

No § 19a(2) GWB-decisions have been issued so far. The procedures to be followed in specifying the conditions of data portability, for example, still need to be developed. The

[937] See Schweitzer in Immenga/Mestmäcker, GWB, 7. Aufl. 2022, § 19a Rn. 130 et seq.

[938] Bundestag publication 19/23492, p. 77.

Bundeskartellamt, too, will have to give thought to the enforcement style to be used. The commitment decision procedure (§ 32b GWB) may frequently provide a role model. Stakeholders affected by these conditions will need to be heard.

An obvious question for the German legislator is whether to amend the § 19a(2) GWB-list of possible data-related prohibitions or obligations in the future.

The possibility to impose an obligation to business users access to the data generated by their offer – similar to Article 6 No. 10 DMA – could be an obvious candidate. One may wonder, however, whether such an obligation is still necessary once the DMA has entered into force. Its practical relevance would then be limited to the gaps left by the DMA. For example, Article 6 No. 10 DMA will only apply to the core platform services identified in the designation decision under Article 3 DMA. In some circumstances, an effective protection of competition may justify the expansion of such a duty to other services provided by a norm addressee. Also, § 19a GWB may, in the future, be applied to undertakings that are not covered by the DMA.

Another possibility would be to oblige norm addressees who combine different datasets or cross-use data in different markets to provide access to those data to competitors on non-discriminatory terms. Data access obligations of this kind have already been implemented in the frame of merger commitments in BMW/Daimler and Google/Fitbit (see part E(IV)(2)(c) above), which may more generally inform the further conceptualisation of such obligations. The issue of a non-discrimination policy when it comes to the collection of data has recently been raised in the context of changes of 'app tracking policies' by both Google and Apple.[939]

Finally, there is a question whether the Bundeskartellamt should be empowered to impose access to data obligations also in 'scenario 2'-settings, i.e. in settings where an undertaking which has played no role in the generation of the relevant data and which has not been authorised by a data co-generator requests access to bundled individual level or aggregate data of a § 19a GWB-norm addressee in order to effectively compete on complementary markets, e.g. markets for mobility-related services. Given the competitive advantages the norm addressees have in collecting competitively relevant data and the competitive advantages that follow from these data troves across markets, there may be strong reasons to include 'data access scenario 2' into the list of obligations that the Bundeskartellamt may impose under § 19a(2) GWB: the denial of access to bundled individual level data or aggregate data to (potential) competitors who have not contributed to the generation of the data may be precisely one of those anti-competitive strategies with cross-market potential that § 19a GWB strives to capture.

[939] Google planned to remove third-party cookies on its Chrome browser and to replace their functionality with 'privacy sandbox'-tools. Apple has required app providers to obtain user permission for tracking through a pop-up window. See with further references Schweitzer/Gutmann in Jenny/Charbit, Competition Case Law Digest, 5th ed. 2022, p. 505. See also Geradin/Katsifis/Karanikioti, Google as a de facto Privacy Regulator: Analyzing Chrome's Removal of Third-party Cookies from an Antitrust Perspective, TILEC Discussion Paper No. DP2020-034.

However, in the implementation of § 19a GWB, it has to be kept in mind that – different from the DMA – this provision remains part of competition law proper. Even if somewhat more pro-actively than § 19 GWB, it strives to address market failures associated with a specific type of (cross-market) power. Its goal is not to address innovation system or transformation system failures more broadly (for these concepts see part D(I)).

III. Contract law

The European and German legislatures are well advised to further observe the markets for machine-generated and other data before any further legislative proposals in the field of contract law are considered. The main function of contract law is to help the parties with default rules for incomplete contracts.[940] Such default rules should reflect what reasonable parties would agree upon in a given situation. If the markets are not yet developed, as it is the case for the emerging European data markets, the legislature cannot rely on such majoritarian defaults, however.

But the recommendation to further observe the development of the markets does not mean that the European Commission and the German authorities should be inactive. The state can cooperate with the market actors in the development of best practices or soft-law instruments that can later be used as blueprints for default rules if they are proven by legal practice as sound templates for contracts. The Draft Data Act follows this approach in Article 34 which allocates the task of developing model contract terms to the European Commission. The European Commission has announced to cooperate with experts from legal practice. This approach will also have the positive side-effect to inform the European Commission about the current practices. However, one should not expect that this initiative will go beyond the scope of the Draft Data Act itself. For scenarios not covered by the Draft Data Act, namely scenarios 2 and 3 and for contracts on data collected during the use of services, it may be a reasonable policy option to initiate additional dialogue fora with the market actors and to support the development of best practices.

Any more far-reaching intervention into contractual freedom, especially any enactment of mandatory rules, should only by envisaged on the basis of a market failure analysis. As explained with more details above (part F(I)(2)), this approach should also be upheld after the re-allocation of access and usage rights by the DMA and the Draft Data Act. It is obvious that the DMA and Draft Data Act will not overcome all dysfunctionalities of data markets, not even within their limited scope of application. Data holders will uphold their data-related market power in many situations. But these imbalances of power should be primarily addressed by means of competition law. Contract law, by contrast, should only be used for interventions if

[940] See Savigny, System des heutigen römischen Rechts, Vol. 1, 1840, p. 58. On the prevailing theory on incomplete contracts in the current law and economics literature see Cooter/Ulen, Law and Economics, 6th ed. 2014, p. 283-86; Shavell, Foundations of Economic Analysis of Law, 2004, p. 299-301.

structural imbalances of power are pertinent. The empirical analysis presented in part D, however, has not verified such a structural imbalance, especially not with regard to machine-generated data where actors of different kinds and sizes may either collect and hold data-sets or be interested in getting access to those datasets.

The European and German legislature should therefore be cautious to use broad-brush arguments of imbalance of power as a justification for interventions. This holds also true for the questions of whether courts should be empowered to review standard terms and conditions of data access agreements in B2B scenarios.[941] However, such a review may still be justified on a different market failure analysis. Following the more recent economic analysis, a review of standard terms may be justified in scenarios where those terms are set aside as irrelevant 'small print' and not appreciated as a valuable feature of the product with the result that competitors do not compete over them ('lemon market').[942] Such a scenario is reasonably likely for data sharing agreements where the data-holder is under a legal obligation to grant data access and wishes to avoid or limit such data access by means of restrictive terms and conditions and where the other party is mainly interested in the product or service as such and does not spend much attention to the data collected by the product or service, especially in case of consumers or SMEs as users of the product or service. Article 13 Draft Data Act addresses this problem, see (part F(I)). The provision is drafted in a broad language and seems to cover all contractual terms "concerning the access to and use of data" irrespective of whether such access is based on Articles 4 or 5 Draft Data Act or on a different legal ground. Such an interpretation is also supported by Article 8(1) Draft Data Act which is expressly meant to be applicable beyond Articles 4 and 5 and refers in this regard also to Chapter IV. It is however not entirely clear if Article 13 is applicable only to data access based on legislation enacted after the Draft Data Act in accordance with Article 12(3). If Article 12(3) would be applicable on the review of standard terms under Article 13, such a review would not be provided for in the Draft Data Act for access agreements based on the DMA, competition law grounds or older sector-specific regulation. The scope of application of Article 13 should be clarified on the European level. For the German situation, we see no further need for action. § 310(1) BGB already today provides for a flexible instrument to review unfair standards terms in B2B data sharing agreements where this is necessary.

Another market failure that may justify further intervention concerns information asymmetries[943] between providers of products or services that are used to generate and collect usage and other customer data on one side and customers on the other side. Frequently, customers do not know what data is collected by the providers. This lack of information may

[941] But see Recital 54 Data Act.

[942] On the justification of a review of standard terms based on the „lemon markets" problem see Schäfer/Ott, Lehrbuch der ökonomischen Analyse des Zivilrechts, 5th ed. 2012, p. 552-558; see also Basedow in MüKoBGB, 9th ed. 2019, Vor § 305 paras. 4-8.

[943] For the classical economic analysis of information asymmetries see Fleischer, Informationsasymmetrie im Vertragsrecht, 2001, 175–177 and 1000–1001; Shavell, Foundations of Economic Analysis of Law, 2004, p. 332–334.

prevent users from requesting access to data or, where negotiations on data access are taking place, evaluate the possible usages and the actual or potential value of the respective data. The problem has already been taken up by the European legislature. Article 3(2) Draft Data Act obliges the seller or lessor of a product to provide the buyer or lessee of the product with information about the nature and volume of the data collection and further information. A similar approach has been implemented by Article 9 P2B Regulation[944] which provides that providers of 'online intermediation services' shall include in their terms and conditions a description of the technical and contractual access to any personal data or other data, or both, which business users or consumers provide for the use of the online intermediation services concerned or which are generated through the provision of those services. It should be considered to implement comparable transparency obligations for those scenarios that are not covered by the Draft Data Act and the P2B Regulation, most importantly for co-generated data which is generated by the use of a service. Although we do not recommend at the current stage to broaden the scope of application of the access rights of Article 4 and 5 Draft Data Act to services, see part F(I), we still suggest to introduce information duties for service contracts under which one party, the service provider, may use the service to collect data about the conduct of the customer, and the other party, the customer, has no access or knowledge about the collected data, e.g. if the provider of an ERP (enterprise resource planning) software collects data about the business processes of its customers to which the customer has no access. Such an information should ideally complement the already existing or proposed instruments on the European level, e.g. by amending the Draft Data Act, but it could also be introduced on the national level, e.g. as new paragraph of § 241 BGB.

IV. Data Intermediaries and the Data Governance Act (DGA)

1. Background

High hopes have recently been placed in data intermediaries as promising tools to promote data sharing.[945] Given this 'data intermediary hype', this section enquires into the actual prospects for data intermediaries in the context of competition and innovation policies. It asks what the conditions for and means to fulfil these promises are. This requires looking at the evolving legal framework which affects the incentives of data intermediaries and market actors. In particular, the section explores the obstacles for the establishment of data intermediaries, the context for their activities, and the necessary conditions to be set and complimentary measures to be taken to make them work. The overall goal is to discuss how the findings would translate into viable policy options to advance the regulatory framework that would contribute to an effective market design on access to data.

[944] OJ 2019 L 186, 57.

[945] Datenethikkommission der Bundesregierung, Gutachten, 2019, p. 133; Schallbruch/Schweitzer/Wambach, Ein neuer Wettbewerbsrahmen für die Digitalwirtschaft, Bericht der Kommission Wettbewerbsrecht 4.0, 2019; Bundesregierung, Datenstrategie – Innovationsstrategie, 2021, p. 33–35.

As a core piece of legislation, the EU legislature passed the Data Governance Act (DGA) on 16 May 2022,[946] which aims to foster the establishment of 'data intermediation services'. The general aspiration is that data intermediaries should improve the accessibility of data to promote innovation.[947] As a contribution to the establishment of an infrastructure for data sharing, the DGA is a legal framework that aims to improve the availability and use of data in the EU[948] through fostering the emergence of data intermediation services. Such services support and promote voluntary data sharing between companies as well as data sharing obligations,[949] and they are also considered as a means to challenge the positions of large platform operators,[950] to prevent unauthorised data access, and to protect against antitrust violations.[951] These purposes of data intermediaries are in the focus of this study.[952]

As a starting point, we specify what we understand as data intermediaries and on which ones we will focus and why (under 2). An outline of the actual development of markets for such data intermediaries follows (under 3). It is then crucial to look at the new legal framework in the EU, namely the Data Governance Act (under 4). To discuss policy options for further advancing the legal framework for data access with regards to data intermediaries, the final sub-sections address the uncertainty of the new market design for data intermediaries (under 5) and how to better integrate data intermediaries in the market order for data sharing (under 6).

