Attention, here comes the EU Data Act!

A critical in-depth analysis of the Commission's 2022 Proposal

by **Matthias Leistner and Lucie Antoine***

Abstract: The paper outlines the main elements of the 2022 EU Commission's Data Act Proposal. The proposal is the apex of the Commission's recent regulatory initiatives in the field of platforms and the data economy. The paper provides for a critical in-depth analysis of the proposal that forms the basis for concrete recommendations to improve the current text, all guided by the aim to help this legislative initiative to reach its objectives by curbing it, where necessary, and at the same time making it more focused and efficient.

Recommended citation: Matthias Leistner and Lucie Antoine, Attention, here comes the EU Data Act! A critical in-depth analysis of the Commission's 2022 Proposal 13 (2022) JIPITEC 339 para 1

A. Introduction and general remarks

1 On 23 February 2022 the Commission has published its proposal for a "Regulation on harmonised rules on fair access to and use of data (Data Act)" [1]. The proposal is the apex of the Commission's regulatory initiatives for the data economy, with the Digital Markets Act, the Data Governance Act, the Digital Services Act and the AI Act already being adopted or close to actual final adoption.[2]

2 Although this most recent proposal of the current Commission has its main focus (and certainly the largest degree of intended regulatory impact) on the IoT sector, certain elements of this ambitious legislative project also go beyond the IoT sector specifically. The Data Act follows the objectives to

* Prof. Dr. Matthias Leistner, LL.M. (Cambridge), Professor and Chairholder for Civil Law and Intellectual Property Law with Information Law and IT-Law, Ludwig Maximilian University Munich; Lucie Antoine, Research Assistant and PhD Candidate, Ludwig Maximilian University Munich. This paper goes back to the authors' study 'IPR and the use of open data and data sharing initiatives by public and private actors' (2022) requested by the European Parliament's Committee on Legal Affairs, published on 3 May 2022, available at <https://ssrn.com/abstract=4125503>. The following summary contains but the absolutely inevitable references; comprehensive references can be found in the study.We thank Heike Schweitzer, Josef Drexl, Wolfgang Kerber, Axel Metzger, Ansgar Ohly, Louisa Specht, Gerald Spindler, Tatsuhiro Ueno and Herbert Zech for their consistently helpful comments and valuable ideas in our various discussions of the subject.

1 European Commission, Proposal of 23 February 2022 for a Regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act), COM(2022) 68 final (hereinafter "Data Act").

2 Data Governance Act: promulgated in the Official Journal on 3 June 2022, OJ L152/1; Digital Markets Act and Digital Services Act: adopted by European Parliament on 5 July 2022, Council's final approval for the Digital Markets Act on 18 July 2022; AI Act: ongoing proceedings in European Parliament and Council.

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 (such as the recent pandemic). 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.

3 The Data Act shall introduce 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[3]; second, an *unfairness test for B2B contract clauses* on data sharing which have been imposed on SMEs[4]; third, a framework for *B2G data sharing* based on exceptional need[5]; fourth, provisions on *switching between cloud service providers,*[6] and, fifth, safeguards against *unlawful access to non-personal data held in the Union in international contexts*[7].

4 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.

5 In the following, we summarise some analytic and critical remarks on the proposal which to us seem to be most imminent for the further legislative discussion that is meanwhile well underway. On that basis, we provide for a list of recommendations to improve the current text of the proposal.

3 Articles 3–12.

4 Article 13.

5 Articles 14–22.

6 Articles 23–26.

7 Article 27.

B. Overlaps, balances and consolidation

6 As a general remark on legislative technique, concerning the entirety of the currently planned instruments of the "*data package*"[8], 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.

7 Elsewhere 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.[9] 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.

I. Relation to the GDPR

8 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[10], in particular

8 In particular the Data Governance Act, the Digital Markets Act and the Digital Services Act.

9 Matthias Leistner and Lucie Antoine, 'IPR and the use of open data and data sharing initiatives by public and private actors' (2022), 73 et seq.

10 See for instance Andreas Sattler, 'Autonomy or Heteronomy – Proposal for a two-tier interpretation of Art. 6 GDPR' in Sebastian Lohsse, Reiner Schulze and Dirk Staudenmayer (eds), *Data as Counter-Performance – Contract Law 2.0?*

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.[11] 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.[12]

9 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 – should be put under scrutiny.[13] 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.[14] 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.[15] It seems necessary to *fundamentally specify the scope and impact of the GDPR in the sector*,[16] 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.

