

IPR and the use of open data and data sharing initiatives by public and private actors ¹

ABSTRACT

This study analyses recent developments in data related practice, law and policy as well as the current legal framework for data access, sharing, and use in the European Union. The study identifies particular issues of concern and highlights respective need for action. On this basis, the study evaluates the Commission's proposal for a Data Act.

The study is commissioned by the European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs at the request of the Committee on Legal Affairs.

Current developments, legal framework and need for action

In the first three parts of this study, we have comprehensively analysed recent developments in data related practice, law and policy as well as the **current legal framework** for use of data and for data sharing initiatives in the European Union. On this basis, we have identified and systematised certain issues of concern and highlighted the **respective need for action**.

With regard to the **Database Directive**, we have therefore **proposed**

- to **specify the conditions** of protection for machine-generated data;
- to **reform the exceptions and limitations**;
- to substantially **shorten the term of protection**;
- to introduce a **pre-emption clause** in particular with regard to national unfair competition law;
- to introduce a **compulsory licence regime**;
- to develop (non-mandatory) **model contract terms** for the allocation of sui generis rights in the context of data related bilateral and/or network contracts.

With regard to **trade secrets protection**, we have **proposed**

¹ Full study in English: [https://www.europarl.europa.eu/RegData/etudes/STUD/2022/732266/IPOL_STU\(2022\)732266_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2022/732266/IPOL_STU(2022)732266_EN.pdf)



- in the context of new access, sharing, and use rights to distinguish between (more sensitive) business information pertaining to specific market information or information about the very parameters of competition as such on the one hand and general technical or creative know-how on the other hand in order to strike a **more precise balance** between access and use interests on the demand side and the interest of protection on the rightholders' side taking into account the public interest in free and undistorted competition;
- to develop **(non-mandatory) model contract terms** for the licensing of trade secrets and for allocating the 'ownership' in cooperative data sharing networks.

The Commission's proposal for a Data Act

In the fourth part of this study, we have evaluated the Commission's proposal for a 'Regulation on harmonised rules on fair access to and use of data (Data Act)' based on the need for action which we have identified in the first three parts of the study.

Introduction and general remarks

The Data Act constitutes an ambitious project and a courageous policy decision with the objectives to open certain markets related to the IoT and cloud sector, to define explicit provisions for data sharing on contractual basis as well as to reduce technical barriers and allow B2G data access in exceptional situations. In order to establish 'harmonised rules on fair access to and use of data' it is a remarkable achievement that the Data Act proposes **institutional, decentral structures (which from our viewpoint are typical for private law claims and should also be enforced accordingly)** for data access, sharing, portability, and use, thereby going way beyond the current legal framework focused primarily on (more centralised) data and services governance.

The Data Act introduces five new instruments: first, the **user's right** – applying in B2C and B2B relations – to **access** and **use data** generated by IoT products and to **share** such data with third parties; second, an **unfairness test for B2B contract clauses** on data sharing which have been imposed on SMEs; third, a framework for **B2G data sharing** based on exceptional need; fourth, provisions on **switching between cloud service providers**, and, fifth, safeguards against **unlawful access to non-personal data held in the Union in international contexts**.

Some of these proposed instruments (data sharing, mandatory unfairness control of B2B contracts, cloud and edge service provider switching), in particular because of their **sweeping scope** (B2C as well as B2B), their **mandatory character**, and the **central role of the user** concerning the access and sharing rights, require fundamental scrutiny in light of the involved **impact on the principle of contractual freedom** as well as with regard to their impact on **free competition** and their **prospective efficiency**. Also, certain 'fine-tuning' is necessary with particular regard to the objective to **reduce market entry barriers for newcomers** (or at least not to erect new or heighten existing barriers to market entry), in the markets for IoT products and cloud services.

Overlaps, balances and consolidation

As a general remark on legislative technique, concerning the entirety of the currently planned instruments of the '**data package**', the relation between the different existing and in particular the newly proposed instruments, their purposes and their content **needs to be** further clarified and **consolidated**. If the involved intricate **overlap, consolidation** and **balancing** issues remain unsolved or unclear, they will be a major factor causing legal uncertainty (chilling effects) as well as possibilities for opportunistic behaviour in the upcoming years.