2. Functions and definition of data intermediaries

a) Taxonomies and possible economic functions of data intermediaries

Scholars[953] and institutions[954] have put forward more than a dozen of taxonomies on data sharing in general (see further on different models for data sharing, part D(II)(2)(d)) and data

[946] OJ 2022 L 152, 1.

[947] Godel/Natraj, Independent assessment of the Open Data Institute's work on data trusts and on the concept of data trusts, 2019, p. 8.

[948] COM SWD(2020) 295 final, 1.

[949] See Recital 27 DGA.

[950] Bundesregierung, Datenstrategie – Innovationsstrategie, 2021, p. 35.

[951] See Wendehorst/Schwamberger/Grinzinger in Pertot, Rechte an Daten, 2020, p. 111.

[952] Notwithstanding that public and scholarly debate also discuss other functions, such as strengthening consumer's rights and allow them to participate in the commercial exploitation of their data. On the function to decrease asymmetries in information and bargaining power, Hardinges, Data trusts in 2020, https://theodi.org/article/data-trusts-in-2020/ (last visited 4.7.2022); see Wendehorst/Schwamberger/Grinzinger in Pertot, Rechte an Daten, 2020, p. 106, on the negotiating power of data trusts.

[953] See Wernick/Olk/von Grafenstein, Technology and Regulation, 2020, p. 65; Zingales, Data collaboratives, competition law and the governance of EU Data Spaces, 2021; Richter/Slowinski IIC 2019, 4.

[954] For the Commission COM SMART 2020/694, 36; OECD, Enhancing Access to and Sharing of Data: Reconciling Risks and Benefits for Data Re-use across Societies, 2019, p. 38; Pawelke, Daten teilen, aber wie? Ein Panorama der Datenteilungsmodelle, 2020.

intermediaries in particular. The designations they use refer to distinct organisational structures or functional relationships regarding data sharing, such as data spaces, data trusts, data marketplaces,[955] or data collaboratives.[956] In general, very different conceptualisations exist[957] and there is no clearly established terminology.[958] Simon et al. have identified 35 functionalities, which feature data intermediaries.[959] In addition, more abstract criteria for delineation were discussed, especially regarding the competitive relevance of data intermediaries' business models (e.g. ownership, openness, sector, remuneration, or number and nature of relationships).[960]

However, rather than such designations and criteria, what matters most are the economic functions which data intermediaries could take over. The reason why data intermediaries appear promising to policymakers is that they might solve different problems and overcome crucial market failures in the data economy. These intermediaries who perform a matching function[961] can bring together data holder and users, improve accessibility of data,[962] decrease information asymmetries regarding data and reduce costs of risk[963] for actors in the data ecosystem to share their data with another.[964] Furthermore, data intermediaries can reduce transaction cost e.g. by standardization and technical and contractual management of data transfers and enforcement of the agreed conditions.[965] Those data intermediaries which operate open platforms[966] can capture the value of network effects and pass them on to data holders and users if they can realise economies of scale and scope and network effects.[967]

These economic functions of data intermediaries are determinants for the competitiveness of data-related markets, and data intermediaries are actors who can arguably perform such

[955] See for various definitions in the literature Simon et al., Definition and analysis of the EU and worldwide data market trends and industrial needs for growth, 2021, p. 22–23.

[956] Used as a wide term by Zingales, Data collaboratives, competition law and the governance of EU Data Spaces, 2021.

[957] Kühling ZfDR 2021, 1 (4), also providing some background; for further background, see also Richter ZEuP 2021, 634 (640–642).

[958] COM SMART 2020/694, 40 e.g. differentiates between data marketplaces, industrial data platforms, data trustees, data collaboratives, data cooperatives and "Personal Information Management Systems" (PIMS).

[959] However, they use the term "data marketplaces" as general term for data intermediaries, see Simon et al., Definition and analysis of the EU and worldwide data market trends and industrial needs for growth, 2021, p. 34.

[960] See Richter/Slowinski IIC 2019, 4 (10 et seq.); Martens et al. JRC121336 (2020), 28; see also classifications of orientation and ownership in Simon et al., Definition and analysis of the EU and worldwide data market trends and industrial needs for growth, 2021, p. 28–29.

[961] Richter/Slowinski IIC 2019, 4 (13); COM SWD(2018) 125 final, 10.

[962] See COM SWD(2020) 295 final, 12.

[963] See COM SWD(2020) 295 final, 12; Richter/Slowinski IIC 2019, 4 (14–15).

[964] See Richter/Slowinski IIC 2019, 4 (13).

[965] See Martens et al. JRC121336 (2020), 29; COM SWD(2020) 295 final, 11.

[966] See Richter/Slowinski IIC 2019, 4 (11).

[967] See Martens et al. JRC121336 (2020), 15.

functions. Therefore – for the purpose of this study –, the term data intermediary will be defined broadly, as will subsequently be discussed. This allows to further differentiate when looking at data intermediaries in specific regulatory contexts and different legal areas.

b) Definition of data intermediaries and data trustees

In the context of this study, we follow a broad understanding by defining 'data intermediary' as an entity which enables and/or facilitates data sharing between data holders and data users. Data intermediary is therefore defined and used as an umbrella term, which presupposes that two criteria are fulfilled:

- (1) Separate entity/third party as separate *actor* in the data ecosystem: data intermediaries are defined as (possibly) independent entities and therefore as separate (third[968]) actors, which perform a distinct economic activity. Therefore, legal analysis can treat them as a separate party to a contract, for example they may be categorised as an undertaking under Article 101 TFEU and could possibly be held liable. In case of collaboration between different undertakings, at least a certain degree of independent organisation, such as a joint venture, is necessary. As a consequence, mere agreements between entities on data sharing (e.g. by agreeing on the legal, economic and technical terms) are *not* considered data intermediaries within the meaning of this study if there is no separate actor who would orchestrate or perform the data sharing.[969] Also mere technical interfaces as such (e.g. API), which enable for data sharing, are not considered as data intermediaries.

- (2) Enabling/facilitating data sharing between holders and users of data: the main function of a data intermediary is to enable and/or facilitate data sharing between data holders and data users. This often involves the establishment of infrastructure for the interconnection of data holders and data users.[970] 'Data sharing' means the provision of data by a data holder (a person or entity that supplies data[971]) to a data user for the purpose of joint or individual use of such data.[972] *Using* the data implies the technical processing of the data (e.g. transform it, merging it with other datasets, or feeding it into other systems for developing new insights, products or services).[973] Given this criterion, data escrowees, which restrict the use of data to avoid conflict with legal requirements (e.g. antitrust law

[968] See Kühling ZfDR 2021, 1 (5).

[969] Even though such agreements are obviously relevant under Article 101 TFEU.

[970] See also Article 10(a) and Recital 27 DGA.

[971] Data holder does not imply the legitimacy of the holder to share the data (unlike Article 2(8) DGA). The data holder may have legal or de facto control over the data.

[972] The term "data sharing" is used irrespective of its legal basis (e.g. voluntary agreements or Union or national law – as Article 2(10) DGA requires). Also, data sharing does not imply the nature of the arrangement (e.g. license), remuneration, or whether it is performed directly or through an intermediary.

[973] "Data user" does not imply the lawfulness of accessing and using this data (unlike Article 2(9) DGA). Also, "its own" does not imply the commerciality or non-commerciality of the purpose. The purpose (e.g. for business, academic work or in government) is context specific.

or data privacy/protection),[974] are not considered data intermediaries, as long as they do not intermediate data between data holders and data users. The same is true for mere privacy management tools (PMT)[975] and data cooperatives within the meaning of the DGA (see under 4(b)).

The breadth of the definition makes many other criteria irrelevant to the question as to whether an actor qualifies as data intermediary: first, it is irrelevant whether the data intermediary is open or not to include additional data holders and user (see under 4(b)). Second, data intermediaries can cover both personal- and non-personal data. Third, they can be organised as a commercial or non-commercial entity (see under 4(b)). Fourth, the definition does not distinguish whether the data intermediary covers voluntary or mandated data sharing.[976] Fifth, for the definition of a data intermediary it is irrelevant whether the data intermediary offers the services for remuneration. Sixth, it is also irrelevant if it acts only in its own interest (e.g. data brokers and marketplaces, or merely functional data pools) or owes a particular duty to consider the interests of data users/holders.

Nevertheless, these distinctions do become relevant for differentiated sub-categorisations (e.g. data trustee). Also, they inform the economic analysis, because they may become decisive when it comes to inquiring into distinctive use cases, business models and technical arrangements (e.g. what role remuneration plays). Some distinctions also have legal relevance, e.g. data protection law applies once personal data is involved, and its requirements considerably affect and explain data sharing related business models.[977]

With regards to data intermediaries, the term data trustee (also data trust or trusted intermediary/third parties[978]) is frequently used in different contexts and for various functions.[979] This study regards a large share of ‘data trustees’ as being a specific sub-group of data intermediaries, namely those ones which bear a fiduciary duty to act in the interest of the data holder (and sometimes also the data users[980]). This fiduciary duty may, for example, stem from an empowerment of the data trustee to make certain decisions on behalf of the data

[974] See ALI-ELI Principle for a Data Economy, Final Council Draft, 2021, p. 114; Specht-Riemenschneider et al. MMR-Beilage 2021, 25 (27).

[975] See ALI-ELI Principle for a Data Economy, Final Council Draft, 2021, p. 111; Specht-Riemenschneider et al. MMR-Beilage 2021, 25 (27).

[976] Originally, the Commission’s proposal of the DGA only covered voluntary data sharing, which has been criticized and amended accordingly.

[977] See Kühling ZfDR 2021, 1.

[978] See OECD, Enhancing Access to and Sharing of Data: Reconciling Risks and Benefits for Data Re-use across Societies, 2019, p. 38.

[979] On the genesis of the term ‘Data trust’ und ‘Datentreuhand’ and the strands of discussion, see Richter ZEuP 2021, 634 (641–642).

[980] Examples for ‘doppelseitige Treuhandverhältnisse‘ in Specht-Riemenschneider et al. MMR-Beilage 2021, 25 (35–36).

holder.[981] The legal nature and economic function of such fiduciary duty (e.g. best interest clause; mandates to exercise data rights on behalf of the data holder[982]) is not clearly determined and can be explored further in our study.[983] Also, such fiduciary duty does not exclude the possibility that the data trustee follows its own interests as well.

Some commentators reserve the term 'data trustee' for data intermediaries that cover personal data.[984] In fact, often the use cases for data trustees involve personal data, but it is not a necessary condition,[985] and therefore, we use the term data trustee regardless of the type of the data it handles.

