Research Article

Matthias Leistner and Lucie Antoine*

IP Law and Policy for the Data Economy in the EU

https://doi.org/10.1515/econ-2022-0043
received August 06, 2022; accepted June 15, 2023

Abstract: The current policy vision for Europe's digital future centres around facilitating the availability of data by means of data access, sharing, and portability rights. In the existing legal framework, such rights are already foreseen in different legal instruments. In actual practice, however, (horizontal) data sharing is governed in the first place by contracts. Currently, well-established business practices and non-mandatory model contract terms are lacking. To reduce transaction costs and chilling effects in the sector, the main task would therefore be to provide a set of non-mandatory default rules or soft-law model contracts. The database maker's sui generis right or trade secrets protection, mainstays of this area, have the potential to aggravate access problems and hamper efficient access and portability regimes. While the Trade Secrets Directive as a very modern and necessarily flexible instrument, on principle, is rather well-equipped for achieving balanced results, the Database Directive is in imminent need of reform, in particular as even the Data Act Proposal leaves many issues of the database sui generis right unsolved.

Keywords: intellectual property, data economy, data act, digital industries, regulation, European Union

1 Acceptance of the Access and Portability Perspective in the European Union

Since 2015, both the legal and the political debate on fostering the development of data markets in the EU has shifted from an incentive-oriented "property" approach to a competition-oriented institutional analysis of existing and future problems in data markets. The *access* to and the *portability* of data, the *incentives* for data sharing, and the necessary *infrastructure*, such as interoperability and data quality, have thereby been identified as key issues for establishing a European data economy. Various seminal reports (Crémer et al., 2019; Furman et al., 2019) and an intense discussion (e.g. Drexl, 2018; Drexl et al., 2017; Kerber, 2016; Leistner, 2017, 2021a; Leistner et al., 2021; Schweitzer & Welker, 2021) in academia, policy and practice laid the foundation for the Commission's sweeping project to develop a regulatory framework for Europe's digital and data-driven future.

As a result, the Data Strategy (European Commission, 2020) of early 2020 defined the objectives of facilitating the availability of data by means of data access and sharing (G2B, B2G, B2C, and B2B), establishing a data governance structure, reducing technical barriers and tackling market imbalances. In winter 2020, the 'Digital Services Package' (see further Eifert et al., 2021; Leistner, 2021b), consisting of the Data Governance Act, the Digital Markets Act, and the Digital Services Act, was presented as a first step for pursuing these goals. All three Regulations meanwhile have entered into force.

With the proposal for a Data Act in February 2022, the Commission has presented a further cornerstone of its strategy for a data-driven economy. In June 2023 a political agreement has been reached during the trialogue negotiations; the final text is expected to be adopted in autumn. After giving an overview of the existing framework and current challenges with regard to data (see below 2), we will also take a brief (comprehensively, Leistner & Antoine, 2022) look at the new approaches in the Data Act proposal (see below 3).

2 Existing Regulatory Framework

From an IP perspective, the question arises which role is played by the various IP instruments for protecting data collections, such as particularly the *database sui generis right* and the protection of *trade secrets*. Obviously, these existing protection instruments can come into conflict with

*** Corresponding author: Lucie Antoine,** Chair for Private Law and Intellectual Property Law, with Information and IT-Law, Ludwig Maximilian University Munich, Munich, Germany,
e-mail: lucie.antoine@jura.uni-muenchen.de
Matthias Leistner: Chair for Private Law and Intellectual Property Law, with Information and IT-Law, Ludwig Maximilian University Munich, Munich, Germany

or at least have an impact on existing and future access, portability, and sharing liberties or rights. In that sense, IP rights constitute an institutional infrastructure. But is that infrastructure balanced, proportionate, and effective? Does it interfere with the general objective to facilitate access to and availability of data? And how can the different objectives be balanced against each other? To answer these questions and to briefly evaluate the Data Act proposal in light of "our" answers, we will first give a brief overview of the instruments of protection potentially applying to data collections (see below 2.1), before we address the current legal framework on data access, sharing, and portability and its relation to IP and trade secrets – covering the status quo as well as possible ways ahead (see below 2.2).

2.1 Protection of Data Collections by IP Rights and as Trade Secret

Data collections can in particular be protected under the database maker's sui generis right according to Art. 7 of the Database Directive (96/9/EC) or as a trade secret under the conditions of the Trade Secrets Directive ((EU) 2016/943).