In our study we have made several proposals concerning such overlap, consolidation and balancing issues which we have addressed mainly by proposing certain changes to the substantive provisions of the Data Act and by proposing certain avenues for adequate contextual delineation. Also, we have made proposals in regard to necessary institutional consolidation in the area of public enforcement and its relation to **necessary private**

rights and enforcement mechanisms, as otherwise there will be a manifest danger of overlapping and contradicting enforcement decisions of different competent authorities in different sectors, concerning both the level of the Member States and the level of the Union.

Relation to the GDPR

In particular, concerning the **processing of personal data**, the Data Act takes into account the entire 'toolbox' of the GDPR by referring to any legal basis foreseen in Article 6 GDPR (or Article 9 GDPR) instead of relying solely on the data subject's consent. Requiring consent in the sense of Article 6 (1) (a) GDPR – or under the even stricter standards of Article 9 (2) (a) GDPR – in each case would indeed considerably reduce the practical efficiency of the new data access and sharing rights due to the high standards, legal uncertainty and practical difficulties with the GDPR's concept of consent, in particular in regard to dynamically involving use scenarios as well as for uses based on relevant sensitive data. However, Article 6 (1) (f) GDPR as the obvious main alternative route to legal processing of IoT data in private settings, poses equally problematic issues concerning the **lacking legal certainty** with regard to the balancing of interests. In this overall context it should always be borne in mind that the GDPR expressly pursues two – equally important – objectives consisting in the protection of natural persons with regard to the processing of personal data *and* the free movement of personal data.

In the context of the proposed Data Act, the broad definition of personal data in Article 4 (1) GDPR – which at the same time entails a *negative* definition of *non-personal* data – could be put under scrutiny. Large parts of the data processed in the data-driven economy relate (at some point) to an identifiable natural person or at least cannot always be clearly distinguished from non-personal data when larger or combined datasets are concerned. The same applies for data generated by IoT products: Location data (e.g. connected cars), use data (e.g. smart home devices) or search queries 'asked' to a virtual assistant can qualify in many cases as personal data in the sense of the GDPR. It might be necessary to **fundamentally specify the scope and impact of the GDPR in the sector**, i.e. to at least consider **amendments to the definition of personal data** in such scenarios in a way which is in line with the objective to improve the **free flow of sufficiently anonymised or manifestly publicly available data**, as well as to specify and clarify the specific possibilities to **balance** the legitimate objectives behind the Data Act with the fundamental right to protection of personal data by interpreting the respective heads for lawfulness of processing in Article 6 GDPR in accordance with the legal duties set out in the Data Act.

In this regard, our study, first, proposes certain ways to achieve the necessary and proportional balance, while preserving effective protection of personal data, and which can be implemented by **certain clarifications in the Data Act proposal** and without changing the text of the GDPR. Second, apart from these detailed proposals, one more fundamental aspect will be central to genuinely improve the conditions for businesses in the internal market in that regard in the future. As the Data Act aims at reducing the practical and technical barriers for data sharing by introducing standards for interoperability and other relevant technical features, in the context of the GDPR this could also be an occasion to further implement legally reliable **technical and organisational standards for the sufficient anonymisation of data**.

Relation to intellectual property rights and trade secrets protection

As regards the necessary balance with IP protection and trade secrets, the proposed provisions of the Data Act consequently and rightly focus primarily on potential overlaps with trade secret protection (particularly Chapter II, III) and with the sui generis right of database makers.

In principle, from the viewpoint of legal technique, the **relation to trade secrets** is satisfyingly addressed in Article 4 (3) and Article 5 (8). We have made further proposals to distinguish between (more sensitive) trade secrets relating to the very parameters of the competition process itself and (less sensitive) trade secrets in regard to technical know-how and other secret information not directly related to the very parameters of the competition process. From our viewpoint – for the sake of legal certainty – it should also be **clarified that the**

FRAND ‘licences’ (as they are foreseen in Article 8) will also have to define and cover necessary and justified use acts in regard to trade secrets. This would be of mainly clarifying character as the necessary justification already follows from Article 4 (3) and Article 5 (8). However, it would also allow to take the character of certain data as trade secrets into account when further specifying the terms and range of FRAND compensation.