The term 'data intermediary' is not to be confused with the legally recognised concept of 'data intermediation services' (DIS) according to the Data Governance Act (DGA). While there are substantial overlaps, not all DIS covered by the DGA can be held data intermediaries under the here proposed definition. The exact delineation and consequences for analysis are further elaborated below (under 4.).

c) Overview with examples

The following chart illustrates the relationship between 'data intermediaries', 'data trustees' and 'data intermediation services':

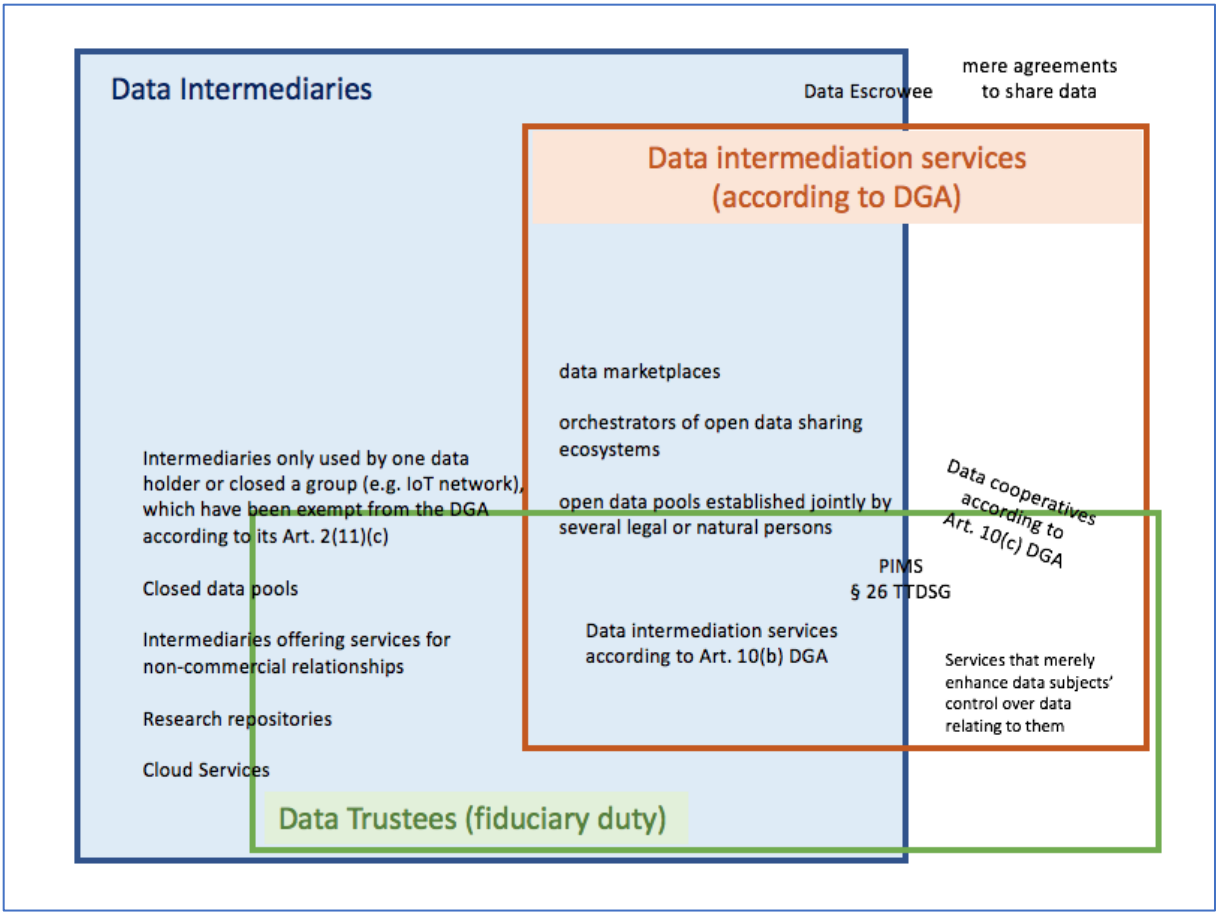
[981] See for a conceptualisation Fewer/Crothers/McPhail/Perrin, The Price of Trust? An Analysis of Emerging Digital Stewardship Models, 2020.

[982] See ALI-ELI Principle for a Data Economy, Final Council Draft, 2021, p. 111; Specht-Riemenschneider et al. MMR-Beilage 2021, 25 (28–29), primarily distinguishing between different purposes.

[983] On the legal uncertainty see Wendehorst/Schwamberger/Grinzinger in Pertot, Rechte an Daten, 2020, p. 103. E.g. Specht-Riemenschneider et al. MMR-Beilage 2021, 25 (35) argue that it must be main duty stemming from a contract, not ancillary duty, to act in the interest of the data holder.

[984] See e.g. Kühling ZfDR 2021, 1 (6).

[985] As a broader definition, see also ALI-ELI Principle for a Data Economy, Final Council Draft, 2021, p. 103–114; Specht-Riemenschneider et al. MMR-Beilage 2021, 25 (35).



3. Market developments

Looking at current market developments for data intermediaries and respective business models, one can say that several models exist and appear to be in a rather nascent phase.[986] In 2020, the European Commission conducted a study, according to which approximately 150 organisations in the EU offer services as data intermediaries, under which only a few larger companies operate.[987] The U.S. tech giants are not noticeably active here,[988] but the European Commission feared that without further regulation, they could enter data intermediary markets without facing any noticeable competition.[989]

[986] But see also on failed intermediary models and the history of data marketplaces Simon et al., Definition and analysis of the EU and worldwide data market trends and industrial needs for growth, 2021, p. 20–21.

[987] See COM SMART 2020/694, 43, according to which many of the existing data intermediaries have below 100 customers.

[988] But see also Gellert/Graef, The European Commissions proposed Data Governance Act, 2021, p. 12, on the Data Transfer project developed by Apple, Facebook, Google, Microsoft and Twitter (https://datatransferproject.dev/ (last visited 4.7.2022)).

[989] See COM SWD(2020) 295 final, 16–17.

In 2021, the so far most comprehensive study by Simon et al. identified around 178 cases of data marketplaces,[990] amongst which two are dedicated to agricultural data,[991] four cover data regarding connected car and the automotive industry,[992] and two on sensor data and nine on other B2B data.[993] In general, the authors of the study identified a high degree of fragmentation. Predominantly the data intermediaries focus on the regional level or domain-specific industries.[994] The intermediaries are either state-supported or set up by consortia of businesses or other organisations. A noticeable development in Europe has been the establishment of International Data Spaces (IDS) and particularly, GAIA-X.

4. The new legal framework: the Data Governance Act (DGA)

a) Goal and content of the DGA

With the Data Governance Act (DGA), a comprehensive legal framework for data intermediaries has recently been adopted in the EU.[995] The DGA affects contractual freedom, because it stipulates requirements for data intermediation, sets the standard of liability, and also provides for public oversight and enforcement over certain economic activities of market actors. The following analysis enquires into these rules and limits of the legal framework for *voluntary* and non-sector-specific data exchange via data intermediaries. The focus lies on the implications of these rules for competition and innovation, also considering their interplay with other legal regimes.

As an EU Regulation, the DGA sets out a harmonised legal framework for data intermediation services (DIS). The act will enter into force on 24 September 2023. However, the rules on DIS will be applicable only by 24 September 2024.[996] The DGA is the first act that has been finalised in implementation of the European Commission's Data Strategy of 2020.[997] The legislator's underlying aspiration is that the legal framework provided by the DGA should improve the availability and use of data in the EU[998] by increasing trust in DIS. Therefore, its obligations

[990] See Simon et al., Definition and analysis of the EU and worldwide data market trends and industrial needs for growth, 2021, p. 26; the database is accessible under https://doi.org/10.4121/14679564.v1 (last visited 4.7.2022).

[991] See for the current stage of the market in agriculture also Specht-Riemenschneider et al. MMR-Beilage 2021, 25.

[992] E.g. https://www.caruso-dataplace.com/ (last visited 4.7.2022).

[993] For details see Simon et al., Definition and analysis of the EU and worldwide data market trends and industrial needs for growth, 2021, p. 29–30.

[994] See Id., p. 47–53 on an evaluation of data sharing initiatives.

[995] Also, national rules, such as the German § 26 TTDSG, are evolving for specific contexts of data intermediation.

[996] Article 37 DGA.

[997] See COM(2020) 66 final.

[998] See COM SWD(2020) 295 final, 1.

aim to achieve the trustworthy provision of DIS.[999] This should foster the emergence of DIS, which are held to support and promote voluntary data sharing between companies (be it pooling or bilateral data sharing), but also to facilitate data sharing obligations.[1000] On the merits, it is novel and appears rather questionable to what extent the mere prospect of enhancing trust between market players can justify legal intervention.

To achieve this goal, the DGA installs a mandatory compliance regime,[1001] which requires DIS to officially register their services as a precondition for lawfully providing them in the EU. They are obliged to comply with various requirements, otherwise they face penalties and can be suspended from offering their services.[1002] In particular, the DGA provides for (at least some) neutrality of DIS regarding the data that is exchanged between data holders und users[1003] and make it structurally independent from players which often have significant market power.[1004] Neutrality and independence are regarded as key elements to bring about more trust and control,[1005] in addition to other obligations (see below). From a broader regulatory perspective on data access, the DGA deserves particular attention, because it is based on implicit assumptions on all relevant aspects related to data access (e.g. interoperability, standardisation, data protection law, exchange of sensitive data etc.). Also, the DGA defines the amount of leeway for sectoral policies of the Member States regarding DIS and therefore, also limits their policy options.

b) Scope of the DGA: 'Data Intermediation Services'

The DGA addresses DIS, which are classified as a sub-category of data intermediaries here (see already 2(b)).[1006] Crucial is Article 2(11) DGA, which contains a positive definition of DIS,[1007] being "a service, which aims to establish commercial relationships for the purpose of data sharing between an undetermined number of data subjects and data holders, on the one hand, and data users on the other hand, through technical, legal or other means, including for the exercise of data subjects' rights in relation to personal data".[1008] Therefore, two features stand

[999] See Recital 5 and 32 DGA, COM SWD(2020) 295 final, 21; Martens et al. JRC121336 (2020), 7.

[1000] See Recital 27 DGA.

[1001] Baloup et al., White paper on Data Governance Act, 2021, p. 26.

[1002] Member States must lay down penalties for the infringement, see also Recital 55.

[1003] See Recital 33 DGA. On the concept of neutrality Baloup et al., White paper on Data Governance Act, 2021, p. 31.

[1004] See Recital 27 DGA.

[1005] See Recital 33 DGA.

[1006] One can reasonably argue that there are also DIS, which do not qualify as data intermediaries under the here proposed definition.

[1007] This definition has been included after the Commission's proposal had been criticized for not containing a definition and a lack of clearly delineating the scope.

[1008] See also first sentence of Recital 28 DGA.

out for DIS: first, the DGA only applies to data intermediaries that are *open for an undetermined number* of data holders and users.[1009] Hence, the DGA does not apply to services provided for closed systems of data sharing. Second, the DGA includes commercial and non-commercial entities as DIS, only if they aim to establish *commercial relationships* with regards to data sharing. These criteria are indicative of the market-centred approach the legislator has taken. The underlying assumption is that the DGA should create trust which should enable DIS to scale up.[1010] However, closed data sharing systems are – arguably – neither in need for trust-increasing measures nor is usually their main aspiration to grow and therefore fall outside the scope of the DGA.