2.1.1 Database Sui Generis Right – Broad Scope and Legal Uncertainty

The *database sui generis right* aims at protecting the database makers' investment in a database by means of an exclusive right. Pursuant to Art. 7 (1) Database Directive, any substantial investment in obtaining, verification, or presentation of the contents of a database gives rise to the database maker's right to prevent extraction and/or re-utilisation of the whole or of a substantial part of the contents of that database. As the European Court of Justice (ECJ) interprets the definition of 'database' very extensively (Freistaat Bayern v. Verlag Esterbauer, 2015, paras 18 et seq.), the vast majority of data sets aggregated in a data-driven economy in principle qualify for protection as database (Drexl, 2018, p. 67 et seq.; also Leistner, 2017, p. 27 et seq.; 2021a, p. 226 et seq.). Furthermore, the substantive threshold of database sui generis protection, i.e. the requirement of a '*substantial investment*', is rather low (Leistner, 2017, p. 30).

The decisive criterion for possible protection under the sui generis right has, therefore, become whether the investment concerned the *collection* or mere *creation* of a database's content. This distinction has been introduced by the ECJ in order to prevent protection by the exclusive right in sole source situations in which data are solely available from one particular source and cannot be obtained with comparable investments by another competitor or market participant otherwise (British Horseracing Board v. Hill, 2004, paras. 30 et seq.; Fixtures Marketing v. Oy Veikkaus, 2004; Fixtures Marketing v. Svenska Spel, 2004; Fixtures Marketing v. Organismos prognostikon, 2004). Parts of the literature have interpreted the ECJ's argumentation (that investments in the *creation* of data, which is, for instance, collected as a mere by-product of another main activity (spin off-situations), cannot qualify for sui generis protection) in a strict way, as to generally exclude machine-generated data from the scope of Art. 7 Database Directive. But, as we have pointed out elsewhere, this is by no means sure: First, the ECJ's interpretation was in principle tailored to sole-source situations, and second, numerous national courts have already recognised certain investments in necessary technical infrastructure for measuring, obtaining, or documenting existing data as sufficient for a protection under the sui generis right (German Federal Supreme Court (BGH), HIT Bilanz, 2005 and Autobahnmaut, 2010; Austrian Federal Supreme Court (OGH), 2015).

If this line of case law were further followed or even generalised by the ECJ in the future, most IoT data (and many others) would certainly qualify for protection, if based on substantial investments into the installation of sensors and similar measuring infrastructure (being regarded as investments into the collection of [physically] existing data in nature or of technical processes). Thus, this problem needed to be addressed (see already European Commission, 2022, pp. 15 et seq., 131 et seq.; Leistner, 2017, p. 27 et seq.). And indeed, in order to resolve the current legal uncertainty regarding the sui generis right's conditions of protection, the proposal for a Data Act initially contained an explicit provision to clarify the sui generis right's scope with respect to machine-generated data in Art. 35, which, albeit, followed a very sector-specific and limited approach to the problem (Derclaye & Husovec, 2022; see also below 4). However, both European Parliament and Council watered the provision down even further to solely exclude the applicability of the database sui generis right for the purposes of the Data Act. That would mean to miss a unique opportunity to clarify the scope of the database sui generis right and to reduce legal uncertainty significantly. Meanwhile, it seems that at least machine-generated data shall be generally excluded from the scope of the sui generis right. This, in turn, leaves certain crucial, more technical questions open, such as the question of whether the new provision would have a retroactive effect or not.

2.1.2 Trade Secrets Protection – A Flexible "Newcomer" with Growing Importance

Besides the database sui generis right – and in practice of even larger importance – *trade secrets protection* can extend in principle to all data collections (Aplin, 2017). Whereas the Database Directive dates back to 1991, the Trade Secrets Directive harmonised the protection of trade secrets in the EU only in 2016. Being thus a relatively "new" piece of legislation, the Trade Secrets Directive, on principle, offers sufficient flexibility to address the needs of a data-driven economy.

The protection of trade secrets is based on the consideration that incomplete information constitutes an indispensable prerequisite for functioning competition so that in particular market-related information has to be protected against unlawful acquisition, disclosure, and use. In addition, trade secrets protection – even though not an exclusive right – aims at reducing transaction costs for factual protection measures and at facilitating access to information by means of licencing contracts. Pursuant to Art. 2 (1) of the Trade Secrets Directive, information can be protected as a trade secret if it is not generally known, has commercial value due to its secrecy and is subject to reasonable steps to keep it secret. Due to this broad definition, diverse types of data sets but also algorithms and program codes needed for the processing of data are eligible for trade secrets protection if the requirements of Art. 2 (1) Trade Secrets Directive are fulfilled (Leistner, 2021a, p. 219 et seq.).