Database sui generis right (Article 35)

The difficult role of the database sui generis right in the context of data access, use and sharing has been comprehensively outlined in the third part of our study. We have demonstrated that the database sui generis right has the potential to intensify de facto control over data, to aggravate existing access problems and to lead to hold-up issues in certain situations.

These issues are addressed (in a rather limited, cautiously delineated sector specific way) by Article 35. Pursuant to Article 35, the sui generis right ‘does not apply to databases containing data obtained from or generated by the use of a product or a related service’.

While the explicit clarification that machine-generated databases do not fulfil the conditions of the sui generis right seems acceptable as a bright line rule to reduce the significant legal uncertainty concerning the conditions for protection in the sector, the wording and legal technique of Article 35 should be refined: Apart from certain necessary technical clarifications of the provision’s wording it is recommended that it should be clarified (in the sense of a **Union law pre-emption doctrine**) that within the scope of the Database Directive, if a given database does not fulfil the conditions for protection, Member States shall be precluded to protect such a database on different grounds (such as *parasitisme* or unfair competition protection against misappropriation, unless additional factors, such as consumer confusion, warrant such additional unfair competition law based protection).

In fact, the restatement that machine-generated databases do not qualify for protection under the sui generis right solves some of the mentioned problems in regard to the conditions of protection by providing for a bright line non-conflict rule for certain cases. However, many of the problems we have identified in the first parts of this study and in earlier publications are not addressed by this very targeted provision. In this regard there is **still need for action**.

The role of private law enforcement

In general, the Data Act is characterised by broadly formulated standards (‘general clauses’) and many new legal concepts and terms. These provisions, terms and concepts will have to be further clarified and specified in the upcoming years. Since the Data Act – in particular in its central part on the introduction of new data access and sharing rights for users of IoT devices – assigns an important role to private agents’ requests and bilateral or tri-lateral (contractual) agreements as a private law institution, the task to specify the proposed provisions should centrally lie with **private law courts**, thus should be addressed within **private law enforcement** and by private law courts instead of by a system of different intersecting public authorities. Therefore, in the interest of effective and proportionate enforcement it is **recommended to lay down express rules on private rights and litigation** and, more generally, on the substantive and procedural relationship between the public enforcement mechanisms, foreseen in Articles 31 et seq., and private litigation as the main pillar of putting this new regulatory framework into practice.

The proposed rules on B2C and B2B data access and sharing

From our viewpoint, the new system of proposed B2C and B2B data access, sharing and use in Chapter II and III is the central element of the Data Act. Besides the already mentioned necessity of **instruments for private enforcement**, our main concerns relate, first, to the **horizontal scope** and **generalising mandatory law character** of the proposed data access and sharing system, secondly to certain **inherent limitations** of that system, and thirdly to the **central role assigned to the users** in that new proposed system.

Scope and objective

The provisions proposed in Chapter II and III granting access and use rights for users and the right to share data with third parties in regard to data 'generated' by IoT products and related services are designed to constitute generally applicable, basic rules for all sectors in this field. Due to this **horizontal character covering the entire 'sector' of IoT products**, the proposed provisions, on the one hand, have a very broad scope of application – from industry to private use of connected products (**B2C and B2B alike**). On the other hand, in regard to the relevant data, the scope of the Data Act is limited to 'data generated by the use of products or related services' and thus does not substantially cover any **inferred or derived data**. Furthermore, the access to, use and sharing of these data is limited to uses **which do not compete** with the IoT product from which the data originate.