10 In this regard, first, we propose 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, e.g. by recognising Article 4 (1) and Article 5 (1) of the Data Act as "legal obligation" in the sense of Article 6 (1) (c) 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* – ideally by complementing this with at least a rebuttable presumption of sufficient anonymisation when businesses comply with such established anonymisation standards.[17]

II. Relation to intellectual property rights and trade secrets protection

11 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.[18]

(Nomos/Hart 2020) <https://www.jura.uni-muenchen.de/personen/s/sattler_andreas/veroeffentlichungen/autonomy-or-heteronomy.pdf>.

11 Andreas Sattler, 'Autonomy or Heteronomy – Proposal for a two-tier interpretation of Art. 6 GDPR' in Sebastian Lohsse, Reiner Schulze and Dirk Staudenmayer (eds), *Data as Counter-Performance – Contract Law 2.0?* (Nomos/Hart 2020), 16; see further Matthias Leistner, Lucie Antoine and Thomas Sagstetter, *Big Data* (Mohr Siebeck 2021), 275 et seq.

12 See title of the GDPR; Article 1 GDPR and Recital 13 GDPR.

13 Already Nadezhda Purtova, 'The law of everything. Broad concept of personal data and future of EU data protection law' (2018) 10 Law, Innovation and Technology 40.

14 See e.g. European Commission, Guidance on the Regulation on a framework for the free flow of non-personal data in the European Union, COM(2019) 250 final, 4 et seq.

15 Acc. to Article 4 (1) GDPR "personal data" refers to any information relating to an identified or identifiable natural person.

16 See also Inge Graef, Martin Husovec and Jasper van den Boom, 'Spill-Overs in Data Governance: Uncovering the Uneasy Relationship Between the GDPR's Right to Data Portability and EU Sector-Specific Data Access Regimes' [2020] Journal of European Consumer and Market Law 14 et seq.; Inge Graef, Raphael Gellert and Martin Husovec, 'Towards a Holistic Regulatory Approach for the European Data Economy: Why the Illusive Notion of Non-Personal Data is Counterproductive to Data Innovation' [2019] European Law Review 605 et seq.

17 See further Matthias Leistner and Lucie Antoine, 'IPR and the use of open data and data sharing initiatives by public and private actors' (2022), 65. The German Data Ethics Commission has proposed to introduce a respective system, see its 'Opinion' (2019), 131 <https://www.bmi.bund.de/EN/topics/it- internet-policy/data-ethics-commission/data-ethics-commission-node.html>.

18 See already Matthias Leistner, 'The existing European IP

12 In principle, from the viewpoint of legal technique, the *relation to trade secrets* is satisfyingly addressed in Article 4 (3) and Article 5 (8).[19] In the context of new access, sharing, and use rights we propose however 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.[20]

13 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.

14 As a tool for complementing the Data Act, *(non-mandatory) model contract terms* for the licensing of trade secrets and for allocating the "ownership" of trade secrets in cooperative data sharing networks should be developed in order to reduce legal uncertainty.[21]

III. Database sui generis right (Article 35)

15 The database sui generis right has a difficult role in the context of data access, use and sharing as it 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.[22]

16 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".

17 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,[23] the wording and legal technique of Article 35 should be refined: Apart from certain necessary technical clarifications of the provision's wording[24] 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[25] (such as *parasitisme* or unfair competition protection against misappropriation, unless additional factors, such as consumer confusion, warrant such additional unfair competition law based protection).

18 In fact, the restatement that machine-generated databases do not qualify for protection under the sui generis right solves some of the problems in regard to the conditions of protection by providing

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* (Nomos 2021), 209, 222 et seq. <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3625712>.

19 More sceptical Weizenbaum Institute for the Networked Society, 'Position Paper regarding Data Act' (2022), 12 et seq. <https://www.ssoar.info/ssoar/handle/document/79542>.

20 Matthias Leistner and Lucie Antoine, 'IPR and the use of open data and data sharing initiatives by public and private actors' (2022), 64.

21 Matthias Leistner and Lucie Antoine, 'IPR and the use of open data and data sharing initiatives by public and private actors' (2022), 64.

22 Comprehensively, Matthias Leistner and Lucie Antoine, 'IPR and the use of open data and data sharing initiatives by public and private actors' (2022), 59 et seq.

23 With a rather critical view, Estelle Derclaye and Martin Husovec, 'Why the sui generis database clause in the Data Act is counter-productive and how to improve it?' (2022) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4052390>.

