Position Statement
of the Max Planck Institute for Innovation and Competition
of 25 May 2022
on the
Commission's Proposal of 23 February 2022
for a Regulation on harmonised rules on fair access to and use of data (Data Act)

Authors: Josef Drexl,[i] Carolina Banda,[ii] Begoña González Otero,[iii] Jörg Hoffmann,[iv] Daria Kim,[v] Shraddha Kulhari,[vi] Valentina Moscon,[vii] Heiko Richter,[viii] Klaus Wiedemann[ix]

Table of Contents

[i] Professor Dr iur, LLM (UC Berkeley), Director of the Institute, Honorary Professor of the University of Munich.
[ii] LLM in IP & Competition Law (MIPLC), Doctoral Student and Junior Research Fellow of the Institute.
[iii] Dr iur, Senior Research Fellow of the Institute.
[iv] Doctoral Student and Junior Research Fellow of the Institute.
[v] Dr iur, LLM in IP & Competition Law (MIPLC), Senior Research Fellow of the Institute.
[vi] LLM in IP & Competition Law (MIPLC), Doctoral Student and Junior Research Fellow of the Institute.
[vii] Dr iur, Senior Research Fellow of the Institute.
[viii] Dr iur, LLM (Columbia), Senior Research Fellow of the Institute.
[ix] Doctoral Student and Junior Research Fellow of the Institute.

The Max Planck Institute for Innovation and Competition is a research institute within the Max Planck Society for the Advancement of Science. The Max Planck Institute is committed to fundamental legal and economic research on processes of innovation and competition and their regulation. Its research focus is on the incentives, determinants and implications of innovation. The Institute informs and guides legal and economic discourse on an impartial basis. It hereby provides its position on the Commission's Proposal for a Regulation on harmonised rules on fair access to and use of data (Data Act).[1]

I. Introduction

(1) The Max Planck Institute welcomes the Commission's initiative to propose a Data Act (in the following, 'Proposal') with horizontally applicable rules for all sectors of the digital economy.

(2) On its website, the Commission states that the 'Data Act will ensure fairness in the digital environment, stimulate a competitive data market, open opportunities for data-driven innovation and make data available for all.' The Institute is also in support of these objectives. This Position Statement will thus aim to assess whether and to what extent the Proposal can be expected to promote these objectives and how the text could be improved to reach better results. The Institute particularly hopes to provide further insights and guidance to the European legislature for the upcoming legislative process.

(3) The Proposal seeks to enact a set of rules that are applicable without regard to the specificities of individual sectors. The Institute agrees that horizontal rules are needed and that on certain issues it is now time to adopt such rules. However, the Institute would like to call to mind that sector-specific rules can be more targeted and therefore more effective in reaching good results. Hence, the proposed horizontal rules should not be expected to replace sector-specific regulation or necessarily provide a good template for future sectoral rules *per se*. While the Commission argues that in principle future legislation should be aligned with the horizontal rules of the Data Act,[2] the legislature should not blindly pursue such alignment. Especially the IoT data access and use right of Chapter II of the Proposal is most needed to be applied by default in situations where existing, especially sector-specific, data access and use regimes do not apply.

---

1 Proposal of the Commission 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. See also the accompanying Commission Staff Working Document – Impact Assessment Report, SWD(2022) 34 final (in the following 'Impact Assessment Report').

2 Explanatory Memorandum of the Proposal, p 5.

(4) In addition, it should be noted that the rules of the Proposal do not, or not sufficiently, address all the issues of the data economy that deserve to be regulated. An example of this is access to and use of the data for the training of artificial intelligence (AI). The Commission claims that the Proposal 'deals with highly strategic technologies such as cloud computing and artificial intelligence'.[3] Yet the Commission did not engage in a broad and thorough analysis of all the considerations that should be taken account of for regulating data access and use for enhancing the development of AI. Nor will the IoT data access and use right as proposed for Chapter II provide such regime. Apart from concerns that Chapter II may not be the most effective tool, IoT-generated data only constitute one category of data that are used for the training of AI.

(5) Hence, the Data Act will not be the last piece of the puzzle that the EU legislature will add to the legal framework for the digital economy. This is important to note, because the Institute has the impression that the Commission in certain instances seeks to achieve too much with the tools it proposes, while the tools are not really fit for purpose. Therefore, the European legislature should not hesitate to cut back the scope of application of the proposed rules, and adapt their design, to better target well-defined objectives and thereby increase the effectiveness of the rules. This Position Statement will propose such an approach especially for the IoT data access and use right of Chapter II.

(6) There is an emerging discussion about whether the Proposal favours the interests of one group of market players over those of others. The reason for this seems to lie in discrepancies between the wording of the operational part of the Proposal and statements in the recitals and the Impact Assessment Report. The Institute considers that such discussion is more likely triggered by a lack of transparency about the objectives of the rules. In many instances, this Position Statement will therefore highlight such uncertainties and present conceptual approaches that the Institute deems appropriate for the design and interpretation of the rules. In doing so, the comments will be guided by public interest and the attempt to reach a fair balance of interests among all stakeholders. In most of its Chapters, the Proposal delineates the rights and obligations of private actors in the data economy. But also in this regard, the public interest in enhancing the sharing of data as non-rival assets in the interest of society at large will be of primary importance. As regards the 'beneficiaries' of the rules, the Institute is of the opinion that the rules should work effectively for all stakeholders. This means for instance that Chapter II should not only increase value for industrial and commercial users of IoT devices, but also for consumers, while not preventing the data holders from using the data.

[3] Explanatory Memorandum of the Proposal, p 7.