Consequently, these provisions can neither be consistently construed as addressing specific situations of abuse of dominant market positions (or other situations of specific market failure) nor as addressing specific situations of information asymmetry, imbalances in negotiation power (or other situations of specific contract failure). This is because under the perspective of situation-specific market failure or situation-specific contract failure, the scope and structure of these mandatory provisions would be at the same time both, too broad as well as too narrow. The scope of **mandatory law regulation is too broad** as these provisions obviously also apply in situations where no information or market power asymmetry can be identified at all. This is because, in particular **in B2B settings**, the user of the IoT product might as well be better informed and more experienced than the IoT product provider and data holder, and might also have a relatively stronger market position resulting in a relatively stronger negotiation position. In such a setting, broadly applicable, **sector-wide mandatory** provisions on data access and sharing cannot be justified as a corrective for a specific situation of market or contract failure. On the contrary, in some of these situations they might outright interfere with efficient, contract-based allocation of data, as because of their mandatory character, they prevent any reservation of data-related aftermarkets based on factual data control or contracts, even in situations, where this would be the efficient solution (e.g. a small newcomer (not a dominant undertaking) in the IoT producers' market could otherwise not enter the market at all) and would therefore benefit both parties to a respective contract. At the same time, the **scope is too narrow**, as we have identified situations of potential market failure in regard to the access to aggregated data, and, namely structured data, i.e. **contextualised, standardised data**, as the genuine main bottleneck for the development of many data oriented services at the moment. However, for such situations, the new provisions do not really provide a comprehensive remedy, because their **field of application is limited to volunteered and observed data** and their fundamental structure is oriented towards the access to and sharing of individual-level data (which at best indirectly and inefficiently helps to remedy situations where access to aggregate, contextualised datasets would be necessary and justified).

Instead of remedying specific situations of market or contract failure, the newly proposed provisions on data access, use and sharing in the Data Act are based on the general assumption that access to and use of IoT data in order to provide new products or services (in particular, but not only, maintenance, repair and other aftermarket services or products) will liberate aftermarkets and other new markets through the provision *and* commodification of data access rights, and will thus, in their total effect, create more benefits through enhanced dynamic efficiency than costs (through the undoubted interference with static and dynamic efficiency in certain situations, in particular B2B situations). The objective is thus to provide an **institutional framework for the development of certain new markets**, in particular in regard to new products or services in markets related to the distribution of **IoT products** (such as repair, maintenance and other related markets), through generally opening and institutionally structuring hypothetical or actual upstream markets for the access to the necessary data generated by such products. This new regulatory approach, which goes way beyond the existing, comparably problem-specific approaches in competition law, consumer protection law and sector-specific regulation is at the same time limited in scope to IoT products and related (after)markets as well as in regard to upstream markets for volunteered or observed) data generated by the use of such products.

Thus, while the regulated sector (use of any IoT product, B2C and B2B) is very broad and unspecific (**broad horizontal field of mandatory regulation**), the affected data categories (only volunteered and observed data, i.e. no inferred data) as well as the statutorily enabled uses (use for developing competing products is expressly excluded) are remarkably limited (**limited vertical depth of regulation**).

However, even in light of these crucial limitations, it has to be borne in mind that the sectors in which data-collecting IoT products are used, **vary widely**, and thus, the conditions on the relevant markets, the relationship between the actors and the amount and categories of the co-generated data differ significantly. Also, the aspect of possible new **barriers to market entry** (or at least chilling effects) for original producers which have not yet implemented IoT components in their products at all (and the general aspect of not chilling potential competition), should not be lost out of sight. General competition law by and large only sanctions market dominant firms for exclusionary conduct by leveraging their dominance on a primary market to a secondary market (although of course recent reforms, such as the most recent reform of the German Competition Act, have already cautiously departed from this approach inter alia in the context of the data economy). By contrast, the Data Act might be interpreted as a decision for generally opening (hypothetical) markets in the IoT sector through a **general ex-ante (market design) approach**, since from the viewpoint of the Commission the existing, competition law-based case-by-case analysis has turned out not to be effective enough to generally foster the development of certain data-driven markets. Even following this assumption, it would however also have to be shown, whether a generalised **mandatory law** framework (extending to all B2B-situations) is indeed required to reach this objective throughout the entire sector, whether solely opening secondary markets (by excluding data access, use or sharing in order **to compete** with the data holder) is sufficient and in particular, how such secondary markets shall be defined and delineated from situations of (direct) competition with the data holder in borderline cases. In that latter regard, the Data Act remains rather cautious, thus at the same time significantly limiting the impact of this new regulatory instrument for crucial case groups.