24 In detail Matthias Leistner and Lucie Antoine, 'IPR and the use of open data and data sharing initiatives by public and private actors' (2022), 120. See also 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)' (2022), paras. 258 et seq.; European Copyright Society, 'Opinion of the European Copyright Society on selected aspects of the proposed Data Act' (2022), 2 et seq. <https://europeancopyrightsocietydotorg.files.wordpress.com/2022/05/opinion-of-the-ecs-on-selected-aspects-of-the-data-act-1.pdf>.

25 Estelle Derclaye and Martin Husovec, 'Why the sui generis database clause in the Data Act is counter-productive and how to improve it?' (2022), 2 et seq.

for a bright line non-conflict rule for certain cases. However, many of the problems we have identified in our study[26] and in earlier publications[27] are not addressed by this very targeted provision. In this regard there is *still need for action.*[28]

19 With regard to the *Database Directive*, we therefore *propose* (beyond the Proposal for a Data Act)[29]

- to substantially *shorten the term of protection*;
- to *exclude* databases of *public bodies* from sui generis protection;
- to *reform the exceptions and limitations;*
- to introduce a *compulsory licencing 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.

C. The role of private law enforcement

20 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,[30] 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.[31] 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.[32]

D. The proposed rules on B2C and B2B data access and sharing

21 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.

I. Scope and objective

22 The provisions proposed in Chapter II and III granting access and use rights for users and the right to share

26 Matthias Leistner and Lucie Antoine, 'IPR and the use of open data and data sharing initiatives by public and private actors' (2022), 49 et seq.

27 Matthias Leistner, 'Big Data and the EU Database Directive 96/9/EC: Current Law and Potential for Reform' in Sebastian Lohsse, Reiner Schulze and Dirk Staudenmayer (eds), Trading Data in the Digital Economy: Legal Concepts and Tools (Nomos 2017), 27 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3245937>; Matthias Leistner, '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* (Nomos 2021), 209; Matthias Leistner, Lucie Antoine and Thomas Sagstetter, *Big Data* (Mohr Siebeck 2021), 410 et seq.

28 See also 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)' (2022), para. 265.

29 Comprehensively Matthias Leistner and Lucie Antoine, 'IPR and the use of open data and data sharing initiatives by public and private actors' (2022), 59 et seq.

30 Also highlighting the private law character, Dirk Staudenmayer, 'Der Verordnungsvorschlag der Europäischen Kommission zum Datengesetz' [2022] Europäische Zeitschrift für Wirtschaftsrecht 596.

31 Rupprecht Podszun and Clemens Pfeifer, 'Datenzugang nach dem EU Data Act: Der Entwurf der Europäischen Kommission' [2022] Gewerblicher Rechtsschutz und Urheberrecht 953, 960 et seq.

32 Similarly, 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)' (2022), paras. 8, 240 et seq.; Rupprecht Podszun and Clemens Pfeifer, 'Datenzugang nach dem EU Data Act: Der Entwurf der Europäischen Kommission' [2022] Gewerblicher Rechtsschutz und Urheberrecht 953, 960 et seq.

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.[33] 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*.[34] 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.

23 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.[35] 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.[36] 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[37] (which at best indirectly and inefficiently helps to remedy situations where access to aggregate, contextualised datasets would be necessary and justified).[38]

24 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[39] (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*

33 Data Act, Explanatory Memorandum, 5.

34 Recital 14, 17.

35 In B2B relationships, situations in which – due to particular investments etc. – a limitation of the user's access and use rights (by means of an agreement) may seem reasonable to both of the parties are undoubtedly conceivable, see Heike Schweitzer and Martin Peitz, 'Ein neuer europäischer Ordnungsrahmen für Datenmärkte?' (2018) Neue Juristische Wochenschrift 275, 280.

36 Matthias Leistner and Lucie Antoine, 'IPR and the use of open data and data sharing initiatives by public and private actors' (2022), 25; from a competition law perspective Jacques Crémer, Yves-Alexandre de Montjoye and Heike Schweitzer, 'Competition Policy for the digital era' (2019), 75 et seq.

37 First case group as defined by Jacques Crémer, Yves-Alexandre de Montjoye and Heike Schweitzer, 'Competition Policy for the digital era' (2019), 75.

38 See also Wolfgang Kerber, 'Governance of IoT Data: Why the EU Data Act will not fulfill its objectives' (2022), 12 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4080436>.