(7) Still, from a normative perspective, the Proposal adopts a regulatory approach. It sets out detailed obligations that various kinds of business operators are required to fulfil and that national authorities will enforce pursuant to Article 31. In the light of the freedom to conduct a business laid down in Article 16 Charter of Fundamental Rights of the EU, such obligations should only be adopted provided that (a) there is a clear justification for such intervention; (b) the proposed rules are well-designed and capable – including in comparison to alternative means – of achieving their objectives; and (c) the rules are proportionate in the light of the legitimate interests of all stakeholders and public interest grounds. Thereby, particular attention needs to be paid to the objectives of the individual rules, their scope of application, their effects on different stakeholders and public interest grounds and finally their effectiveness.

(8) The Institute is particularly concerned about the lack of precision of the text as regards private enforcement, although the regulation of the rights and obligations between different actors of the economy is at the very centre of most of the Chapters of the Proposal. This lack of precision runs the risk of not only creating legal uncertainty among private parties. It could also undermine the effectiveness and uniformity of application of the Data Act across the Member States. This is even more the case because the Data Act is proposed as a directly applicable regulation and not in the form of a directive. While questions of interpretation can always be referred to the Court of Justice of the European Union (CJEU), additional precision about the private law implications of the rules is required to reduce the need for referrals by national courts to the CJEU.

(9) Several issues deserve specific consideration across different Chapters. There are three fields of law – (a) intellectual property (IP) law; (b) trade secrets protection; and (c) data protection law – that are in potential tension with the goal of the Proposal to enhance access to data. For all three fields the Proposal seems to rest on the principle that the application of the existing legal instruments in these other fields of the law – with the notable exception of the *sui generis* database right addressed in Chapter X (Article 35) – should be safeguarded. Still, it is equally clear that this cannot discharge the legislature from the need to coordinate the rules of the Data Act with IP, trade secrets and data protection law. This is the reason why, in the following, the Position Statement will first comment on the rules of the individual Chapters and then more comprehensively address the interaction with these other fields of the law (part XI below). This does not rule out that the interface with IP, trade secrets and data protection law will be addressed in the comments on the individual Chapters whenever this seems appropriate. Moreover, the comments will assess the territorial scope of application of the Proposal as set out in Article 1(2) and discuss the – so far neglected – private international law implications of the Proposal (part XII below). The Position Statement will

conclude with further recommendations for the Commission on how to continue its work in view of future actions to promote innovation in the data economy more broadly (part XIII below).

II. The IoT data access and use regime (Chapter II)

(10) The rules in Chapter II addressing the right of the users of 'IoT products'[4] constitute without doubt the core element of the substantive part of the Proposal. The Institute has for a long time favoured additional data access and use rights over the introduction of data ownership rights as a means to enhance the sharing of data.[5] More specifically, scholars of the Institute have argued in favour of a horizontal data access right of the users of connected (IoT) devices as a means to open up the market for aftermarket services.[6] Accordingly, the Institute is in general in favour of such legislation. Still, there are a number of concerns that the Institute wishes to address. In the light of these concerns the Institute recommends a number of changes to the rules contained in this Chapter.

(11) The Institute is in particular convinced that the purpose for which the user may use the data is in need of further clarification and better delineation. More specifically, the rights addressed under Articles 4 and 5 should not include a right to commercialise and monetise the data for whatever purpose. As will be shown below, the Proposal – although with some ambiguities – seems to argue for allowing for such commercialisation, while the Impact Assessment Report seems to advocate the opposite, limiting the permitted use by a third person to added value services.[7] The Institute proposes to limit the scope of the permitted uses both in the operational part and the recitals of the Data Act in line with Policy Option 2 set out in the Impact Assessment Report.

(12) The concern that the text of the Proposal may be too permissive as regards the permitted uses interacts with the other concern that the IoT data access and use right defines the scope of the data that the data holder has to make

[4] This Position Statement will use this term in the following, adopting the terminology of the Proposal. A more intuitive and frequently used term would be 'connected devices'.

[5] 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' (2017) Max Planck Institute for Innovation and Competition Research Paper 17-08, available at <https://ssrn.com/abstract=29259924>.

[6] See Josef Drexl, 'Connected devices – An unfair competition law approach to data access rights of users' in German Ministry of Justice and Consumer Protection and Max Planck Institute for Innovation and Competition (eds), Data Access, Consumer Interests and Public Welfare (Nomos: Baden-Baden 2021) 477-527. See also Josef Drexl, 'Data Access and Control in the Era of Connected Devices', Study on Behalf of the European Consumer Organisation BEUC (Brussels 2018).

[7] Impact Assessment Report, pp 33, 34 and 67-68.

available under Articles 4 and 5 too narrowly by adopting a 'conduct-based' approach, which would exclude access to further-processed data. In contrast, the Institute proposes a both 'purpose-bound' and 'interest-based' approach that would extend access to all, including further-processed, data that are necessary for enabling added value uses and services.

(13) The two concerns interact because, if the data were defined too narrowly in application of the conduct-based approach, it might often not be possible for a third party to provide a related aftermarket service to the user of the product. Conversely, the purpose-bound approach to defining the data can only justify added value uses and services and not commercialisation. Both concerns will be discussed in more detail in the following.