2.1.3 The Impact of Protection Instruments on Access, Use, and Portability of Data

Because of their far-reaching applicability in data-driven business scenarios, both the database sui generis right and trade secrets protection have the potential to create hold-up situations and to aggravate access problems in certain situations. Based on empirical evidence, the database sui generis right's unclear scope with regard to machine-generated data has been identified as an important obstacle for data sharing in the IoT sector, for instance, due to the risk that sui generis protection is invoked 'opportunistically' in order to 'block' data access (see European Commission, 2022, p. 15 et seq.). Looking at trade secrets protection for data, a clear answer cannot be given yet: according to a recent study on the legal protection of trade secrets in the data economy, there is still no unambiguous evidence for the question of whether trade secrets protection facilitates or – in certain situations – may hamper data sharing (Radauer et al., 2022).

As a consequence, precise identification of justified access requirements and the resulting actual or potential problem zones at the interface to IP protection is necessary, and in regard to such concretely identified actual or potential problem zones, an equitable balance between existing and future data access, use, and sharing liberties or rights on the one hand, and the existing protection instruments on the rightholders' side on the other hand, has to be found.

2.2 Access, Use, and Portability of Data

2.2.1 The Status Quo

Under the existing acquis, data access, portability, and sharing are primarily governed by contract law, general competition law, certain very limited sector-specific instruments, and – in relation to personal data – by the General Data Protection Regulation (GDPR).

Art. 20 GDPR has introduced a claim to the portability of personal data as an individual right of the data subject. This entails the right to request the porting of volunteered and observed personal data from one controller to another. Even though Art. 20 GDPR also expresses the GDPR's objective to safeguard the fundamental right to protection of personal data (Art. 8 (1) Charter of Fundamental Rights of the European Union; Art. 16 (1) TFEU), the implementation of the portability right was driven by the objective to reduce lock-in effects and thus reflects a robust pro-competitive approach (Metzger, 2021, p. 295). As a result, Art. 20 GDPR became the centre of a lively debate about whether portability rights should be applied broadly in order to foster the development of data markets. Currently, however, Art. 20 GDPR is not very effective in practice. This is partly due to certain shortcomings of the provision, namely its limited scope (not covering real-time access and inferred data). Most importantly, the practical difficulties resulting from a lack of interoperability prevent effective implementation of the portability right. Business models, which would be based on this right, such as porting services, do exist in certain fields (e.g. *Soundiiz*, *Freeyourmusic* or *Songshift* offer porting services with regard to music streaming platforms) but are still scarce. As regards potential conflicts with IP rights or trade secrets of the controller or third parties, Art. 20 (4) GDPR provides for a 'balancing of interest' clause which leaves sufficient room for a flexible and equitable interpretation.

Besides certain sector-specific regulations (further Graef et al., 2020), access to data in B2B relations can primarily be granted under the rather strict conditions of *general competition law*. Pursuant to the requirements

established for IP rights in the ECJ's Magill judgment (RTE and ITP v. Commission, 1995) and since then consolidated and cautiously broadened in IMS Health (IMS Health v. NDC, 2004) and Microsoft (Court of First Instance, Microsoft v. Commission, 2007), a claim to a compulsory licence can be based on Art. 102 TFEU where a data holder with a dominant market position (in an actual or even a hypothetical upstream licencing market) refuses, without objective reason, access to data which is indispensable to compete in a downstream market with the effect that any competition on that market is eliminated, thereby preventing the emergence of a new product or service[1] (Microsoft v. Commission, 2007, paras 643 et seq.) for which there is a potential consumer demand (ECJ, Bronner v. Mediaprint, 1998, para. 40; IMS Health v. NDC, 2004, paras 38, 48 et seq.). In short, Art. 102 TFEU, on the one hand, solely applies to market-dominant firms controlling indispensable data and has, therefore, no effect below this threshold which significantly limits the impact of that provision. On the other hand, compulsory licences under that provision entail, first, even access to information protected as a trade secret (Microsoft v. Commission, 2007, para. 289) and, second, not only access but also the use of the information protected by IP rights or as a trade secret by a competitor of the data holder and, thus, can promote innovation even if this leads to innovative products or services in competition[2] with the products or services of the data holder.