From our viewpoint, all this has three main general consequences resulting in two main policy recommendations. First, given the diversity of their field of application, the new provisions have to be re-evaluated with particular attention to their **scope** and necessary **flexibility** in particular through the use of flexible open-ended standards in the legislative text. Related to this on an instrumental level is the important question which institutional players shall specify these standards in the future as this will be crucial for the necessary balance between flexibility through the use of open-ended standards and fostering sufficient legal certainty through the specification of these standards in case law (this particularly also concerns the question of **private** and/or public **enforcement** and their relationship to each other).

Secondly, it has to be kept in mind that none of these new provisions should be designed, construed or applied in a way which puts disproportional **new cost burdens on newcomers** in the very markets the Data Act intends to open and incentivise (this particularly at least concerns necessary lenience in regard to SMEs as well as – again – the issues of the necessity of mandatory law, efficient enforcement and necessary legal certainty which might be endangered if overlapping, multi-institutional public law enforcement causes significant additional administrative and information costs, e.g. because of resulting legal uncertainty and additional bureaucracy). As a **policy recommendation**, these two aspects lead to a need to **reconsider the broad scope** of the proposed mandatory framework (possibly in favour of a more sector-specific approach) and/or to re-evaluate whether **mandatory rules** are indeed needed in those B2B-constellations, where no manifest imbalance exists between the parties to the contract

Thirdly, one has to remain aware that **potential additional access problems**, which have been identified in the first part of this study, go way beyond the specific field of certain data co-generated by IoT products and the opening of related aftermarkets for products or services which are not in direct competition with the data generating IoT product itself. This is especially true for access needs of competitors to complete datasets for competing in secondary markets (which might include inferred data), and access to large aggregated datasets (e.g., training data and other **inferred data**) of big data conglomerates for innovation purposes (second and third case group) which might even lead to products or services which are in direct competition with the data

generating product or service. Due to the strict **exclusion of services**, data generated by the use of (online) services or platforms are not covered by the proposed Data Act. This sector is therefore hitherto only covered in the 'data package' by the proposed Digital Markets Act, albeit limited to data held by gatekeepers (i.e. the GAFAM companies plus presumably less than a handful of other gatekeeper platforms) and to specific market situations. Therefore, it will be necessary to design and construe the new provisions in the Data Act in a way which allows the Act to at least indirectly contribute to the solution of some of these (partly related) data access problems. Also, it has to be kept in mind that the mentioned **access problems**, in particular in regard to aggregated, contextualised or standardised data and **in regard to certain larger (not purely data-processing, but data-driven) services**, might need to be addressed, going beyond the limited data related rights vis-à-vis Big Tech companies in the proposed Digital Markets Act. By contrast, the Data Act proposal is primarily designed to enable data access and use by third parties in a particular sector and in regard to but one central use scenario (aftermarket services for IoT devices). This leads to the **policy recommendation** to reconsider the **limitation of the scope** of the Data Act's proposed access and sharing regulation to IoT-products and related services, to re-evaluate the exact extent of the principled **exclusion of inferred data** as well as to reconsider the principled requirement of **non-competing use**.

The proposed central role of the user

Generally, and in particular for B2B constellations, it also needs to be justified why the **user** should be in a **central role**. Whereas protecting **personal data** by means of strong subjective rights (as provided by the GDPR) is mandated by the fundamental right to protection of personal data, the need for allocating mandatory access, use and sharing rights in regard to non-personal data to the users as suggested by the Data Act, is less self-evident. Allowing access to and use of data generated by IoT products and related services for **B2C relations** can also be seen as an expression of guaranteeing data sovereignty and 'empowering' of private consumers in regard to perceived information asymmetries or other reasons for an assumed weaker bargaining position of private consumers.