Out of all DIS that could fall under the definition of Article 2(11) DGA, Article 10 DGA specifies and exemplifies three kinds of DIS,[1011] and thereby further limits the scope of the DGA:

- Article 10(a) DGA quite broadly defines that the DIS "may include bilateral or multilateral exchanges of data or the creation of platforms or databases enabling the exchange or joint use of data, as well as the establishment of other specific infrastructure for the interconnection of data holders and data users"[1012]. According to Recital 28 DGA this includes data market places, orchestrators of data sharing ecosystems for instance in the context of common European data spaces, as well as data pools that are "established jointly by several legal or natural persons with the intention to license the use of such pool to all interested parties in a manner that all participants contributing to the pool would receive a reward for their contribution to the pool". Depending on the design, GAIA-X can be regarded as 'typical' example of this sort of data intermediary.[1013]

- Article 10(b) DGA specifically refers to DIS that relate to data subjects and individuals who make their data available for use and explicitly includes the enabling of data subjects' rights under the GDPR, meaning to enhance data subjects' control over data relating to them.[1014] This includes PIMS, though it is not entirely clear if only and to which extent.[1015]

[1009] See Article 2(11) DGA: "for the purpose of data sharing between an undetermined number of data subjects and data holders on the one hand and data users on the other hand"; excluding intermediating services, which are only used by one data holder or closed group (e.g. IoT network), see Article 2(11)(c) DGA; see also Recital 28 DGA.

[1010] See Richter ZEuP 2021, 634 (644–645).

[1011] It remains not entirely clear why the legislator makes this distinction between three different types of DIS, see Hartl/Ludin MMR 2021, 534.

[1012] See also last sentence of Recital 27 DGA.

[1013] See Falkhofen EuZW2021, 787 (791).

[1014] See Recital 30 DGA.

[1015] See Furthermore EDPB-EDPS, Joint Opinion 03/2021 on the Proposal for a regulation of the European Parliament and of the Council on European data governance (Data Governance Act), p. 31; Falkhofen EuZW 2021, 787 (790).

- Article 10(c) covers 'services of data cooperatives' within the meaning of 2(15) DGA.[1016] Given their rather vague definition,[1017] such data cooperatives perform consultancy and negotiating functions rather the data transfer and sharing being their core business.[1018] They are not of further interest within this study.

Various services are not covered by the DGA. Article 2(11) DGA mentions (in a non-exhaustive list) value-added services,[1019] content sharing service providers under the DSM Directive,[1020] services which are only used by one data holder or closed group (e.g. IoT network),[1021] and public sector bodies that offer DIS that do not aim to establish commercial relationships for the purpose of data sharing.[1022] Furthermore, Article 15 DGA exempts data altruism organisations and other not-for-profit entities to some extent. In addition, Recital 29 DGA mentions other activities which the definition of data intermediation services does not cover.[1023] Moreover, Recital 28 DGA clarifies that services – e.g. cloud storage or analytics software – are no DIS under the DGA if they only provide technical tools for data sharing "but are neither used for aiming to establish a commercial relationship between data holders and data users, nor allow the provider to acquire information on the establishment of commercial relationships for the purpose of data sharing, through the provision of such services." Overall, it remains still[1024] unclear, which of these cases are exemptions from the scope or if they just exemplify the definition.

c) Conditions for providing Data Intermediation Services

Article 12 DGA mandates the DIS to fulfil substantial requirements when offering their services. These obligations can be grouped as follows:

[1016] See also Recital 31 DGA.

[1017] See Baloup et al., White paper on Data Governance Act, 2021, p. 29, for criticism on the vagueness of the definition. Furthermore EDPB-EDPS, Joint Opinion 03/2021 on the Proposal for a regulation of the European Parliament and of the Council on European data governance (Data Governance Act), p. 32.

[1018] See Anicic et al., Konzeptstudie Datengenossenschaft, Parts 1 and 2.

[1019] See also Recital 28 DGA.

[1020] See also Recital 29 DGA.

[1021] See also Recital 28 DGA.

[1022] See also Recital 29 DGA.

[1023] Such as consolidated tape providers, account information service providers, and "[o]ther services that do not aim to establish commercial relationships, such as repositories aimed at enabling re-use of scientific research data in accordance with Open Access principles".

[1024] The Commission's proposal for the DGA has been rightly criticized for being too imprecise when it comes to its scope (Baloup et al., White paper on Data Governance Act, 2021, p. 27–28; Spindler CR 2021, 98 (102–103); Richter ZEuP 2021, (649–652, 662); Furthermore EDPB-EDPS, Joint Opinion 03/2021 on the Proposal for a regulation of the European Parliament and of the Council on European data governance (Data Governance Act), p. 29–30, and the legislator has improved and sharpened the definition in the trilogue to some extent.

1) Structural separation/unbundling of services: Article 12(a) DGA obliges the DIS to provide its services through a separate legal person. This separation principle aims to prevent conflicts of interest[1025] and limit the risk of cross-data usage.[1026] It stipulates a structural unbundling between data provision, specific 'intermediating' data-related business activities and data use.[1027] DIS who provide their services in the EU necessarily have to fulfil this requirement.[1028] Yet, for being able to capture some benefits of vertical integration, Article 12(e) DGA clarifies that DIS (and therefore the same legal person) may offer some added-value tools and services, as long as they facilitate data exchange (e.g. through 'temporary storage, curation, conversion, anonymisation, pseudonymisation').[1029] This clause accounts for the view that DIS would commonly offer such tools and services to sustain their intermediation business model and that such tools and services are to the advantage of data holders and users. Yet, in any case Article 12(e) DGA requires data holders (or data subjects) to explicitly request or approve such tools and services.

2) Limitations on data use: the DGA defines and limits the purposes, for which the DIS may use data: according to Article 12(a), the DIS may not use data for which it provides its intermediation services 'for other purposes than to put them at the disposal of data users'. In addition to this data neutrality requirement,[1030] Article 12(c) DGA also limits the use of data, which the DIS collects about the activities of holders and users of the service when performing its service. The DIS may use such data only for the development of that service (e.g. fraud detection or cybersecurity), and has an obligation to make this data available to data holders upon request. Both provisions resemble the recurrent issue in competition law of anti-competitive cross-data usage (see part E(III)(1)). Yet, Article 12(a) DGA is a strict *per se* prohibition which applies regardless of the outcome of the competition analysis under Article 102 TFEU.[1031] Also, similar prohibitions in Article 5 No. 2 and Article 6 No. 2 DMA are limited to specific contexts and only address gatekeepers (see part E(V)).[1032] As another limitation, Article 12(e) DGA addresses situations, in which the DIS legitimately offers third-party added-value tools for facilitating the exchange of data. In such cases, Article 12(e) DGA also prohibits third parties which provide such tools to use the data for other purposes than facilitating the data exchange as provided by the DIS. Furthermore, Article 12(d) DGA prohibits the DIS to shift the format of the received data for other purposes than for the data

[1025] See Recital 33 DGA.

[1026] See Baloup et al., White paper on Data Governance Act, 2021, p. 33.

[1027] See Recital 32 DGA.

[1028] See Baloup et al., White paper on Data Governance Act, 2021, p. 34.

[1029] See also Recital 32 DGA.

[1030] See on the "novelty" and context of this principle Richter ZEuP 2021, 634 (654).

[1031] See already part E(III)(2) on access to data under Article 102 TFEU.

[1032] See Baloup et al., White paper on Data Governance Act, 2021, p. 32.

exchange. Even in that case, the DIS must offer an opt-out possibility to data subjects or data holders.[1033]

3) Conditions for the provision of service and use of data: the DGA contains provisions on the terms and conditions between the DIS and its data holders/users. Article 12(f) DGA stipulates a general obligation to the DIS to "ensure that the procedure for access to its service is fair, transparent and non-discriminatory for both data subjects and data holders, as well as for data users, including as regards prices and terms of service". This provision aims to ensure the neutrality of the service from the perspective of data holders and users.[1034] Simultaneously, it can also increase market transparency and foster condition-based competition,[1035] and it sets a benchmark for a review of explicit contractual access rights (see part E(II)(2)). This obligation is complemented by the prohibition that DIS make their terms "dependent upon whether or to what degree the data holder or data user uses other services provided by the same provider or a related entity" (Article 12(b) DGA). This provision aims to prevent DIS from contractually bundling services (or incentivising their bundled usage), which would undermine the structural separation, so that ultimately markets are kept open. Finally, Article 12(h) DGA entails a duty to 'ensure a reasonable continuity of provision of its services'[1036] and – if the DIS also stores data – to install sufficient guarantees that this data remains accessible to data holders/users in case of insolvency.[1037]

4) Interoperability and Standards: the DGA also aims to foster interoperability. Article 12(i) DGA requires the DIS to "take appropriate measures to ensure interoperability with other data intermediation services", which includes using "commonly-used open standards in the sector in which the data intermediation service providers operate". For this purpose, the European Commission encourages and facilitates Union-wide codes of conduct, especially on interoperability and "[t]he European Data Innovation Board should facilitate the emergence of additional industry standards, where necessary".[1038] Interoperability is also privileged in Article 12(d) DGA: the DIS may shift the format of received data solely for the purpose of data exchange to "enhance interoperability within and across sectors or if requested by the data user […] to ensure harmonisation with international or European data standards".

5) Technical, organisational and legal safeguards: Article 12 DGA requires the DIS to install various technical, organisational, and legal safeguards. These safeguards aim to protect the

[1033] Unless Union law mandates such conversion.

[1034] See Baloup et al., White paper on Data Governance Act, 2021, p. 31.

[1035] See Richter ZEuP 2021, 634 (656).

[1036] See Baloup et al., White paper on Data Governance Act, 2021, p. 34–35, drawing a parallel to public services.

[1037] See Id., p. 36, on the broader implications of such "action revendicatio".

[1038] See Recitals 32, 34 DGA. See also EU Strategy on Standardisation, COM(2022) 31 final, on this topic.

interests of the data holders and users. They include: installing procedures to prevent fraudulent or abusive practices (Article 12(g) DGA); implementing measures in order to prevent unlawful transfer or access to non-personal data (Article 12(j) DGA); informing data holders 'in case of an unauthorised transfer, access or use of the non-personal data that it has shared' (Article 12(k) DGA); ensuring "an appropriate level of security for the storage, processing and transmission of non-personal data", which includes ensuring "the highest level of security for the storage and transmission of competitively sensitive information" (Article 12(l) DGA) (see part E(III)(1)). Furthermore, the DIS has to maintain a log record of the intermediation activity (Article 12(o) DGA).