- **Delineation of the permitted uses**

(14) As regards the concern that the Proposal defines the permitted uses too broadly, it is to be noted that Article 4 does not contain any purpose restriction. Quite to the contrary, Recital 28, 1st sentence, explicitly states that '[t]he user should be free to use the data for any lawful purpose.' The situation is slightly different for the third party, who, according to Article 6(1), should only be allowed to use the data for purposes agreed with the user. However, this purpose limitation only confirms the first observation: The user of the IoT product should be considered to be empowered to authorise a third party to use the data for any legal purpose. It is only Article 6(2)(c) that could be read as an indication that the third party is only allowed to use the data for providing a service to the user. The provision states that the third party shall not make the data available to another third party, 'unless this is necessary to provide the service requested by the user'. Hence, despite some doubts arising from Article 6(2)(c), the wording of the operational part seems to support the conclusion that the user could also sell the data to any third party for the sole purpose of generating income.

(15) Yet the question remains whether the IoT data access and use right is really meant to enable the user to commercialise the data in the user's own economic interest. Here, the recitals and the Explanatory Memorandum are even more ambiguous. Recital 28 elaborates on the permitted uses of the data. First and foremost, the IoT data access and use right is expected to overcome a vendor lock-in. The data holder should not be allowed to retain the data for the sole purpose of technically tying aftermarket services, such as repair services, to the IoT product. Thus, the data access right seeks to promote competition, including price competition, in the aftermarkets in the interests of consumers.[8] Convincingly, Recital 28 also explains that overcoming the vendor lock-in could 'stimulate innovation in the aftermarket'. Then, however, Recital 28 immediately adds that the Regulation should also 'stimulate the development

[8] As explicitly explained in the Explanatory Memorandum, p 13.

of entirely novel services making use of the data, including based on data from a variety of products and related services.' Here, unfortunately, the text does not indicate who the innovator can be. Nothing argues against allowing an industrial purchaser of IoT machinery to use the data in the context of its own R&D activities. This should of course also include the right to combine these data with other IoT data this user may have generated by using other products and services. However, the Recital could also be read in the sense that any user, including a consumer, could sell the data to a 'third party' who would use these data for its R&D efforts. As part of such efforts, the third party could enter into respective data use agreements with multiple users of the same kind of product – and produced by the same manufacturer – to build larger datasets.

(16) Indeed, in the Explanatory Memorandum, the Commission seems to more clearly advocate the latter reading. In the Memorandum, the Commission explains that the IoT access and use right should serve two rather distinct purposes, namely, allowing for 'a competitive offer of aftermarket services', on the one hand, and 'broader data-based innovation and the development of products or services unrelated to those initially purchased or subscribed to by the user', on the other hand. In this context, the Commission also states that the right should 'empower' consumers using products or related services to enable innovation 'by more market players'.[9] Even the general goals as formulated by the Explanatory Memorandum may be read in a way that supports the right of the user of the product to commercialise the data. The aims are described as, first, to ensure 'fairness in the allocation of value from data among actors' and, secondly, 'to foster access to and use of data'. In contrast, a purpose-bound approach to defining permitted uses would rather restrict access and use of the data by third parties, while the right of the user to commercialise the data by making it available to any third party would allocate income ('value') to the user of the product.[10]

(17) The Impact Assessment Report follows a much more restrictive, purpose-bound approach. In describing Policy Option 2, on which the Proposal is supposed to build, the Report limits the 'entitlement of third-party companies' to providing 'added value services', which the Report describes as 'any service the provision of which depends on or is improved by data coming from products, including repair, insurance or data analytics'.[11] Unlike Recital 28, the Report remains completely silent on the use of the data for the development of non-related products or services in the context of the IoT data access right. Even more clearly, the table on Policy Option 2 is equally limited

9 Ibid.
10 Ibid, p 2.
11 Impact Assessment Report, p 33.

to 'added value services'.[12] Nor are any secondary (non-added value) uses mentioned in the summary of the preferred option.[13]

(18) This puts the EU legislature in a rather uncomfortable situation. Both the provisions of Articles 4 and 5 as well as the recitals seem to go much further than what the Impact Assessment Report supports. Whether this has occurred due to oversight or whether the Commission intentionally intends to open up the IoT right for any uses is not clear. Therefore, the Commission should provide additional information on how the Proposal should be understood and support clarifications in the operational part and the Recitals of the Data Act. Most importantly, however, the legislature should make up its own mind and decide on the most preferable approach.

(19) As already mentioned above, the Institute recommends that the legislature follow the purpose-bound approach, limiting the permitted uses to added value uses and services, as suggested in Policy Option 2 of the Impact Assessment Report. The primary reason is that there is no justification for opening up this right to any legal uses including commercialisation. It is true that making IoT data available for unrelated uses, such as for the training of AI for various purposes, is key for the future development of the data economy. However, this does not justify an obligation of the data holder to share the data with the user for any purpose. What is more important is that the economic reasoning for opening up aftermarkets does not apply here. Quite to the contrary, competition policy would argue against unlimited uses. Use of the data for purposes unrelated to the product and related services does not affect the economic interests of the manufacturer. Hence, there is no reason to believe that manufacturers are less willing than the users of IoT products to share their data with third parties for secondary uses. Moreover, the individual-level data that the users of IoT products can grant access to do not constitute viable substitutes for the much larger aggregated datasets of the manufacturers. The latter are of much higher utility and value to third parties, for instance, as training data for the development of AI. Direct access to these larger datasets will also help save transaction costs, since the third party will only have to negotiate with the manufacturer as a single person and not myriads of individual users of IoT products. Apart from this the primary interest of users of IoT products, even more so where they are consumers, relates to making full use of the product, and does not consist in commercialisation of the data in unrelated markets One cannot expect that all users, especially consumers, will be particularly willing to engage in the trading of data. Even if the intention of the Proposal is to open up a 'second route' for sharing IoT data, this route will hardly increase the level of sharing.