The *Digital Markets Act* implements further access and portability rights. The DMA, however, only applies in relation to so-called *gatekeepers*. Gatekeepers are very narrowly defined in the Regulation. Practically, the DMA only applies to the GAFAM companies plus presumably a handful of companies of comparable size and impact. Art. 6 (9) contains the right for business users and end users to port data provided or generated in the context of their use, thus volunteered and observed data, including continuous and real-time access. In addition, Art. 6 (10) foresees a right to data access for business platform users free of charge, with effective, high-quality, continuous, and real-time access, including inferred data from such use in aggregated or non-aggregated form. Whereas these two provisions enable users to access and port *individual-level use data*, Art. 6 (11) introduces a sector-specific access right for search engine providers to ranking, query, click, and view data – thus, aggregated data – of the gatekeeper under FRAND terms. Notably, Art. 6 (11) allows for access to aggregated data even for search engine providers which directly compete with the gatekeeper (and data holder).

In European *contract law*, access to individual-level data in B2C relations is provided solely by the Digital Contents Directive ((EU) 2019/770), which provides for a post-contractual portability right for non-personal data in Art. 16 (4). With respect to B2B relations, a right to access and portability of individual-level use data does so far not exist in European contract law. However, the *Platform to Business Regulation* ((EU) 2019/1150) stipulated certain transparency obligations for platform providers in relation to business users concerning contractual and technical access to volunteered and observed data of the user (further Schweitzer et al., 2022, p. 130).

Horizontal data access and sharing is primarily based on contractual agreements (European Commission, 2022, p. 17; OECD, 2019, p. 101). Whereas so far neither well-established business practices nor model contract terms exist (Schweitzer et al., 2022, p. 273 et seq.), in the recent years several soft law instruments have been developed in order to provide guidance (American Law Institute and European Law Institute, 2021; European Commission, 2018). Nonetheless, contracting 'on data' is still characterised by significant information and transaction costs as well as legal uncertainty in the EU market.

2.2.2 The Way Forward

Meanwhile, certain case groups can be distilled from the academic and policy discussion in which actual or potential market failure seems conceivable and access, sharing, and use rights might therefore be justifiable. The first case group refers to access, use, and portability of individual-level data that is collected by a producer or service provider. The second case group concerns access of competitors to complete, aggregated data sets, where this is necessary in order to establish workable competition in aftermarkets or complementary markets. The third case group relates to access to large aggregated datasets held by big data conglomerates necessary for the development of innovative unrelated products or services, e.g. in the context of AI (Crémer et al., 2019, p. 75 et seq.).

As described earlier, the currently existing statutory EU framework of access, use, and portability rights does particularly address the first case group, hence, *access to individual-level use data* which has been provided by a data

1 This requirement has in fact been watered down to a requirement of prevention of the emergence of a better or more efficient product in the Microsoft judgement.

2 This is because in IMS Health the ECJ accepted a dominant position (of the IP holder) in a mere hypothetical upstream market as sufficient basis for a compulsory license although the license seeker needed the essential IP protected information because it was objectively necessary to compete with the services of the IP holder in the downstream services market.

subject/user or observed by a provider – such access rights mainly address *switching cost problems (lock in) or access to data in order to provide individual aftermarket services*. Existing mechanisms in EU law are Art. 20 GDPR (personal data), Art. 16 (4) Digital Contents Directive (on B2C post-contractual level), as well as Arts. 6 (9) and (10) of the Digital Markets Act (in relation to gatekeepers).

General EU competition law can under certain conditions reach further: it can not only mandate access to (and use of) individual-level data but also under certain conditions grant access for competitors to aggregated datasets where this is objectively indispensable for innovation in a downstream market, which can even be the market, where the data holder offers products or services, since any downstream market in relation to the upstream market for data licences will suffice even if the latter is a hypothetical market (Crémer et al., 2019, p. 102 et seq.; Schweitzer & Welker, 2021, p. 141 et seq.). However, Art. 102 TFEU applies only in relation to *market dominant firms* (and as far as the further requirements for a compulsory licence are fulfilled). Thus, essentially, Art. 6 (11) of the Digital Markets Act is the only current provision in the European data *acquis* covering access to (certain) aggregated datasets which extends even to directly competing search engine providers.