6) Special obligations regarding DIS related to data of individuals: for DIS which provide services regarding individual, and especially personal data (see Article 10(b) DGA), the DGA contains specific obligations. Article 12(m) DGA stipulates a 'best interest clause', according to which DIS "shall act in the data subjects' best interest when facilitating the exercise of their rights". In particular, this due diligence obligation[1039] contains duties to inform and advise data subjects "in a concise, transparent, intelligible and easily accessible form about intended data uses by data users and standard terms and conditions attached to such uses, before data subjects give consent". By that means, the legislator aims to prevent individuals that use such services to make more data relating to them available than what is actually in their own interest.[1040] Crucial from a contractual point of view (see part E(II)) is Recital 33, which states that such DIS should "bear fiduciary duty towards the individuals, to ensure that they act in the best interest of the data subjects". All DIS which provide tools for obtaining consent or permissions to process data must specify the jurisdictions in which the data use is intended to take place (Article 12(n) DGA). Moreover, they have to "provide data subjects with tools to both give and withdraw consent and data holders with tools to both give and withdraw permissions to process data".

d) Enforcement

The conditions set out in Articles 11 and 12 DGA are subject to public enforcement. To this end, Article 14(2) DGA grants investigative powers to the competent national authorities, and Article 13(4) DGA allows the authorities to impose fines and to order the termination or suspension of the service. Article 34 DGA requires that penalties are effective, proportionate and dissuasive and leaves it to the Member States to specify the penalties by outlining some criteria to be taken into account when imposing penalties.

[1039] Helberger/Micklitz/Rott, The Regulatory Gap: Consumer Protection in the Digital Economy, 2021, p. 6

[1040] See Recital 30 DGA.

At the same time, the DGA is silent on private enforcement. A comparative view on other legal acts of the EU is inconclusive on whether private enforcement can be used in addition to public enforcement.[1041] But one may argue that private enforcement applies according to the rules of the Member States. Moreover, Recital 33 DGA states that questions of liability regarding the DIS "could be addressed in the relevant contract, based on the national liability regimes". In particular, data holders and data users can assert contractual claims against DIS to the extent that the conditions of Article 12 DGA are affected. This includes suing for contractual performance, damages, termination, and injunctive relief (also under § 1 UKlaG) as well as the review of explicit contractual access rights (see part E(II)). But also, competitors in Germany can take legal action against unfair practices or ineffective general terms and conditions in the event of violations of the obligations standardised in Article 12 DGA on the basis of § 3a UWG.[1042]

5. Uncertainty of effects of the new market design for data intermediaries

Form a theoretic point of view, data intermediaries can perform several desirable functions in data-driven markets – whether in the context of voluntary data sharing or mandatory data sharing. In theory, they can contribute to a more efficient data value creation by providing control over data flows both ways: they can enable and foster data sharing as well as prevent sharing to ensure compliance with the law (including Articles 101 TFEU and the GDPR).

As has been shown, the DGA provides a legal framework for a sub-set of data intermediaries. These rules have been criticised by economic and legal scholars in several aspects, which all relate to how the question how the DGA will affect the future development of data intermediaries. The concerns can be shared to some extent. First, it can be agreed that the DGA provides a framework with high legal uncertainty. The definition of the scope and the rules of the DGA are novel and vague, so that they are in need of further interpretation by the respective authorities and courts.[1043] The interviews have confirmed some general uncertainty in the industry about the DGA's scope of application on GAIA-X- federated applications. In fact, the exact scope of several obligations remains unclear[1044] and it is uncertain, how DIS can meet them case-by-case. This appears critical, as legal certainty plays a striking role in the light of public enforcement and penalties to be introduced.[1045] While the European Data Innovation Board will support the European Commission to specify technical requirements and to develop a consistent enforcement practice (see Article 30 DGA), much remains to be seen. In general,

[1041] See Richter ZEuP 2021, 634 (657–658).

[1042] See Id., 658–659.

[1043] See Gellert/Graef, The European Commissions proposed Data Governance Act, 2021, p. 14; Baloup et al., White paper on Data Governance Act, 2021, p. 36.

[1044] See Baloup et al., White paper on Data Governance Act, 2021, p. 37.

[1045] See Article 34 DGA.

a side glance to other legal regimes is informative for the interpretation of the DGA: the obligations under Article 12 DGA resemble the combination of (far reaching) ex post remedies under competition law as well as ex ante obligations under the DMA, for utility providers or in sector specific regulation.[1046] Yet, parallels can only be drawn to some extent,[1047] because the provisions of the DGA need to be interpreted in light of their own legislative goals, namely increasing trust of data holders and users as well as fostering the emergence of data intermediaries.[1048]

Second, this legal uncertainty adds to the unpredictability of the regulatory effects of the DGA. In this regard, its positive impacts have been widely questioned. Based on the premise that regulation might make it generally more difficult to implement business models and harm/eliminate the establishment of data intermediaries,[1049] some assume that the DGA may rather hinder than foster the development of DIS.[1050] Others argue that the DGA would have no effect and question the attractiveness of the legal framework as it would fail to attract supply of and demand for DIS.[1051] Moreover, the DGA would miss the point by referring to other deficits to be overcome to foster data sharing, as e.g. information asymmetries on the quality and provenience of data, uncertainty on enforcement of purpose limitation of the use of data,[1052] de facto lock-in and lack of standardisation.[1053] The interviews have at least confirmed the impression that companies who already started to build up data intermediation services now carefully consider business strategies in light of the DGA and that clear trends are not yet visible. This can be explained by the remaining time for implementation until September 2025. What has been emphasised is the need for the company to offer value-added services on top of the mere intermediation service.

Interviewees have also referred to the requirement of structural separation as being overly strict, making businesses now carefully consider withdrawing from the market or not entering it. Indeed, also from a theoretical point of view, this requirement has been criticised as being overly interventionist.[1054] The structural separation requirement is held as difficult to enforce and too rigid and undifferentiated – i.e. Baloup et al. claim that it should be limited to

[1046] See Baloup et al., White paper on Data Governance Act, 2021, p. 35.

[1047] See Richter ZEuP 2021, 634 (653).

[1048] See Recital 5 DGA.

[1049] See Specht-Riemenschneider et al. MMR-Beilage 2021, 25 (32).

[1050] See Kühling ZfDR 2021, 1 (23).

[1051] See Hartl/Ludin, MMR 2021, 534.

[1052] See Kerber, DGA – einige Bemerkungen aus ökonomischer Sicht, 2021, p. 3.

[1053] See Specht-Riemenschneider/Kerber, Designing Data Trustees, 2022, p. 41–42.

[1054] Baloup et al., White paper on Data Governance Act, 2021, p. 35, have questioned whether the obligations of Article 12 DGA would unproportionally restrict the DIS' freedom to provide business under Article 16 of the EU Charter of Fundamental Rights; see also Hartl/Ludin MMR 2021, 534, who question the proportionality for already existing business models.

competition-law sensitive situations, meaning for markets exposed to a higher risk of cross-data usage.[1055] But also when accounting for the regulatory context, it has been questioned whether DIS can be competitive compared to other services which are unregulated or less strictly regulated (especially under the proposed DMA).[1056] In this regard, the data neutrality requirement would appear overly strict, considering that DIS are yet to be established and they are not in a comparable situation to gatekeepers as addressed by the DMA.[1057] As a consequence, the principle of strict data neutrality may effectively lead to less innovation,[1058] because DIS will either disappear or not even enter the market.

Given the nature of the DGA as a corner stone to the establishment of an infrastructure for data sharing, but not addressing a well identified market failure,[1059] all predictions about future developments remain speculative in the light of the current lack of evidence. So far, scholars have based their criticism on anecdotal evidence and preconceptions about data-driven innovation. The experimental nature of the DGA[1060] leads us to the conclusion that significant uncertainty remains on whether this regulation will evoke the desired effects.

Two implications for policy making follow from this analysis. First, given the unforeseeable effects, the legislature should closely monitor market developments in the area of data intermediation services to prevent dysfunctional market design.[1061] Article 35 DGA provides an evaluation and review clause, according to which the European Commission shall evaluate the Regulation and provide a report by 24 September 2025. However, the specifically mentioned aspects for assessment do only include aspects of compliance, but not the effectiveness of the regulation. The German Government should gather evidence on the market developments in the upcoming years to come up with suggestions for necessary amendments of the regulation.

A second implication is that regardless of the predictability of the regulatory effects of the DGA, it is conceded that data intermediaries can indeed perform several desirable functions in data-driven markets. Therefore, as a minimum condition for advancing digital regulation, the legal

[1055] See Baloup et al., White paper on Data Governance Act, 2021, p. 34. See also Specht-Riemenschneider et al. MMR-Beilage 2021, 25 (32), who argue that the DGA stipulates a "one-size-fits-all approach", which does not adequately reflect the particularities of different data trustee models.

[1056] See Gellert/Graef, The European Commissions proposed Data Governance Act, 2021, p. 11–13; Kerber, DGA – einige Bemerkungen aus ökonomischer Sicht, 2021, p. 3.

[1057] See Baloup et al., White paper on Data Governance Act, 2021, p. 34–35; still, Recital 27 DGA mentions also the importance of independency of DIS from players with significant market power.

[1058] See Richter ZEuP 2021, 634 (654–655).

[1059] But see COM SWD(2022) 45 final.

[1060] See Richter ZEuP 2021, 634 (661–663).

[1061] This is also true for the further market developments of PIMS under § 26 TTDSG, which can be followed with interest, as the effect of legislative intervention can be observed – albeit in a very narrow field of application – once the delegated act on the procedure and technical modalities has entered into force.

framework in sum should support (or at least not hinder) their development. This implies that the legislature should take data intermediaries more consciously into account when further advancing and applying rules that concern data access and digital markets, and that rules on data intermediaries are coherently integrated into the legal framework. The following section deeper enquires into this claim.

6. Integration of data intermediaries in the market order for data sharing

a) Overview

With regards to the DGA, commentators have stressed the need of compatibility with the rest of the EU acquis – but considered this to be a "mere afterthought that is left to market players to figure out".[1062] Indeed, a coherent integration of data intermediaries in the legal orders of the EU and the Member States is ambitious and requires discussing both the relevance for and the interaction with several other legal regimes. By this means the potential of regulatory synergies can be identified, and the remaining need for the legislature to advance the legal framework can be distilled. While the DGA provides a new legal regime that interacts with all other regimes for a sub-set of all data intermediaries, this section also asks how the other legal regimes do and could consider data intermediaries even beyond the scope of the DGA. Given the phenomenological nature of data intermediaries, the analysis covers the interfaces with all legal regimes, which this study has previously discussed as essential parts of a market order for data sharing.

b) Data protection

The most striking existing rules regarding data intermediaries relate to data protection. If access to and sharing of *personal* data is at stake, data protection rules apply (see part E(I)(4)). A frequently discussed issue is, how data intermediaries – and in particular data trustees – can foster the exchange of personal data. Data trustees[1063] are not necessarily related to personal data (see above), but in fact they often intermediate between data subjects and processors and support data subjects in exercising their data-related rights, e.g. for pseudonymisation purposes, or mandating as agent to exercise data protection preferences.[1064] In this regard, questions about data protection are at the centre of attention in legal scholarship. This is particularly true for

[1062] See Gellert/Graef, The European Commissions proposed Data Governance Act, 2021, p. 15.

[1063] Some people see this identical to the definition of Article 10(b) DGA, see Kühling ZfDR 2021, 1 (7); Beise RDi 2021, 597 (602).

[1064] See Kühling ZfDR 2021, 1 (4–7).