[12] Ibid, p 34. Nor would Option 3 extend the use of the data by third persons beyond added value services.

[13] Ibid, p. 67.

- **Delineation of the data**

(20) The purpose-bound and interest-based approach should also decide on what data the data holder has to make available. The right has to be 'fit for purpose' and effectively serve the interest of the user. Hence, if the right is expected to enable added value uses and services in the interest of the users, under Articles 4 and 5, the data holder should be required to make those data available that are needed to fulfil that purpose.

(21) However, this is not what the Proposal seems to achieve. Despite the strong claim in the recitals that the right should enable third parties to provide aftermarket services in the interest of the users, the Proposal adopts a purely conduct-based approach to defining the data in the context of Article 4 or 5.

(22) Yet the operational provisions of the Proposal remain opaque. Articles 3(1), 4(1) and 5(1) require a making available of 'data generated by the use of a product or related service'. Article 2 defines the concepts of 'data', 'product' and 'related service', but it does not define what data can be considered as 'generated' by a product or a related service. Hence, in principle, nothing argues against interpreting these provisions in a functional, purpose-bound manner, with the result that they also cover further-processed data, which can indeed be considered as indirectly co-generated by the use of the product or the related service, to the extent that access is needed to enable added value uses and services.

(23) However, where the wording of the provisions is unclear, the Recitals will have to guide the interpretation. It is in the Recitals where the Proposal opts for a conduct-based approach. Recital 14 states that the right should only relate to data that 'represent the digitalisation of user actions and events …, while information derived or inferred from this data … should not be considered within the scope of this Regulation.' This shows that the Proposal takes the user's act of generating the data as the point of departure for defining the data that shall be the object of the right. No credit is paid to guaranteeing the effectiveness of the right as regards the attainment of its purpose.

(24) Indeed, general exclusion of derived and inferred data would seriously endanger the effectiveness of the right. Data collected by embedded sensors or software through IoT products are often quickly analysed and processed to draw additional information from the first-level (sensor) data. This may happen through mere calculation whereby additional information is used (so-called 'derived data'), or through data analysis relying on statistical assumptions (so-called 'inferred data'). It is easy to discern that a third-party provider of aftermarket services will almost ever need access to such derived and inferred data. For instance, in the context of predictive maintenance of specific industrial machinery, it may be necessary to identify an overheating of the machine. Sensors embedded in the machine can only register variations

of the temperature over time. This is not sufficient for knowing when intervention is needed. Of course, the machine will often have – and should have – an inbuilt mechanism of automatically stopping the operation when it overheats. However, it is the very purpose of predictive maintenance to avoid such interruption. To know when intervention is needed, a range of temperature tolerance has to be defined. This however is information that only the manufacturer can provide. Based on such information, a computer can calculate whether the machine is indeed overheating (case of derived data). Yet whether the machine is affected by a technical defect (and what kind of defect) requiring maintenance constitutes (probabilistic) information in terms of inferred data, since there could also be external causes for the overheating. This simple example shows that 'data generated by the use of the product' as understood in the recitals will not suffice to enable a third-party provider to deliver an aftermarket service.

(25) Therefore, for defining the relevant data, the Institute recommends preferring a functional purpose-bound approach to the Proposal's conduct-based approach. In this regard, the EU legislature would be following models in the field of sector-specific regulation. In particular, the type approval legislation[14] does not limit the data access right for enabling the repair of motor vehicles excluding derived or inferred data. Rather, it adopts a purpose-bound approach by defining the data that the vehicle manufacturer is obliged to provide as 'repair and maintenance information'.[15] Hence, under Article 4 of the Data Act Proposal, the user of the product should equally be vested with a right to access and use all data, including derived and inferred data, that are required for the related (aftermarket) service (such as predictive maintenance). The recitals could clarify that the data holder is obliged to provide access to all the data that it would provide to a potential subsidiary to which the manufacturer outsources the provision of the aftermarket service.

(26) In addition, the arguments that the recitals provide for the conduct-based approach are not convincing. These arguments are two-fold. On the one hand, the recitals seem to consider the act of generating the data a justification for recognising the right in the first place. Hence, one may conclude that the IoT access and use right should therefore not go beyond the data that are the direct results of the use of the product or related service. On the other hand, the recitals argue that extension of the right to derived and inferred data would conflict with intellectual property protection. Both arguments will be rejected in the following.

[14] Referred to by the Commission in the Explanatory Memorandum, p 6.

[15] See Art 61 Regulation (EU) 2018/858 of the European Parliament and of the Council of 30 May 2018 on the approval and market surveillance of motor vehicles and their trailers, and of systems, components and separate technical units intended for such vehicles, amending Regulations (EC) No 715/2007 and (EC) No 595/2009 and repealing Directive 2007/46/EC, [2018] OJ L 151/1.

(27) As regards the justification, Recital 6, 1st sentence, obviously building on the goal of 'ensuring fairness in the allocation of the value from data among the actors in the data economy' as put forward in the Explanatory Memorandum,[16] relies on the nature of IoT data as data that are at least co-generated by two actors, the designer or manufacturer of the product, on the one hand, and the user, on the other hand. At the same time the Commission relies on the importance of the data as an input for 'aftermarkets, ancillary and other services'. In sum, the Commission seems to argue that, since the user has contributed to the generation of the IoT data, the data holder should not be allowed to exclude competitors from the relevant service markets by denying access to the data to the disadvantage of the user as a co-generator of the data. Consequently, the IoT data access and use right of the user is proposed, whereby the right is vested in the user as a co-generator of the data.