However, **in B2B constellations**, such allocation of non-personal data to the customers/users of IoT devices needs genuine justification. As we have explained, in B2B constellations, where the customer/user is not a consumer, such mandatory allocation of data access, use and sharing rights, cannot across the board be justified by the identification of specific situations of market or contract failure – this would at best be possible for SME users vis-à-vis large IoT companies or for certain very specific sectors where empirical data clearly suggest the general actual or potential existence of such imbalanced situations. The Data Act goes beyond this, covering all B2B relations, where IoT products are used by businesses on the basis of sales, rental or lease contracts, alike. Thus, it seems that the mandatory allocation of data access, use and sharing rights to business users of IoT products is based on the perceived co-initiative and co-investment of such business users in the generation of the resulting use generated data through their actual use. As for the allocation of exclusive rights in such data, it has been decided by the CJEU in the context of the database *sui generis* right, that the mere generation of data in the course of another main business activity (i.e. as a spin-off of such a main business activity), shall not give rise to exclusive rights based on such more or less incidental generation of data. As for B2B situations under the Data Act proposal, the crucial (and somewhat different) question is whether the contribution to the generation of data through use of IoT products in the context of another main business activity, should give rise to certain limited and non-exclusive access, use and sharing rights for the user.

Whereas certain contextual elements in the *acquis communautaire* (in particular the conception of minimum use rights of the lawful user in the Computer Programs and the Database Directive) can serve as a tentative model for the access, use and sharing rights for business users in the Data Act, the crucial question remains whether the **initial allocation of such rights to the users** of the devices is efficient, when assessed in light of one of the main objectives of the Data Act, i.e. to create new markets for such data as a necessary precondition for the offer of new products and services in aftermarkets related to the originally distributed IoT product or its use. To answer this question, it will have to be considered, whether the users of such devices are sufficiently

informed and incentivised to actually make use of their new rights, in particular also to share (and effectively market) them. In a rather limited field, i.e. the provision of specific new or at least cheaper or better services in aftermarkets, one might assume that the users as prospective customers of such services, might indeed be the best informed agents and might have sufficient incentives in order to initiate the necessary sharing of data by the data holder. At the same time effects, such as switching costs and inertia bias as well as the associated transaction costs, might well reduce the incentives of the users to effectively initiate data sharing. To make this envisaged regulatory system work, first, the relevant provisions of the Data Act must allow for **broad, non-static and transferrable as well as monetisable sharing claims** at least where trade secrets are not affected. Secondly – and more importantly – it will have to be considered whether the central (and to a certain extent ‘proto-exclusive’) role of the users in regard to initiating and authorising upstream data sharing is indeed as such justifiable and sufficient to effectively foster the emergence of dynamic and diverse new data markets as a precondition of new data related products or services.

In this context, it should also be kept in mind that the very generating, obtaining and observing of data generated by the use of a product or related service at the same time requires substantial ex-ante and continuous organisational, technical and financial efforts by the **data holders**. Also, in many situations, the data holders might be in a better situation to assess, negotiate and implement efficient data contracts, whereas the users’ respective initiative and role seem less central and functional in that regard. In order to effectively incentivise data sharing, the role and legal as well as practical position of the **data holders (IoT producers and related companies)** should therefore be equally taken into consideration, when regulating the sharing of such data on a non-exclusive basis with third parties. In accordance with our analysis, we have made several proposals to achieve this goal in our study some of which we also list in our following main policy recommendations.

Ex-post evaluation plan

We have been asked to also point at solutions, e.g. a data collection plan, which would allow for an ongoing evaluation of how legal solutions recommended in the study are implemented and if they are efficient and effective. In that regard **Article 41 foresees an ex-post evaluation of the Data Act** by the Commission *two years* after the date of its application with a particular view to certain adaptations of the central instruments of the Data Act. Indeed, such clause as well as any other provision injecting necessary flexibility and adaptability into the legal instrument seem highly recommendable in light of the very dynamic development of the regulated market sector. Art. 41 in principle provides a coherent basis for the evaluation of the Data Act and possible future adaptation although one might consider, in the interest of increased flexibility, whether in addition the Commission should also be empowered to make certain necessary mere specifications of open standards in the Data Act by way of delegated acts. As for possible ex-post evaluation and data collection, we have noted certain essential aspects in our study which we have summarised at the end of our following list of main policy recommendations.

In sum, we propose with regard to the **Data Act in general**,

- to **clarify and strengthen the role of private law enforcement**;
- to make the proposed public enforcement structures **optional** to the Member States and to streamline them, at best by a **one-stop shop** approach including a European ‘meta-authority’ for data related topics;
- to thoroughly assess the **coherence of the Data Act with the entire ‘data package’** and the existing legal framework;
- to include provisions on the applicability of the Data Act in **multipolar settings** (e.g. data sharing networks) and to re-evaluate whether the current regulatory approach is well equipped to cover such situations;

- to **develop accompanying non-mandatory model contract terms**.