Personal Information Management Systems (PIMS),[1065] which are intermediaries that are used to manage consent but can be extended, e.g. also to enforce data subject's rights[1066] or to claim damages for the violation of data protection rules.[1067]

Within the scope of the DGA, none of these aspects are explicitly addressed. Article 1(3) DGA states that the DGA is without prejudice to GDPR. This means that in any case, DIS have to comply with the GDPR, and the DGA does not alter/affect rules on data protection. The provision clarifies that the DGA "does not create a legal basis for the processing of personal data and does not alter obligations and rights set out in" the GDPR and the ePrivacy-Directive. In fact, the DGA does not specifically distinguish between personal and non-personal data, but if personal data is affected, the requirements of data protection laws apply in any case.[1068] At the same time, the DGA is somewhat even stricter than the requirements of the GDPR,[1069] because the GDPR does allow data processing for a purpose other than the one originally specified if the data subject consents to it, while Article 12(a) DGA strictly prohibits this.

This once more confirms the relevance of a discussion of recent years that has frequently pointed to data protection laws and their curbing effect on the establishment of data intermediaries.[1070] The discussions question the 'intermediary friendliness' of current data protection law and revolve around four issues. First, a crucial question for the functioning of data intermediating services with regard to personal data is to what extent current data protection law enables data intermediaries to manage consents of data subjects. The GDPR requires informed consent (Article 4 No. 11 GDPR), the determinateness of consent (Articles 5(1)(b), 6(1)(1)(a) GDPR), and allows revocability of consent at any time (Article 7(3) GDPR). Given these strong rights of the data subject, the requirements for agency and consent (through third party) but also regarding the breadth of consent remain unclear.[1071] A second, question is to what extent data trustees can exercise data subject's rights, especially to rectification (Article 16 GDPR) and erasure (Article 17 GDPR).[1072] Thirdly, the legal framework for the liability of data trustees is discussed. In particular, the question arises in case the data trustee transfers data to a user who breaches data protection law, and the data trustee

[1065] For practical examples of PIMS see Schwartmannn/Weiß, Datenmanagement und Datentreuhandsysteme, 2020, p. 10–16; see for the current stage of the market Blankertz/Specht-Riemenschneider, Wie eine Regulierung für Datentreuhänder aussehen sollte, 2021, p. 25–29.

[1066] See Kühling ZfDR 2021, 1 (7); on definition of PIMS also Specht-Riemenschneider et al. MMR-Beilage 2021, 25 (27).

[1067] See Kühling ZfDR 2021, 1 (12).

[1068] See Spindler CR 2021, 98 (104).

[1069] See Richter ZEuP 2021, 634 (655); Kühling ZfDR 2021, 1 (23).

[1070] For details see Kühling/Sackmann/Schneider, Datenschutzrechtliche Dimension Datentreuhänder, 2020.

[1071] See Specht-Riemenschneider/Kerber, Designing Data Trustees, 2022, p. 35–37.

[1072] See e.g. Kühling ZfDR 2021, 1 (12), claiming that there are no significant legal barriers.

could have foreseen such breaches.[1073] Fourth, it has been discussed to what extent parties to a contract can exclude the possibility of the data holder to mandate data trustees.[1074] This could have consequences on evolving competition, as it would prevent data trustees from entering the market. Such contractual clauses would appear doubtful in the light of review of the terms and conditions of a contract, data protection laws and – in case of market dominance – Article 102 TFEU.[1075]

Different proposals have been made to reform data protection law to enable and foster the activities of data intermediaries. Some commentators argue that clarifications and legislative steps are needed:[1076] This would include installing a regulatory framework, which would clarify questions of liability, quality, trustee's obligations, prohibit tying, rules for insolvency;[1077] provide a legal basis for justification of data transfer to the data trustee to eliminate legal uncertainty;[1078] and to clarify agency through data trustees when it comes to the exercise of data subjects' rights.[1079] Other commentators argue that no such invasive steps are needed to provide sufficient legal certainty for data intermediaries to operate with personal data. Rather more guidance through supervisory institutions is held to be sufficient,[1080] scepticism regarding sector-specific regulation in parallel to GDPR is put forward,[1081] and the market is held as too premature so that existing rules would leave enough leeway and incentives to develop such intermediation services.[1082] Therefore, policy options in the area of data protection and data intermediaries have already been extensively discussed. Not the least due to a lack of political will to reform data protection laws, this study does not reiterate these claims. Rather it calls on policy makers to consider the broader regulatory picture for an effective integration of data intermediaries in the market order for data sharing

c) Contract law

As regulatory intervention in private actors' relations, the DGA deliberately limits the contractual freedom with regards to data access via DIS. The obligations are not alterable by mutual consent of the parties – unless the DGA states otherwise.[1083] So even if one can think of

[1073] See Kühling ZfDR 2021, 1 (14–19).
[1074] See Kühling/Sackmann/Schneider, Datenschutzrechtliche Dimension Datentreuhänder, 2020, p. 19–26.
[1075] See Kühling/Sackmann/Schneider, Datenschutzrechtliche Dimension Datentreuhänder, 2020, p. 19–26.
[1076] See Datenethikkommission der Bundesregierung, Gutachten, 2019, p. 134.
[1077] VZBV, Neue Datenintermediäre, 2020.
[1078] See Specht-Riemenschneider et al. MMR-Beilage 2021, 25 (46).
[1079] See Specht-Riemenschneider et al. MMR-Beilage 2021, 25 (46).
[1080] See Kühling ZfDR 2021, 1 (23).
[1081] See Kühling ZfDR 2021, 1 (22).
[1082] See Kühling ZfDR 2021, 1 (20).
[1083] E.g. Article 12(e) DGA.

cases in which e.g. the strict data neutrality requirement could be departed from to the benefit of both (data holder and data user) *and* without harming the common good (i.e. competition),[1084] an agreement to deviate from the obligation would be void. In other words, even if the data holder had equal bargaining power, he could not consent that the DIS may use the data for commercial exploitation.[1085] The reason for this strict interpretation lies in the debatable function of the provisions to generally create trust in the activities of market actors and incentivise them to share data.

Once the provisions of the DGA for data intermediaries are applicable, they will affect the lawfulness of terms and conditions for such contracts on data access which involve DIS within the meaning of Articles 10 and 2(11) DGA. Several obligations imposed by Article 12 DGA arguably qualify as *per se* prohibitions, because the DGA aims to strengthen the trust of market actors in data intermediaries at large.[1086] Due to the systemic nature of the obligations, their application is not to the disposal of the parties.[1087] Therefore, under German contract law, a review of standard terms and conditions according to § 307 BGB would not even be opened.[1088] This applies e.g. to the case that terms and conditions of the DIS would reserve rights to use data for purposes beyond what the DGA allows (see neutrality obligation under Articles 12(a) and (c) DGA). The same goes for the case if a DIS would reserve the right to offer value-add services beyond what is allowed under Article 12(e) DGA without the approval of the data holder. Also, the DIS may not make its service "dependent upon whether or to what degree the data holder or data user uses other services provided by the same provider or a related entity" (Article 12(b) DGA). Beyond such clear-cut violations of the DGA, data access terms of DIS can be subject to the test of reasonableness according to § 307 BGB. Here, the DGA sets the measure for review. Finally, DIS could violate some obligations *de facto*, without backing it up in its terms and conditions. This is the case e.g. by offering its services through a structurally not separated entity (Article 12(a) DGA), by offering value-add services beyond what is allowed in Article 12(e) DGA or by not implementing sufficient technical, organisational and legal safeguards that the DGA requires them to implement to protect the interests of the data holders and users.[1089] All these aspects on the interpretation of obligations and its relationship to contract remain to be interpreted and refined by courts and responsible authorities in the next years. There is much leeway, and the legislature should have a critical eye on whether future interpretation and application are legally coherent and economically sound.

[1084] See Richter ZEuP 2021, 634 (655).

[1085] This has been criticized by Kühling ZfDR 2021, 1 (23).

[1086] See Recital 4 DGA.

[1087] Even if their derogation would not harm any party and would appear desirable from an economic point of view, on such considerations see Richter ZEuP 2021, 634, (655–659).

[1088] Wurmnest in MüKoBGB, 8th ed. 2019, § 309 para. 1.

[1089] See e.g. Article 11(5), (7), (7a), (8), (11a) DGA.

The DGA has been criticised as insufficiently addressing the contractual relationship between DIS and data holders and users,[1090] not the least because Article 12(f) DGA incorporates FRAND and price regulation but does not further define what this means.[1091] The previous section on the Draft Data Act (see part F(I)) has already discussed the potential and caveats for making the FRAND principle as mandatory default for all future data access legislation under Chapter III of the Data Act. The EU legislature could consider extending Article 8(1) Draft Data Act also to Article 12(f) DGA.

d) Competition law

aa) Data intermediaries as catalysts for competition law enforcement

Competition law and data intermediaries share different points of contacts. Data intermediaries can enable compliance with and enforcement of competition law. As has already been discussed (see part F(II)(1)(b)), there exist a multitude of possibilities to combine different datasets with one another, as well as the different ways to process data, and the way that sharing, pooling or use of data is organised may matter for the legality of a data exchange under competition law. For example, the risk that competitively sensitive information can be drawn from a specific dataset may differ depending on whether a dataset is transferred to a competitor, or whether the dataset remains on the server of the original 'data controller' and a competitor is given access to a dataset on the basis of queries and for specified purposes only. Where data is pooled, it may well matter whether data access is organised through a data intermediary who may be charged with the task to ensure, among other things,[1092] that no competitively sensitive information is derived from the relevant dataset. Simultaneously, such a data intermediary may ensure FRAND access of third parties to the pooled data where this is necessary to prevent foreclosure. If FRAND access is granted to third parties, negative effects on competition will normally be unlikely. However, the data format standards and interfaces will need to be reviewed for anti-competitive effects.

The analysis of merger remedies has revealed that monitoring trustees play an important role to oversight the implementation of access commitments (see parts E(IV), F(II)(4)). However, so far, they cannot be considered as data intermediaries, because the data transfer itself is performed by the merged entity. In the case of data separation it has been suggested that data intermediaries as independent third parties can play an important role: they can prevent data from being merged or used for purposes that would increase data power and concentration, and strengthen the structural effect of the commitment.

[1090] See Spindler CR 2021, 98 (104).

[1091] See Picht/Richter GRUR International 2022, 395 (397).