(28) However, this justification rationale cannot explain the exclusion of further processed data. For such data, one could equally ask who the data generators are, and with the same logic one can hardly consider the designer or manufacturer of the device as the sole generator of the processed data. Such processing, as seen in the above example (para 24), may often take place within the product (making use of so-called embedded software) and constitute the direct result of a related service as mentioned in Articles 3(1), 4(1) and 5(1). Hence, it cannot be argued that use of the product necessarily excludes processed data, if it is the product itself, including embedded software and the related services, that produces the new data and this production was caused by the use of the product. What changes is that after the creation of the first-level data, such as the registration of the temperature of the machine, further processing makes use of additional information contributed by the data holder. However, such additional contribution does not argue against qualifying the resulting new (processed) information, such as the information that the temperature falls outside the range of tolerance and that the machine most likely has a defect that requires maintenance, as data that are not co-generated by the user. At best, one could argue that the share contributed by the user of the product contributed to the generation of processed data is smaller than in the case of non-processed data. This only confirms that 'co-generation of data' is to a large extent a matter of degree. This proves that the 'generation of data' cannot work as an objective and absolute criterion of fairness for the allocation of rights and the scope of these rights. At best, the amount of contribution is only one factor that has to be weighed with other criteria.[17] In this regard, one has to take into account the

[16] Explanatory Memorandum, p 2.

[17] In this regard, the Institute does not fail to note that the co-generation of data is increasingly used for the allocation of data rights in the data economy. A good example is the ALI-ELI Principles for a Data Economy – Data Transactions and Data Rights, Adopted by the ELI Council in September 2021, available at

interests of all co-generators, whereby their respective shares in the co-generation only constitute one set of considerations. It is certainly not less important to also take account of the legitimate interests in data access of the user as well as the legitimate interests of the data holder to control the data. In the latter regard, the nature and importance of the respective interests as well as the degree of data dependence of the user and the potentially negative consequences of sharing need to be considered. Moreover, this weighing process should decide on both the recognition and the design of data rights. This would mean that for data access and use rights the legitimate interest and degree of dependence of a user on data access can justify broader access to data, even if the user has not contributed so much to their generation, while in a case of a minor interest and lower level of dependence, the contribution to the generation of the data has to be larger. This shows that, where it is indispensable that the data holder makes the necessary data available to enable added value uses and the provision of added value services by third parties, the share that the user contributes to the data generation can be rather small and should therefore not exclude access to calculated or inferred data *per se*. However, the legitimate interest in data access is limited to gaining access to the data needed to enable the respective added value use or service. This confirms that, even if the legislature decided to make use of the concept of 'co-generated' data, it would have to define the data that the data holder should make available in a purpose-bound and interest-based approach.

(29) As regards the second reason, Recital 17 argues that the right must not extend to 'data resulting from any software process that calculates derivative data from such data [generated by the use of the product] as such process may be subject to intellectual property rights'. This Recital does however not in any way further explain the nature and availability of intellectual property protection in such a case. Quite on the contrary, in the light of existing intellectual property law, the argument is puzzling. Copyright protection for computer programs extends neither to the use of the program[18] nor to the data that are generated by using the program. At best, one may think of patents concerning computer-implemented inventions. Where the patent protects a product (a machine in which a computer program is implemented), protection will however not extend to the information that is the result of the use of the product. Whether protection of process patents relating to data processing

<https://europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Publications/ALI-ELI_Principles_for_a_Data_Economy_Final_Council_Draft.pdf> accessed 14 April 2022. Part III Chapter B provides for principles on data rights with regard to 'co-generated data'. There, Principle 18(1) relies on the several factors and is based on the notion that co-generation depends on the degree of contribution. Most importantly, the degree of contribution also influences the question of whether a co-generator has to be vested with a particular data right. According to Principle 19(2) this requires a balancing of different interests, where the share a co-generator has contributed to the data generation is one consideration.

[18] As explicitly stated in Art 5(1) Directive 2009/24/EC of the European Parliament and of the Council of 23 April 2009 on the legal protection of computer programs, [2009] OJ L 111/16.

extends to the information as the direct product[19] is a still rather unsettled legal question under current national patent laws. To the extent that the German Federal Supreme Court has already addressed this question, the Court's restrictive approach makes it very unlikely that such protection would ever be recognised as regards IoT data.[20] Accordingly, Recital 17 should not be followed as regards the assessment of a risk of conflict with IP law. Moreover, Recital 17 does not claim that intellectual property will be an obstacle in all cases. Hence, intellectual property should not be argued as a reason for generally excluding derived and inferred data from the data access and use right. At best, it would suffice to accept intellectual property protection as a defence on a case-by-case basis, against claims based on the data access and use right.

(30) To conclude, the EU legislature is recommended to clarify the notion of 'data generated by the use of a product or a related service' as used in Articles 3(1), 4(1) and 5(1). As regards the latter two provisions, the delineation should follow the described purpose-based approach. However, this approach hardly fits Article 3(1). This provision requires data accessibility by default and, hence, implementation of this requirement as part of the general product design. Hence, the scope of data access has to be designed uniformly for all products. This argues for delineating the data more narrowly, namely, only with regard to the data based on the first encoding that follows the use of the product or the related service. In sum, the EU legislature could implement this distinction by adding the following definition to Article 2:

> 'data generated by the use of a product or related service' means
>
> - data that represent the direct digitalisation of user actions or events,

[19] See Art 25(c) Agreement on a Unified Patent Court, [2013] OJ C 175/1 (defining the scope of future European patents with unitary effect).