In sum, current EU law is characterised by a differentiated IP protection situation which is balanced as regards the 'classic' IP rights as well as trade secrets protection, but which reveals certain problematic uncertainties and tendencies to over-protection as regards the database maker's sui generis right laid down in the Database Directive of 1996 (European Commission, 2022, pp. 15 et seq., 131 et seq.). As for access rights, certain sector-specific access rights in regard to individual level data help reduce switching costs and do allow for certain specific aftermarket services (further Schweitzer & Welker, p. 115 et seq., with examples). By contrast, broader access rights to foster data markets and in particular sharing and use of data in order to develop innovative products or services are not yet broadly foreseen. In regard to this latter objective, the Digital Markets Act introduces some limited data access rights in relation to so-called *gatekeepers*. Besides, compulsory licences can be based on Art. 102 TFEU (i.e. general competition law), albeit only in relation to dominant firms and under certain additional conditions.

3 New Directions: The Envisaged Data Act

Against this background, the most recent proposal for a Data Act, which was published on 23 February 2022, with its main focus on access to, sharing, and use of IoT data, leaves mixed impressions. The Data Act proposal was widely expected to implement a far-reaching, horizontal framework for data sharing in general.

However, the Data Act (in its part on data access, sharing, and use – Ch. II, III) essentially addresses but one particular constellation: access, sharing, and use of individual-level data that is "co-generated" by the use of connected (IoT) products and related services. According to Art. 4 (1) of the proposal, any *user*, being a natural or legal person, has the right to access and use data generated by its use of a product or related service, including in principle continuous and real-time access vis-à-vis the data holder. In addition, Art. 5 of the Data Act provides the user's right to 'authorise' *sharing* of the data generated by a product or related service *with a third party*. Both Art. 4 and Art. 5 only cover volunteered and observed data. However, they do not apply to inferred data – thus excluding the most valuable data category for most actual innovative uses in the context of new business models (Kerber, 2022, p. 12; Leistner & Antoine, 2022, p. 84). With the foreseen mandatory rights (Art. 12 (2)), the Data Act intends to propose a 'cooperative market-model' for co-generated data in the IoT sector, allotting a central role to the users of data-collecting products and related services (Leistner & Antoine, 2022, pp. 16 et seq., 77 et seq.; Schweitzer et al., 2022, p. 209 et seq.). This model shall apply to the entire IoT 'sector', thus to B2C and B2B relations alike. Only small and micro enterprises as data holders are exempted from the obligation to make data available, respectively.

The Data Act follows the objective to open certain secondary markets (aftermarkets for IoT-related services, such as maintenance and repair, insurances, etc.) by facilitating access, use, and sharing of co-generated IoT data. Insofar, the user's access right set forth in Art. 4 might be a consequent instrument to facilitate the user's access to individual-level data (first case group). In addition, the right for sharing data with third parties pursuant to Art. 5 to a certain limited extent indirectly covers the second case group of data access necessary for establishing workable competition in aftermarkets. In that regard, the Data Act cautiously limits the possible function of the sharing and use rights: the shared data must not be used to develop products or services which are in competition with the data holders' products (further Leistner & Antoine, 2022, p. 88 et seq.).

Even with these limitations in mind, the *sweeping scope and generalising character of the proposed Data Act*, which shall cover the entire IoT sector with a mandatory law-based regulation and might thus risk to level

necessary differentiations in particular sectors, seems at least remarkable and will have to be reconsidered in the future legislative discussion.

Further, it seems equally surprising that this new mandatory law framework shall apply to *B2C and B2B relations alike* (Kerber, 2022, p. 25; Leistner & Antoine, 2022, pp. 16 et seq., 80 et seq.). In fact, in regard to B2B relations, even if this was meant to be a "sandbox" market design approach (albeit in this case with a rather over-sized "sandbox"), such market design approach might arguably better be followed by way of a non-mandatory framework of default rules. By contrast, mandatory law risks to prevent certain efficient data contracts in this sector, where, e.g. newcomers to the IoT market can only offer their products and related services on condition of an individually negotiated limited exclusivity of use period concerning the generated data.