[1092] E.g. to ensure compliance with the GDPR.

bb) Data intermediaries as subjects of competition law

At the same time, data intermediaries themselves can be subject to competition law. This becomes evident when looking at the interface between the DGA and competition law: the DGA aims to promote DIS, following the assumption that they can play an important role in making data-related markets more competitive and foster data-related innovation. However, from the angle of competition law, data intermediaries must also be regarded with some caution, as they can enable illegitimate sharing of data and information. When it comes to data intermediaries that qualify as DIS under the DGA, Article 1(4) DGA is clear when it states that the DGA is "without prejudice to the application of competition law". More concretely, Recital 60 clarifies that the DGA "should not affect the application of the rules on competition, and in particular Articles 101 and 102 TFEU". In particular, this concerns "the rules on the exchange of competitively sensitive information between actual or potential competitors through data intermediation services". But in fact, the DGA even reaches one step further and requires DIS to implement some additional safeguards by imposing obligations regarding the storage and transmission of competitively sensitive data (see part E(III)(1)). However, it is not clear, what the exact scope of this obligation is. Originally, Article 11(9) of the European Commission's DGA proposal went far, as it required that DIS "shall have procedures in place to ensure compliance with the Union and national rules on competition". However, this general compliance obligation was deleted in the legislative procedure, now amounting to Article 12(l) DGA, which merely states that DIS "shall further ensure the highest level of security for the storage and transmission of competitively sensitive information". Surprisingly, this is less than Recital 37 DGA requires, stating that

> "Data intermediation services providers should also take measures to ensure compliance with competition law and have procedures in place to that effect. This applies in particular in situations where data sharing enables undertakings to become aware of market strategies of their actual or potential competitors. Competitively sensitive information typically includes information on customer data, future prices, production costs, quantities, turnovers, sales or capacities."

It appears that out of negligence the legislature did not modify the Recital in congruence with the amendment of the DGA's operational part. In substance, a Recital cannot impose such far-reaching binding obligations if these are not reflected in the operational part of the regulation. Therefore, the obligation of the DGA is to be understood as a mere duty to implement technical safeguards that meet the current technical state of the art. Beyond that, particularly the application of Article 101 TFEU sets the benchmark for liability under competition law with regard to the exchange of sensitive information and data. In this regard, the Draft Horizontal

Guidelines the European Commission only mentions 'trustees'[1093] as independent third-party service providers as a general option to be considered by undertakings to implement precautionary measures in the case of exchanging commercially sensitive information. However, it does not further elaborate or guide on the particular role of data intermediaries or data intermediation services.

The absence of data intermediaries in the Draft Horizontal Guidelines can be explained by the fact that there has not yet been any case practice in this field, following the perception that such guidelines should present past case practice to provide legal certainty and consistency of application rather than anticipating cases or steering competition policies in certain directions. However, current legal uncertainty and demand for future guidance appears high in this area. The legislature (EU as well as national) should not overlook the critical role that official guidance may play a crucial role for providing legal certainty for evolving business models.[1094]

e) Draft Data Act

When looking at the Draft Data Act, it surprises that the proposal does not refer to data intermediation services, taking into account that the DGA can be considered as an enabling framework for the Draft Data Act.[1095] Data intermediaries could play an important role to effectuate the data access right under Chapter III of the Draft Data Act by significantly reducing transaction costs and thereby enable data-driven innovation on large scale. The reasons are that rather than the individual user or data recipient, they may better understand and aggregate third-party data demand for innovative purposes, be able to bundle data supplied from multiple sources in a targeted manner, can further aggregate and process user data tailored to the needs of various data recipients, and can manage data transfer from a technical and legal perspective.[1096] The Draft Data Act does not take up on such cases, which might, however, be worth being considered, should the legislature seek to foster AI-driven innovation in the future.

An important debate is taking place on whether or to what extent the Draft Data Act actually allows users to purely commercialise the data which they can receive under Article 4 or share with third parties under Article 5 Draft Data Act – this means that the user of the product would not directly benefit from a service that would make use of such data, but that the user would

[1093] See C(2022) 1159 final, para. 411.

[1094] For the discussion to what extent GAIA-X could prevent the exchange of competitively sensitive information, see part F(II)(1)(b).

[1095] See COM(2020) 66 final, 12.

[1096] Drexl et al., Position Statement of the Max Planck Institute for Innovation and Competition of 25 May 2022 on the Commission's Proposal of 23 February 2022 for a Regulation on harmonised rules on fair access to and use of data (Data Act), para. 338.

provide the data accessed on basis of Article 4 simply for remuneration to third parties.[1097] Data intermediaries are well placed to offer such remuneration on a large scale and further share/sell the obtained data. In the further legislative procedure, this issue should be discussed, taking into account that Article 6(2)(c) Draft Data Act speaks against the legitimacy of such commercialisation, because it forbids the third party (here the data intermediary) to "make the data available it receives to another third party in raw, aggregated or derived form, unless this is necessary to provide the service requested by the user". This implies that a data intermediary cannot approach users and offer payment for data, which the intermediary could then process and provide to third parties who could use such data for innovative purposes.[1098] If considered as politically appropriate, Article 6(2)(c) Draft Data Act could be amended in a way that it would allow data to be shared with third parties via data intermediaries to create data markets, at least for specific purposes. This opening clause could be attached to the DGA to protect stakeholders' interests by requiring that only DSIs under the DGA may be chosen to perform such intermediation.[1099]

f) Sector-specific data access regulation

Data intermediaries can become particularly relevant in the context of data access in specific sectors and take over more targeted roles. Which model of intermediary is suitable and how to further design it depends on the affected specific sector and markets. It can be highly controversial, as the example of mandating a trustee for car data in Germany has shown.[1100] In this respect it is important to mention that the DGA has set the track for sectoral approaches with regard to DIS by giving Union and national legislator the possibility for more specific regulation. The DGA stipulates EU-wide harmonisation regarding the operations of DIS. This is to be seen as a *minimum* standard. Article 1(2) DGA allows to introduce "specific additional technical, administrative or organisational requirements, including through an authorisation or certification regime" by means of European Union legal act or national law, as long as they are non-discriminatory, proportionate and objectively justified. By that means, sector-specific legislation[1101] can introduce stricter standards for DIS that fall under the scope of the DGA.

An already existing example is § 26 TTDSG, even though it concerns the mere management of the end user's consent with regards to telemedia (e.g. websites) and therefore a constellation that does arguably not qualify as data intermediaries as understood within this study (see

[1097] Id., paras. 14 et seq.

[1098] Id., para. 338.

[1099] Ibid., para. 338.

[1100] See Tagesschau, Streit um die Autodaten, 31.1.2022, https://www.tagesschau.de/wirtschaft/verbraucher/autodaten-datensammeln-datenschutz-fahrstil-versicherungen-auto-datentreuhaender-101.html (last visited 4.7.2022).

[1101] See Recital 40 DGA.

above). Nevertheless, it illustrates challenges for future sector-specific regulatory approaches for data intermediaries. § 26 TTDSG stipulates sector-specific regulation of DIS, according to Article 1(2) DGA.[1102] It is a first attempt of the German legislator to provide an explicit legal basis for data protection related consent management through intermediaries. The provision has entered into force on 1 December 2021, but the actual effect remains to be seen. In particular, the TTDSG allows mandating accredited PIMS for consent management. Such consent services must fulfil certain criteria and have to undergo an accreditation procedure, which should be further outlined in a delegated act, which is currently conceptualised.[1103] In substance, the provision goes beyond the obligations of the DGA, as it requires the intermediaries to "have no economic self-interest in giving consent and in the data managed and are independent of companies that may have such an interest" (§ 26(1)(2) TTDSG).[1104] While § 26 TTDSG resolves some of the mentioned legal uncertainties with regards to delegating consent under protection laws, criticism remains. It has been put forward that § 26 TTDSG is not mandatory for telemedia providers – neither with regard to following PIMS settings nor regarding browser settings.[1105] In addition, § 26 TTDSG would continue to allow individual user consent to take precedence over PIMS settings, so it could be assumed that telemedia providers would continue to ask users for consent via cookie banners regardless of whether they use PIMS.[1106] Considering that such intermediaries are held to be inexistent in moment, it appears unclear what incentive § 26 TTDSG provides to create them.[1107] In any case, the effectiveness of this regulatory approach will considerably depend on interoperability and standardisation (see part D(II)(2)(e)(bb)).[1108]

Commentators have argued that the benefits of the DGA could only be reached if it does not only impose obligations on DIS, but also imposes obligations for market actors to make use of such services.[1109] Indeed, if the law requires consumers to buy a particular product, this could (artificially) create the demand for this product to an extent it would incentivise suppliers to enter the markets and offer such product. However, it appears questionable whether such invasive form of market design for data access can be justified in terms of efficiency reasoning

[1102] See Stiemerling/Weiß/Wendehorst, Forschungsgutachten zum Einwilligungsmanagement nach § 26 TTDSG, 2021, p. 21.

[1103] For proposals see Stiemerling/Weiß/Wendehorst, Forschungsgutachten zum Einwilligungsmanagement nach § 26 TTDSG, 2021.

[1104] See critical remark on the vagueness of the requirement and its relationship to the DGA Stiemerling/Weiß/Wendehorst, Forschungsgutachten zum Einwilligungsmanagement nach § 26 TTDSG, 2021, p. 21, fn. 13.

[1105] See Golland NJW 2021, 2238 (2241).

[1106] See Golland NJW 2021, 2238 (2241).

[1107] See Blankertz/Specht-Riemenschneider, Wie eine Regulierung für Datentreuhänder aussehen sollte, 2021, p. 10–11.

[1108] For proposed details see Stiemerling/Weiß/Wendehorst, Forschungsgutachten zum Einwilligungsmanagement nach § 26 TTDSG, 2021.

[1109] See Specht-Riemenschneider/Kerber, Designing Data Trustees, 2022, p. 42.

but could instead only be based on public policy grounds. Answering this question lies beyond the subject of this study; but in any case, for such approaches sector-specific access regulation would be well placed, while significant evidence is needed to justify such cutting market intervention.

G. Policy recommendations

I. Cross-cutting issues

Given the increasing relevance of data for competition and innovation, undertakings have started to explore and develop their potential in a multitude of ways, sometimes striving to use 'their' datasets exclusively, sometimes by engaging in cooperation, sometimes by sharing and exchanging data. In principle, undertakings are free to choose their own strategy in trying to discover new uses of data.

Contrary to the U.S., the EU is adopting a pro-active stance in trying to develop a legal framework for the emerging data economy, with the aim to promote its emergence. Supporting the ongoing transformation by promoting legal certainty is a valid approach in principle. Yet, the emerging legal framework suggests that the EU must take care to ensure (1) coherence across its various legal projects, both with regard to the legal terminology and conceptually; and (2) flexibility, such as to allow for experimentation and adaptation.

Implicitly, the emerging legal framework recognises that de facto data holders can economically exploit 'their' data within the limits drawn by, *inter alia*, the GDPR, the law on trade secrets, the competition rules on information exchange etc. When it comes to data generated by the use of a product or service, a principle appears to be emerging that the product or service user shall have a right to port and use those 'co-generated' usage data, too, and to share it with third parties. For data generated by the use of a machine, this principle is generally recognised by the Draft Data Act. For personal data, it is established by Article 20 GDPR. For data generated by the use of a service, the principle is set out in Article 6 No. 9 and 10 DMA – albeit only vis-à-vis gatekeepers. § 19a(2) No. 5 GWB empowers the Bundeskartellamt to impose such obligations on undertakings of paramount cross-market significance for competition. It will need to be clarified why the access right is recognised broadly and strongly with regard to data generated by the use of a product, also broadly, but in a relatively weak form, with regard to personal data by the GDPR, but only selectively – namely only contingent on a specific position of market power – with regard to data generated by the use of services.

Data are a highly heterogeneous resource. The widespread analogy with raw oil is misleading in this regard. The emerging legal framework implicitly recognises that data are different, and that, consequently, a differentiated approach to data access is needed. There is broad agreement that, while access to 'observed' data may need to be granted, a different balancing of interests will be required when it comes to the sharing of 'derived' data.