[20] The German Federal Supreme Court does not exclude such protection *per se*. See *Bundesgerichtshof*, 21 August 2012, Case X ZR 33/10, *MPEG-2-Videosignalkodierung* (2012) Gewerblicher Rechtsschutz und Urheberrecht 1241. However, the Court adopted a very restrictive approach to recognising such protection; see *Bundesgerichtshof*, 27 September 2019, Case X ZR 124/15, *Receptor Tyrosine Kinase II* (2018) 49 IIC 231, para 21 (English translation). Most importantly, the Court requires that the data sequence as such have utility on the basis of its structure and its technical presentation (and not the information it contains) and that, especially in the light of its reusability comparable to a physical item, such data sequence would generally be eligible for patent protection (not requiring the other elements of patentability to be fulfilled). Accordingly, in the case at hand, this excluded the patent protection for the result of a gene analysis where the applied analysis was protected under a process patent. Statutory patent law supports this by excluding the 'representation of information' from patent protection. See Article 52(2)(d) European Patent Convention. Similarly, scholarship argues against such protection to safeguard the default rule that information as such should not generally become the subject-matter of IP protection. See also Drexl (2018) (n 6) 87-89.

- in the case of a user of a product or related service requesting the making available of data for the purpose of enabling an added value use or third-party added value service, data that result from the use of a product or related service, not excluding derived or inferred data, to the extent that access and use are required for enabling the specific added value use of the user or the provision of a specific added value service to the user.

(31) For the purpose of completeness, it should be mentioned that the delineation of the data just proposed for Article 3(1) would also have to apply in the context of Articles 4 and 5 if the legislature, against the Institute's recommendation, decided to allow for unlimited legal use, and the data access request is not pursuing an added value use or service. As in Article 3(1), the right of unlimited use would take control away from the data holder over how the data could be used. Hence, extension to derived and inferred data would indeed not be justified. In turn, the limitation to 'data that represent the direct digitalisation of user actions or events' would considerably reduce the utility and attractiveness of the data for third persons. This is another reason that argues against allowing for unlimited legal use of the data under Articles 4 and 5.

- **The economic justification for the IoT data access and use right**

(32) This Position Statement has already sketched the weighing of interests as part of a fairness justification of Chapter II. However, in the field of business regulation, intervention should especially be justified from an economic and competition-policy perspective. Although the recitals refer to economic goals, such as promoting competition in aftermarkets, the economic justification for Chapter II remains unclear. The key challenge here is whether market failures and imperfections exist that the proposed rules can remedy.

(33) To start with, Article 3 reacts to the ability of manufacturers of IoT products to unilaterally exclude the accessibility and, hence, usability of the data by third persons based on the product design. However, from a competition-policy perspective, the manufacturer of IoT devices cannot be compared to other actors in the data economy. Their position in the market differs from the large platform operators of the Internet economy that are identified as 'gatekeepers' as termed by the proposed Digital Markets Act (DMA).[21] Unlike these gatekeepers, the manufacturers of IoT products do not benefit from network effects that considerably reduce the contestability of their position in the primary market. Indeed, markets for IoT products should in

[21] Proposal of the Commission of 15 December 2020 for a Regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act), COM(2020) 842 final.

principle be expected to be rather competitive. The fact that one manufacturer decides to bring products to the market that are equipped with data collecting and processing features will not prevent its competitors from doing the same. Quite to the contrary, the so-called 4th industrial revolution seems to be very much driven by competition among competitors. Hence, one would expect that competitive pressure on the primary market should force the manufacturers in the secondary market for the data to enable the users to access and use IoT data in their interest.

(34) On the other hand, markets for IoT products are not free of competition concerns. The design of the product and factual data control enable manufacturers to reserve aftermarkets for added value services, such as repair and maintenance services, for themselves. Competitive pressure on the upstream product market can be considerably reduced due to information asymmetries. For the user, the likelihood that the product will be in need of repair can hardly be assessed. This is especially the case for motor vehicles, where such need depends on multiple factors in addition to the quality of the vehicle, namely, the intensity of use as well as the driving habits not only of the concrete user but also external factors that may cause accidents. For this reason, the European Design Regulation recognises a repair clause providing that replacement parts that are used for repair purposes will not infringe rights protecting the design parts of complex products.[22] Without such exception, motor vehicle providers would not only be able to control the market for replacement parts, but also the repair services market. The provisions of Chapter II react to the same problem based on the insight that the manufacturer is not in need of an intellectual property right for the data to control the repair market. For the manufacturer *de facto* control of the data suffices to reach similar results. *De facto* control of the IoT data hence creates a risk of vendor lock-in, which makes the user dependent on the manufacturer as the single provider of added value services.

(35) However, such vendor lock-in can only be expected where the manufacturer has sufficient market power to deny data access in relation to its customers. This does not necessarily have to be the case. There can be instances where it is the customer who is in a position of superior bargaining power vis-à-vis the manufacturer, such as a large industrial customer vis-à-vis the seller of industrial machinery or a large (national) transport company that orders huge numbers of vehicles (such as buses) in competitive markets. In such instances, the user may even claim to become the single data holder, which may raise the question of whether the law should not equally guarantee that the manufacturer will retain a right to use the data.

[22] Art 20(2)(b) and (c) Council Regulation (EC) No 6/2002 of 12 December 2001 on Community designs, [2002] OJ L 3/1.