With regard to the proposed rules on **B2C and B2B data access, sharing, and use** we propose

- to **reconsider their broad scope of application and/or to critically evaluate the necessity of the mandatory character of the proposed system in B2B constellations** where no imbalance of the parties is present;
- complement the central role of the user with a **regulation of the position of the data holders**;
- to assess whether access to data generated by the use of **services** is already comprehensively covered by the proposed Digital Markets Act and to consider the **extension of the scope of the new data access, sharing and use rights to certain larger (not purely data-processing, but data-driven) services** which are not gatekeepers under the comparatively strict thresholds of the proposed Digital Markets Act;
- to re-evaluate the exact extent of the principled **exclusion of inferred data**;
- to reconsider or at least to specify the conditions of the prohibition to use the respective data for developing a **competing product**;
- to consider whether the obligations to make data available set forth in the Data Act **could qualify as 'legal obligation' in the sense of Article 6 (1) (c) GDPR**, and, in the future, to consider further delineating the notion of 'personal data', at best by developing **technical and organisational standards for anonymisation** and by introducing a **rebuttable presumption** of anonymisation when the respective standards are met;
- to clarify that **FRAND 'licences' will cover necessary and justified use acts in regard to trade secrets**.

With regard to the **unfairness test for B2B contract terms** on data sharing we propose

- to specify that the fairness test does not apply to constellations in which a **micro or small business** is the imposer of a contract clause;
- to add the condition that a **gross imbalance** in the parties' rights and obligations arising under the contract must be the result of the unfair term.

With regard to **B2G data sharing** based on exceptional need we propose

- to reconsider whether the provisions should be **extended to small and micro-sized enterprises**.

With regard to the provisions on **switching between cloud and edge services** we propose

- to foresee an **exception for SMEs as providers**, at least for B2B relations;
- to revise the **relation to the proposed Digital Markets Act**;
- to **clarify the concept of 'functional equivalence'**.

With regard to the provisions on **interoperability** we propose

- to **extend the scope of the general principles** applicable to the operators of European data spaces to also guide future general standardisation processes in regard to cloud portability, data access and data sharing.

With regard to **Art. 35 on the database sui generis right** we propose

- to primarily 'refine' the wording of the provision in order to clarify that databases which fall into the scope of the Database Directive but which do not fulfil the substantive conditions of protection shall

generally not be protected by other instruments of Member States' national law either, absent any additional objectives entirely unrelated to the investment protection objective of the Database Directive (**Union law pre-emption doctrine**).

With regard to an **ongoing and ex-post evaluation** of how legal instruments proposed in the Data Act are implemented and if they are efficient and effective, we propose

- to carefully **choose certain very specific, carefully limited and representative industry sectors** for possible evaluation of central instruments of the Data Act and possibly associated data collection as otherwise the very broad scope and generalising character of the Data Act will prevent the emergence of conclusive results.

Disclaimer and copyright. The opinions expressed in this document are the sole responsibility of the authors and do not necessarily represent the official position of the European Parliament. Reproduction and translation for non-commercial purposes are authorised, provided the source is acknowledged and the European Parliament is given prior notice and sent a copy. © European Union, 2022.

External Authors: (Prof. Dr. Matthias LEISTNER, LL.M. (Cambridge), Ludwig Maximilian University Munich

Ref. iur. Lucie ANTOINE, Ludwig Maximilian University Munich

Research Administrator responsible: Mariusz MACIEJEWSKI

Editorial assistant: Ivona KLECAN

Contact: poldep-citizens@europarl.europa.eu

This document is available on the internet at: www.europarl.europa.eu/supporting-analyses

PE 732.266

IP/C/JURI/2021-80

Print ISBN 978-92-846-9903-2 | doi:10.2861/854176 | QA-04-22-174-EN-C

PDF ISBN 978-92-846-9904-9 | doi:10.2861/033684 | QA-04-22-174-EN-N