39 Cf. European Commission, '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)' (2022), Staff Working Document, SWD(2022) 34 final, 43 et seq.; Deloitte and others, 'Study to support an Impact Assessment on enhancing the use of data in Europe' (2022), 270 et seq. <https://digital-strategy.ec.europa.eu/en/library/impact-assessment-report-and-support-studies-accompanying-proposal-data-act>.

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*).

25 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[40]). 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.

26 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).

27 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

28 Thirdly, one has to remain aware that *potential additional access problems* that have been identified and systematised in recent literature, 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

40 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)' (2022), para. 36.

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 which might even lead to products or services which are in direct competition with the data generating product or service.[41] 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*[42] as well as to reconsider the principled requirement of *non-competing use*.[43]

II. The proposed central role of the user

29 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.[44] 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.[45]

30 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[46] – 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.[47] As for the allocation of exclusive rights in such data, it has been

41 Second and third case group as defined by Jacques Crémer, Yves-Alexandre de Montjoye and Heike Schweitzer, 'Competition Policy for the digital era' (2019), 75 et seq.

42 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)' (2022), paras. 24 et seq.; Rupprecht Podszun and Clemens Pfeifer, 'Datenzugang nach dem EU Data Act: Der Entwurf der Europäischen Kommission' [2022] Gewerblicher Rechtsschutz und Urheberrecht 953, 961.

43 Wolfgang Kerber, 'Governance of IoT Data: Why the EU Data Act will not fulfill its objectives' (2022), 12; cf. Inge Graef and Martin Husovec, 'Seven Things to Improve in the Data Act' (2022), 2 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4051793>.

44 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)' (2022), para. 49.

45 Data Act, Explanatory Memorandum, 13.

46 Similarly, Wolfgang Kerber, 'Governance of IoT Data: Why the EU Data Act will not fulfill its objectives' (2022), 25.

47 Cf. Recital 6. The aspect of "co-generation" is also core element of the ALI-ELI Principles for a Data Economy, see particularly Principle 18 and the flexible factors proposed therein (American Law Institute and European Law Institute, 'ALI-ELI Principles for a Data Economy – Data Transactions and Data Rights', ELI Final Council Draft, (2021) <https://www.principlesforadataeconomy.org/fileadmin/user_upload/p_principlesforadataeconomy/Files/Principles_for_a_Data_Economy_ELI_Final_Council_Draft.pdf>).

decided by the ECJ 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.[48] 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.

31 Whereas certain contextual elements in the *acquis communautaire* (in particular the conception of minimum use rights of the lawful user in the Computer Programs[49] and the Database Directive[50]) can serve as a tentative model for the access, use and sharing rights for business users in the Data Act,[51] 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.[52]

32 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.

III. Necessary flexibility

33 *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. Article 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

48 C-203/02 *British Horseracing Board v Hill* [2004], ECLI:EU:C:2004:695, paras. 30 et seq.; C-46/02 *Fixtures Marketing v Oy Veikkaus* [2004], ECLI:EU:C:2004:694; C-338/02 *Fixtures Marketing v Svenska Spel* [2004], ECLI:EU:C:2004:696; C-444/02 *Fixtures Marketing v Organismos prognostikon*, ECLI:EC:C:2004:697.

49 Articles 5 and 6 Computer Programs Directive. Further on this aspect Matthias Leistner and Lucie Antoine, 'IPR and the use of open data and data sharing initiatives by public and private actors' (2022), 60.

50 Article 8 Database Directive.

51 Cf. Matthias Leistner, Lucie Antoine and Thomas Sagstetter, *Big Data* (Mohr Siebeck 2021), 65 et seq., 444 et seq.

52 Cf. Wolfgang Kerber, 'Governance of IoT Data: Why the EU Data Act will not fulfill its objectives' (2022), 2 et seq.; Rupprecht Podszun and Clemens Pfeifer, 'Datenzugang nach dem EU Data Act: Der Entwurf der Europäischen Kommission' [2022 Gewerblicher Rechtsschutz und Urheberrecht 953, 961.

policy recommendations.

E. Recommendations

34 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"[53] 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*.

35 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*.

36 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.

37 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*.

38 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"*.

39 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.

40 With regard to *Article 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

53 Weizenbaum Institute, 'Position Paper concerning Data Act – Inception Impact Assessment' (2021), 12 <https://www.weizenbaum-institut.de/media/News/Statement/Weizenbaum_Institute_Data_Act_IIA_Position_Paper_final.pdf>.

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*).

41 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.