While these two aspects seem to indicate that the current scope and general character of the proposed Data Act follows too broad an approach, at the same time, paradoxically, the access, sharing, and use rights proposed in the Data Act are at the same time inherently *limited* in a way which puts the future effectivity of this legal framework into certain doubt (Kerber, 2022, p. 2; Leistner & Antoine, 2022, p. 77 et seq.; Schweitzer et al., 2022, p. 213 et seq.). This concerns, first, the limitation to *volunteered and captured data* as such and the resulting exclusion of any inferred data, such as particularly valuable standardised or contextualised data sets (Drexl et al., 2022, paras. 24 et seq.). Second, the exclusion of any reuse of the data to develop products or services *which are in competition with the data holder's products* essentially limits the impact of the act to the mere use scenario of certain aftermarket services for IoT products – in result, the broader case group of access to larger data sets in the interest of certain *innovative* uses and business models remains entirely unaddressed (Leistner & Antoine, 2022, p. 88 et seq.; Schweitzer et al., 2022, p. 211 et seq.). Third, in order to unlock the full potential of the proposed "sector-specific" market-model, the role of the data holder for upstream data sharing should equally be taken into view instead of almost exclusively focusing on the users' position (cf. Drexl et al., 2022, paras. 45 et seq.; Leistner & Antoine, 2022, p. 92 et seq.; Schweitzer & others, 2022, p. 216). Allocating the right to share and reuse data to the downstream *users alone* seems inefficient as often the upstream data holders will be in a better position to initiate data sharing and to deliver essential data to innovative businesses seeking such necessary data.

Even though many academic authors have criticised the general conception of the Data Act (e.g. contributions of Drexl et al., 2022; Efroni et al., 2022; Graef & Husovec, 2022; Kerber, 2022; Leistner & Antoine, 2022; Schweitzer et al., 2022), the proposed cooperative model for data generated by IoT products – as a strategic (political) decision – remained in principle untouched during the legislative process. Instead, the role of trade secrets has been emphasised as a possible defence against the newly proposed data access and sharing provisions, which might turn out to make the proposed new access and sharing regime even less efficient. If the Act comes into force in its current form, it will allow for interesting natural experiments, such as concerning the question of whether it does indeed foster enhanced data sharing in different specific sectors and how it actually changes the cost–benefit calculus for such endeavours.

4 Conclusions

The current policy vision for Europe's digital future centres around the objective to facilitate the availability of data by means of data access, sharing, and portability rights. In the existing legal framework, such rights are already foreseen in different legal instruments covering in particular access to and portability of individual-use level data. Beyond that, primarily general competition law can provide for B2B access in relation to market-dominant data holders under the conditions of Art. 102 TFEU. European contract law, hitherto, does not contain a general access or portability right beyond certain B2C instruments. In actual practice, however, (horizontal) data sharing is governed in the first place by contracts. Currently, well-established business practices and non-mandatory model contract terms are lacking. Only some soft law instruments (best practices) give guidance, albeit on a rather high level without providing for detailed (default) contractual clauses. To reduce transaction costs in the sector and thus to increase businesses' willingness to engage in data sharing and use, the main task would therefore be to provide a set of non-mandatory default rules or soft-law model contracts.

As data collections can in principle be subject to the database maker's sui generis right or trade secrets protection, these rights have the potential to aggravate access problems and hamper efficient access and portability regimes as described above. While the Trade Secrets Directive as a very modern and necessarily flexible instrument, on principle, is rather well-equipped for achieving balanced results (because of its limited scope, applicable exceptions, and proportionate enforcement regime) the Database Directive is in need of reform. Since the Data Act in its current version solves this problem only for machine-

generated data that fall into the scope of the Act's new access and sharing regime, the related broader problems remain largely unsolved.

As for the general perspective of the future 'access rights' landscape in the EU, the current policy approaches leave a mixed impression. In the services sector, any new access rights and other competition-oriented instruments (as foreseen in the Digital Markets Act) are currently mainly targeted towards so-called gatekeepers, i.e. the GAFAM companies plus a handful of other platform businesses of comparable size and impact in the EU market. In the IoT sector, the recently proposed Data Act, by contrast, follows a horizontal approach covering B2C and B2B relations alike. Certain shortcomings of this newly proposed instrument have been listed in Section 3. above; this shall not be repeated here. However, another more general remark seems necessary: it seems fundamentally problematic that the Data Act only addresses IoT products and related services, while the *services sector in general* shall *only* be regulated by the DMA. This results in a certain imbalance: while the DMA essentially only addresses Big Tech, the proposed Data Act will in principle cover any IoT producer (with only some exemptions for micro- and small-sized enterprises). From our viewpoint, this makes the current EU policy for the data society askew as it leaves a legal vacuum for data-related services underneath the thresholds of gatekeepers (in the DMA) or market dominance (in general EU competition law). The European Parliament proposed a broader definition of 'related service' in the Data Act being potentially suitable to tackle this aspect. However, it remains to be seen how the final text defines the scope of the access and use rights in that regard. If the proposed Data Act shall indeed complete the jigsaw puzzle of the EU's regulatory approach to the data economy, the services sector will have to be addressed as well, and some of the key features of the new access and sharing regime should be revised very thoroughly.