(36) As regards the remedies, the question is also whether competition law does not provide appropriate solutions. On the one hand, competition law may fail because the party claiming data exclusivity does not hold dominance, and defining the market very narrowly, namely, for the individual brand product, may be disputed. On the other hand, some national competition laws have developed rules that can address such cases. In particular, Germany reformed its competition law at the beginning of 2021 with a view to strengthening its effectiveness in the digital era.[23] On this occasion, it also amended Section 20(1), which traditionally makes downstream or upstream market foreclosure a violation of competition law. By requiring 'significant imbalance between the power' of the parties involved ('relative market power'), German competition law specifically addresses cases of unequal distribution of bargaining power. Introducing a new Section 20(1a), the reform clarified that relative market power can also exist in a case of dependence on access to data held by another undertaking.

(37) Articles 4 and 5 of the Proposal seem to address such case of data dependence. However, they only do so with regard to downstream foreclosure. The Data Act does not address the equally existing problem of potential upstream data dependence, to which especially suppliers of component parts can be exposed. Where such component parts are built into IoT products, the use of the device may also produce technical information that can be highly valuable for the supplier to improve its products and to innovate. In this regard, the EU legal framework for the data economy will still contain a loophole that should be addressed in the future.

(38) As regards the Data Act Proposal, it is to be noted that Chapter II does not make the exercise of the data access and use right dependent on the existence of economic dependence of the user in the individual case. This may appear as problematic from a competition policy perspective, even more because intervention of competition law in case of mere 'relative market power' – without the need to prove market dominance – is anyhow placed at the fringes of what many would consider legitimate competition law. However, the competition law framework should not prevent the legislature from introducing competition policy-informed rules of general application that prohibit business operators from deviating from conduct that one would expect in situations where the bargaining power is distributed equally.

(39) In addition, one should also note that it is not exclusively the market that distributes the bargaining power unequally. Manufacturers can unilaterally seek and attain superior bargaining power by technically preventing their customers from accessing the data. Thereby, the manufacturers can determine

[23] 10th Amendment Act of 18 January 2021; Gesetz zur Änderung des Gesetzes gegen Wettbewerbsbeschränkungen für ein fokussiertes, proaktives und digitales Wettbewerbsrecht 4.0 und anderer Bestimmungen (GWB-Digitalisierungsgesetz), [2021] Bundesgesetzblatt I p. 2.

how the markets for aftermarkets will work. To remedy this power of designing market conditions, it is legitimate and economically sound that the law prevents the manufacturer from tying aftermarket services to the sale of the primary IoT product.

(40) However, this reasoning can only support the purpose-bound design of the IoT data access and use right in Articles 4 and 5. For extending this right to allow the user to use the data for any legal purpose, the EU legislature would need to rely on a different economic justification. And, indeed, there are clear limitations to economically justifying such non-limited data access right. On the one hand, one should note that IoT data as non-rival assets could also serve multiple secondary (non-related) purposes, such as for the development of AI. This argues generally in favour of enhancing the sharing of such data. Still, the mere non-rival character of the data and their utility should not *per se* justify an obligation of the data holder to share the data with the user for any such purpose. Quite to the contrary, competition policy arguments argue against such extended right as has already been explained further above (para 19).

(41) Moreover, the Commission, if it does in fact intend to argue in favour of allowing the user to commercialise the data, may not even be seeking such economic justification, but intend only to enable users to participate in the economic income that sharing of IoT data for secondary purposes could generate.

(42) The belief that the law has to allocate the value of the commercialisation of data to a specific person is reminiscent of the earlier idea the Commission expressed in its Communication of 2017 on the potential introduction of a data producer's right.[24] However, even at that time, the allocation of such right to the owner or long-term user of an IoT product was exclusively conceived as a means to 'unlock machine-generated data' that are typically controlled by the manufacturer.[25] Mere reference to fairness should not be used as a justification for rules that exclusively pursue distributive goals without being able to rely on specific additional value judgments and goals in the law.[26]

(43) In sum, from an economic perspective, the IoT data use right only seems justified with regard to the use of the data for overcoming vendor lock-ins.

[24] Communication from the Commission of 10 January 2017 – Building a European Data Economy, COM(2017) 9 final, 13.

[25] Ibid.

[26] An example of such rules is the guarantee of appropriate and proportionate remuneration of authors and performing artists in copyright law. Apart from reacting to a potential imbalance of bargaining power, these rules seek to guarantee the goal of copyright law to adequately remunerate these two groups of persons as an incentive for creativity. See Title IV, Chapter 3 of Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC, [2019] OJ L 130/92.

The Data Act should not adopt the principle that the user may use the IoT data access and use right for any legal purpose. Rather, the right should be formulated in a purpose-bound manner.

- **The IoT data access and use right as a non-exclusive right**

(44) As explicitly confirmed in Recital 6, the proposed data access and use right shall not be recognised as an 'exclusive right'.[27] The Institute fully supports this statement. Recital 6 is based on the insight that data should in principle not be owned by anybody. Therefore, the data access and use right should only create a statutory obligation of the data holder to grant access to the data. Its function is limited to overcoming the *de facto* control of the data. It is not designed to exclude data use of third persons that may eventually have access to the data and may be capable of using the data. Conversely, an exclusive right would create considerable uncertainty about whether a person can use data without the authorisation of third persons that may potentially hold exclusive rights in the data. As in the case of intellectual property, recognition of exclusive data use rights would require the parties of any data-sharing agreements to clarify whether there are third-party rights that stand against the envisaged use of the data. Such rights clearing translates into increased transaction costs with a negative impact on data sharing. The reasons for the rejection of the exclusivity of the right are the same as those for restricting *sui generis* database protection in Article 35.