These differences notwithstanding, general principles will need to be developed when it comes to the implementation of data access – principles that will need to take on board the insights gained from analysing data from a contract law perspective, from an IP perspective and from a competition law perspective.

Wherever data access is at issue, the lack of information of the non-data holder regarding what datasets exist, their structure and format must need to be considered. Some informational duties already follow from the P2B Regulation, the Draft Data Act and may be implicit in contract law. But it may be helpful to consolidate and expand them.

Also, standard terms of contract for data access will need to be developed that can be relevant in all settings – whether data are shared voluntarily, as part of a commitment, or based on a data access obligation. Jointly with such standard terms, general principles may be needed regarding the limits of data access as they may follow from the GDPR, the law on trade secrets or the competition law on information exchanges. In all these respects, the goal should be 'practical concordance': data access shall be enabled, while providing a technical and legal framework that allows for an adequate degree of protection for countervailing goals.

Wherever data access is mandated, due account must also be given to the question of *how* data access is achieved. Overarching guiding principles of legal, technical and institutional governance of data access regimes still need to be developed. Among other things, data access will need to be granted on FRAND terms. However, we have shown that the meaning of FRAND may somewhat differ when it comes to access to data as compared to access to SEP. Furthermore, standardisation of data formats and interfaces will be needed to make data portability, data interoperability and data access an effective and a widely available feature within the data economy. The way data access is granted may differ. Sometimes, it will be granted in situ, possibly on the basis of queries, in other situations, data will in fact be ported. Various data governance regimes will need to be developed, possibly, sometimes, with an expanded role for data intermediaries.

From a competition law perspective, the emergence of workable data governance regimes will be essential for making data access effective wherever it must be mandated for undertakings to compete effectively. The debate on data access in ecosystems and data-driven markets will need to be accompanied by the development of well-functioning data governance regimes.

More specifically, we submit the following recommendations:

II. The role of the state

1. The aim of instilling more trust in the digital economy is an important policy objective. But the numerous regulatory initiatives launched by the European Commission with a view to establishing a regulatory framework for the data economy represent a challenge for the targeted companies and sectors. The market for data (sharing) is only emerging. In many respects, the direction of its development is not yet foreseeable. Hence, we recommend some caution in initiating further initiatives. Moreover, these further initiatives have to be closely coordinated with the current regulatory framework to avoid incoherence and too much uncertainty. In particular, a consistent terminology is recommended. Furthermore, the regulatory initiatives should contain some degree of reflexivity and agility, i.e. initial proposals should be adapted or withdrawn if the

targeted markets develop in other directions. In this context, instruments, such as regulatory sandboxes could be used as a discovery procedure mainly in sector-specific contexts before establishing a horizontal regulatory framework.

III. Contract law

2. The markets for data sharing are just emerging in Germany and in Europe. The current legislative proposals, especially the Data Act and DMA, will further push the development in the coming years. Legislatures should build upon the contract practices and model terms generated by the actors on the markets when drafting default rules for data sharing contracts. The generation of such model contract terms should be supported by the European Commission, as proposed in the Data Act. German and European legislation should not go beyond such a development of model contract terms before the markets have started to develop contract practices. Mandatory provisions should only be enacted where clear indications for market failures are observed. The European or German legislature should consider to implement transparency obligations com-parable to Article 3 Data Act and Article 9 Fairness and Transparency Regulation for scenarios that are not covered by the two instruments, most importantly for co-generated data which is gen-erated by the use of a service.

IV. Data Act

We recommend that the German government should support the Draft Data Act in principle. However, the following points merit consideration:

3. In light of the goals of the Draft Data Act, the mandatory, non-waivable nature of the product user's access right in Article 4(1) should be reconsidered. An alternative approach would be to allow product users, absent a legally relevant asymmetry of power, to contractually waive their rights of access as long as the product user retains the right to revoke this waiver after some time.

4. The non-compete clauses in Articles 4(4) and Article 6(2) lit. e of the Draft Data Act are overbroad and should be reconsidered.

5. Article 4(6) of the Draft Data Act, which makes a data holder's use of the data depend on a contractual agreement with the product user, needs to be redrafted. In principle, both the data holder and the product user should have an independent right of use regarding the data.

6. The technical side of data access must be further specified.

7. The Draft Data Act should clarify that private enforcement by the product user and third parties is permitted.

V. Competition law

8. With regard to enhancing legal certainty for data sharing agreements under competition law (Article 101 TFEU), we suggest being cautious with the implementation of a 'Data-BER' until more robust guiding principles are developed. Precedents will be needed to get a better idea of which types of arrangements create risks of collusion, which data governance regimes are workable etc.

9. In order to develop guiding principles for assessing data sharing agreements under Article 101 TFEU, we recommend supporting a more 'informal guidance' mechanism at the EU level. While the regime under § 32c GWB seems to work well, a § 32c GWB-decision does not protect against a prohibition by the EU Commission. The draft revised Commission Notice on Informal Guidance has the potential of upgrading the current system, but falls short of providing a procedural framework that would fully realize this potential. A more participatory regime, including a kind of 'regulatory dialogue' with all relevant stakeholders and involving not only lawyers but also economists and data scientists may be needed to develop a special framework to accompany the emerging practices in a sufficiently quick and flexible manner.

10. Currently, we see no need to change §§ 19, 20 GWB with regard to data access. In principle, the legislator should await the emerging case law and then to engage in a thorough ex post evaluation ('evidence-based antitrust'). However, the legislator may want to highlight specific settings in which refusals to grant access to data may constitute an abuse beyond the preconditions set out in § 19(2) No. 4 GWB – whether under § 19(1) and (2) No. 1 GWB and/or under § 20(1a) GWB.

11. More particularly, we propose that further-reaching data sharing obligations may follow from § 19(1) and (2) No. 1 GWB and/or § 20(1a) GWB in two settings: firstly, an orchestrator of an ecosystem in which data functions as an important link between the various segments or markets may be under a special obligation to grant access to data to those users of the ecosystem that contribute to the generation of the data and to the success of the ecosystem. Primarily, there will be an obligation to grant users access to the individual level data which is generated on the basis of their activity (scenario 1). But in the presence of a vertically integrated ecosystem orchestrator who uses aggregate data to compete and provided a clear and long-term lack of outside options, there may also be an obligation to provide access to bundled individual level or aggregate data (scenario 2) to other business users on FRAND terms such as to enable them to compete effectively. Care must be taken to ensure that such access to data does not conflict with Article 101 TFEU / § 1 GWB, however. Secondly, special data-sharing obligations may be justified in data-driven markets.

12. With regard to the question whether all undertakings shall benefit symmetrically from data access where data sharing obligations follow from § 19 GWB, or whether gatekeepers within the meaning of the DMA or undertakings of paramount cross-market

significance for competition according to § 19a GWB should be excluded, we recommend considering a more differentiated approach: data access of such undertakings should be conditional upon their commitment to open up their own data troves to competitors on FRAND terms. Such conditionality could be introduced by amending § 19a GWB.

13. Where competition law obliges undertakings with relevant market power to share data, an effective implementation of this obligation will be of the essence. Developing and implementing effective data governance regimes – including FRAND conditions – may be highly complex and sensitive to specificities of a given sector, however. While this will frequently argue for sector-specific regulation, it may be a task for competition law to help establish a set of horizontal legal principles that such regimes should follow. In addition, we propose to develop guidance on how to effectively comply with other legal regimes (e.g. Article 101 TFEU or the GDPR) when implementing data access obligations.

VI. Merger control

14. The German legislature should consider decreasing the § 35(1a) No. 3 GWB notification threshold – from 400 Mio. EUR down to e.g. 200 Mio. EUR – to enlarge the number of transactions that would fall under German merger review and could therefore potentially be referred to the EU-Commission under Article 22 EUMR.

15. The German legislature should consider updating and strengthening the current merger review regime and enforcement with particular regard to data-driven markets and digital ecosystems. Such regulatory recalibration would need further, more targeted analysis and consultation. In particular, the legislature should consider modifying substantive rules of merger review with regard to undertakings of paramount significance for competition across markets according to § 19a(1) GWB. This would include considering the effects a merger would have on the whole 'ecosystem' and inquiring into the question whether impediments to effective competition shall be already presumed if a notified transaction were to enable an undertaking under § 19a(1) GWB to acquire more or new data, or if it would make data collection more efficient. A more differentiated presumption could be particularly sceptic to acquisitions that involve services/products that complement each other. Corresponding with the modified substantive requirements, the burden of proof would need adjustment and follow a more differentiated approach.

16. The German government should advocate a reform of merger control at EU level, which would address the substantial review criteria as well as the relationship with national rules and notification thresholds, and which would also require an update of the EU Merger Guidelines. Also, the current practice of the EU Commission to accept commitments on data access, data separation and interoperability should be

reconsidered. Such behavioral commitments should not be accepted in data-related mergers that involve big tech players. Future reforms on the EU level should consider an explicit provision that only structural remedies are permissible in such cases.

VII. DMA/§ 19a GWB

17. The success of the DMA's data access (and in particular: data portability) regime in promoting data-driven innovation and competition in complementary markets will largely depend upon its effective implementation. We recommend that the European Commission pro-actively ensures an open and participatory standardisation process for developing data formats and open interfaces via standardisation requests that includes all relevant stakeholders. As the data economy is still at an early stage, it is essential to monitor the workability and effects of the standards and to ensure that they can be flexibly adapted. A 'participatory' enforcement regime is advisable in this regard.

18. § 19a(2), 1st sentence, No. 5 GWB may continue to play a role alongside the DMA when it comes to the portability of data generated by the use of non-core platform services (or where § 19aGWB designates norm addressees that are not gatekeepers under the DMA). The procedures for implementing data portability under § 19a(2), 1st sentence, No. 5 GWB remains to be developed in these cases. The commitment decision procedure under § 32b GWB may provide a role model.

19. Neither the DMA nor § 19a(2) GWB provide for the imposition of data access obligations of the scenario 2-type. We propose that the possibility of imposing such obligations should be considered (but no "one size fits all"-solution is appropriate in this regard).

VIII. Data Intermediaries

20. The regulatory effects of the DGA are highly unpredictable. In view of the Commission's future evaluation and review of the DGA, the German Government should gather evidence on the market developments in the upcoming years to come up with suggestions for necessary amendments of the Regulation.

21. The general legal framework should facilitate the development of data intermediaries by coherently integrating them into the legal orders of the EU and the Member States. For this purpose, EU and national legislature and competition authorities should consider the following: design data protection rules to effectively integrate data intermediaries in the market order for data sharing; better sync data intermediaries with contract law and FRAND principles, e.g. by extending Article 8(1) Data Act also to DIS under Article 12(f) DGA; refer to data intermediaries and clarify their role under the Data Act; consider data intermediaries as a tool to strengthen the structural effect of merger remedies to prevent data and market concentration; consider the constructive

role of guidance with regards to Art. 101 TFEU, which can increase legal certainty for evolving data intermediation models; to consider introducing stricter, sector-specific rules for data intermediaries only if suggested by strong evidence of market failure or clearly justified under public policy grounds.