Conflict of interest: Authors state no conflict of interest.

Article note: As part of the open assessment, reviews and the original submission are available as supplementary files on our website.

References

American Law Institute and European Law Institute. (2021). *ALI-ELI principles for a data economy – Data transactions and data rights*. ELI Final Council Draft. https://www.principlesforadataeconomy.org/fileadmin/user_upload/p_principlesforadataeconomy/Files/Principles_for_a_Data_Economy_ELI_Final_Council_Draft.pdf.

Aplin, T. (2017). Trading data in the digital economy: Trade secrets perspective. In S. Lohsse, R. Schulze, & D. Staudenmayer (Eds.), *Trading data in the digital economy: Legal concepts and tools* (pp. 59–72). Baden-Baden, Germany: Nomos.

Austrian Federal Supreme Court, 4 Ob 206/14 (2015).

Bently, L., Derclaye, E., Fisher R., Misojcic M., Chicot J., Domini A., … Calatrava Moreno M. (2018). *Study in support of the evaluation of Directive 96/9/EC on the legal protection of databases – Final Report*. https://op.europa.eu/de/publication-detail/-/publication/5e9c7a51-597c-11e8-ab41-01aa75ed71a1.

Crémer, J., de Montjoye, Y., & Schweitzer, H. (2019). *Competition Policy for the digital era – Final report*. https://ec.europa.eu/competition/publications/reports/kd0419345enn.pdf.

Derclaye, E., & Husovec, M. (2022). *Why the sui generis database clause in the Data Act is counter-productive and how to improve it?* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4052390.

Drexl, J. (2018). *Data Access and Control in the Era of Connected Devices – Study on Behalf of the European Consumer Organisation BEUC.* https://www.beuc.eu/sites/default/files/publications/beuc-x-2018-121_data_access_and_control_in_the_area_of_connected_devices.pdf.

Drexl, J., Hilty R., Globocnik J., Greiner F., Kim D., Richter H., … Wiedemann K. (2017). *Position Statement of the Max Planck Institute for Innovation and Competition of 26 April 2017 on the European Commission's 'Public consultation on Building the European Data Economy'*. Max Planck Institute for Innovation and Competition Research Paper No 17–08. https://www.ip.mpg.de/en/research/research-news/position-statement-public-consultation-on-building-the-european-data-economy.html.

Drexl, J., Banda C., González Otero B., Hoffmann J., Kim D., Kulhari S., … Wiedemann K. (2022). *Max Planck Institute for Innovation and Competition Position Statement 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)*. https://www.ip.mpg.de/fileadmin/ipmpg/content/stellungnahmen/Position_Statement_MPI_Data_Act_Formal__13.06.2022.pdf.

Efroni, Z., Hagen P., Völzmann L., Peter R., & Sattorov M. (2022). *Weizenbaum Institute for the Networked Society, Position Paper regarding Data Act.* https://www.ssoar.info/ssoar/handle/document/79542.

Eifert, M., Metzger A., Schweitzer H., & Wagner G. (2021). Taming The Giants: The DMA/DSA package. *Common Market Law Review*, *58*, 987–1028.

European Commission. (2018). *Towards a common European data space. COM(2018) 232 final. Accompanied by the more detailed Staff Working Document (2018). Guidance on sharing private sector data in the European data economy*. SWD/2018/125 final.

European Commission. (2020). *A European strategy for data*. COM(2020) 66 final.

European Commission. (2022). Commission Staff Working Document – Impact Assessment Report accompanying the document Proposal for a Regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data. (Data Act). SWD (2022) 34 final.

European Court of First Instance, Microsoft v. Commission, ECLI:EU:T:2007:289 (2007).

European Court of Justice, British Horseracing Board v. Hill, ECLI:EU:C:2004:695 (2004).

European Court of Justice, Bronner v. Mediaprint, ECLI:EU:C:1998:569 (1998).
European Court of Justice, Fixtures Marketing v. Organismos prognostikon, ECLI:EU:C:2004:697 (2004).
European Court of Justice, Fixtures Marketing v. Oy Veikkaus, ECLI:EU:C:2004:694 (2004).
European Court of Justice, Fixtures Marketing v. Svenska Spel, ECLI:EU:C:2004:696 (2004).
European Court of Justice, Freistaat Bayern v. Verlag Esterbauer, ECLI:EU:C:2015:735 (2015).
European Court of Justice, IMS Health v. NDC, ECLI:EU:C:2004:257 (2004).
European Court of Justice, RTE and ITP v. Commission, ECLI:EU:C:1995:98 (1995).
Furman, J., Coyle, D., Fletcher A., McAuley D., & Marsden P. (2019). *Unlocking digital competition – Report of the digital competition expert panel*. UK Government. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/785547/unlocking_digital_competition_furman_review_web.pdf.
German Federal Supreme Court, Autobahnmaut, I ZR 47/08 (2010).
German Federal Supreme Court, HIT Bilanz, I ZR 290/02 (2005).
Graef, I., & Husovec, M. (2022). *Seven things to improve in the data act*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4051793.
Graef, I., Husovec, M., & van den Boom, J. (2020). Spill-overs in data governance: Uncovering the uneasy relationship between the GDPR's right to data portability and eu sector-specific data access regimes. *Journal of European Consumer and Market Law*, *9*, 3–16.
Kerber, W. (2016). Governance of data: Exclusive property vs. access. *International Journal of Intellectual Property and Competition Law*, *47*, 759–762.
Kerber, W. (2022). *Governance of IoT Data: Why the EU Data Act will not fulfill its objectives*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4080436.
Leistner, M. (2017). Big Data and the EU Database Directive 96/9/EC: Current Law and Potential for Reform. In S. Lohsse, R. Schulze, & D. Staudenmayer (Eds.), *Trading data in the digital economy: Legal concepts and tools* (pp. 27–57). Baden-Baden, Germany: Nomos. https://papers.ssrn.com/sol3/papers.cfm? abstract_id=3245937.
Leistner, M. (2021a). The existing European IP rights system and the data economy. In German Federal Ministry of Justice and Consumer Protection and Max Planck Institute for Innovation and Competition (Eds.), *Data access, consumer interests and public welfare* (pp. 209–251). Baden-Baden, Germany: Nomos. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3625712.
Leistner, M. (2021b). Towards an access paradigm in innovation law? *Gewerblicher Rechtsschutz und Urheberrecht Internationaler Teil*, *123*, 925–931.
Leistner, M., & Antoine, L. (2022). *IPR and the use of open data and data sharing initiatives by public and private actors*. Study requested by the European Parliament's Committee on Legal Affairs. https://ssrn.com/abstract=4125503.
Leistner, M., Antoine, L., & Sagstetter, T. (2021). *Big data*. Tübingen, Germany: Mohr Siebeck.
Metzger, A. (2021). Access to and porting of data under contract law: Consumer protection rules and market-based principles. In German Federal Ministry of Justice and Consumer Protection and Max Planck Institute for Innovation and Competition (Eds.), *Data access, consumer interests and public welfare* (pp. 287–317). Baden-Baden, Germany: Nomos.
OECD. (2019). *Enhancing access to and sharing of data: Reconciling risks and benefits for data re-use across societies*. Paris, France: OECD Publishing. doi: 10.1787/276aaca8-en.
Radauer, A., Bader, M., Aplin, T., Konopka U., Searle N., Altenburger R., & Bachner C. (2022). *Study on the legal protection of trade secrets in the context of the data economy: Final report*. European Commission. https://data.europa.eu/doi/10.2826/021443.
Schweitzer, H., Metzger, A., Blind, K., Richter H., Niebel C., & Gutmann F. (2022). *Data access and sharing in Germany and in the EU: Towards a Coherent legal framework for the emerging data economy*. https://ssrn.com/abstract=4270272.
Schweitzer, H., & Welker, R. (2021). A legal framework for access to data – A competition policy perspective. In German Federal Ministry of Justice and Consumer Protection and Max Planck Institute for Innovation and Competition (Eds.), *Data access, consumer interests and public welfare* (pp. 103–153). Baden-Baden, Germany: Nomos.