(45) However, the text of Chapter II does not reflect the nature of the data access and use right as a non-exclusive right. Quite to the contrary, Article 4(6), 1st sentence, stating that 'the data holder shall only use any non-personal data generated by the use of a product or related service on the basis of a contractual agreement with the user', could be misunderstood in the sense of establishing an exclusive data use right of the user of the product.

(46) The provision does not clarify the available remedies in case the data holder uses the data without any contractual agreement with the user. However, it should not come as a surprise to anybody if national courts took this provision as a legal basis for granting injunctions against data holders to prevent them from making use of the data. If the users of IoT products could claim injunctions to enjoin data holders from using the data, the conclusion should be clear: Article 4(6), 1st sentence, would vest the user with an exclusive data use right. Recognition of such an exclusive right would seriously affect the legitimate interests of both the manufacturers and third persons and hamper free movement of data. When a data holder makes IoT data available to a third person, such latter person would be forced to investigate whether such data sharing occurs with the authorisation of the users of the IoT products that were used for the generation of the data. Since the aggregated datasets of the

[27] In the same sense, see the Impact Assessment Report, p 154.

manufacturers as data holders originate from myriads of different users, the required rights clearing would create prohibitive transaction costs and unbearable legal uncertainty for the third-party recipient of the data.

(47) The obvious conflict of the wording of Article 4(6) with the statement in Recital 6 that the data access and use right is not to be understood as an exclusive right makes Article 4(6) a most opaque provision. The question is what other purpose this rule pursues and whether this rule should either be deleted in its entirety or clarified in the light of the intended purpose.

(48) Some indication of the function of this provision can be found in Recital 24. This Recital primarily highlights the role of the General Data Protection Regulation (GDPR) in governing the legality of the use of personal data by the data holder. Recital 24 clarifies that it is exclusively the GDPR that provides the legal basis for such use. Then, the Recital also addresses the 'basis' for the manufacturer to use non-personal data and finally concludes that this ought to be a contractual agreement between the manufacturer and the user. Article 4(6) is formulated in line with Recital 24. The application is limited to non-personal data, and it requires the data holder to enter into a contractual agreement with the user of the product as a requirement for using the data.

(49) However, the reasoning of Recital 24 as regards non-personal data cannot be followed. This reasoning would indeed lead to the unwanted result that power to control the use of the data would be allocated to the user in the sense of an exclusive right. Moreover, the reasoning of the Recital wrongly assumes that there is a need for a legal basis to use non-personal data. To the extent that non-personal data is not controlled by any intellectual property right or trade secrets law, a person being in control of or having access to non-personal data should always be allowed to use it. The Data Act should build on the default rule that the use of accessible non-personal data is in principle free and no legal basis is needed for its use. In the terms of intellectual property law, non-personal data should in principle be considered to fall into the 'public domain' for the very purpose of promoting data sharing in the interest of society. Article 4(6), 1st sentence, breaks with this principle by requiring the user's authorisation for the use of non-personal data.

(50) However, this wrong assumption does not preclude that the Commission is still pursuing additional purposes with Article 4(6), 1st sentence. In this regard, the second sentence of Article 4(6) may provide some guidance. The Institute is in support of maintaining this second sentence. It prevents the data holder from using non-personal data in a way that runs counter to the commercial interests of the user of the IoT product. Protecting the legitimate interests of the user of the product, the provision is obviously inspired by both data protection law and trade secrets law. In the context of the first sentence, the rule seems to serve the purpose of limiting the contractual freedom of the user

when the user authorises the data holder to use the data. It protects the user where the data holder benefits from superior bargaining power.

(51) Another reason for requiring a contractual agreement on access and use in the framework of Article 4 consists in making Article 13 on the unfairness control of data sharing agreements applicable between the data holder and the user. This raises the question whether the denial of a right of the data holder to use the data without contractual agreement with the user is intended to work as leverage to force the data holder to enter into such an agreement the terms of which could then be controlled under Article 13.

(52) In this regard, however, the Proposal would overshoot the mark. On the one hand, there is no guarantee that, where the parties entered into a sale, rental or lease of the product, this contract would also include an agreement on the use of the data by the data holder. Parties may often overlook the need for such agreement. This could easily result in follow-on disputes on whether the existing contract includes an 'implied licence' granted to the data holder and, if not, whether the data holder should be held liable to pay damages for past unauthorised use of the data. Furthermore, the group of relevant users can include multiple persons and can constantly change over time, especially in the case of durable products. When a product is sold by a user, under Article 4(6), 1st sentence, the data holder may lose the right to use the data without even being aware of this event. At the least, Article 4(6), 1st sentence, would therefore need to be interpreted narrowly in the sense that it only applies as of the moment the user has made a request for data access under Article 4(1). However, also in this case, the data holder would have to stop using the data for the time being. Such obligation could equally undermine the working of existing agreements concerning the sharing of the relevant real-time data between the data holder and third persons. And finally, preventing the data holder from using the data would not strike an appropriate balance between the interests of the user and the data holder. Articles 4 and 5 establish a statutory regime for data access and use for the user. Once the data holder has fulfilled its obligation to make the data available to the user according to Article 4(1), the user is also allowed to use the data. Since, in this situation, the user can already exercise these statutory rights, there does not seem to be any reason why the data holder should be prohibited from using the data.

(53) This means that Article 4(6), 1st sentence, should not be maintained. An alternative rule would consist in an obligation of the data holder to enter into such a data sharing agreement that can more specifically define the right of the data holder to use the data. Such an amendment would make clear that the data holder is not restricted in using the data in situations where the existing agreement on the sale, rental or lease of the product between the two parties does not address the right of the data holder to use the data or where the parties

have not entered into any contractual agreement. Accordingly, the first sentence of Article 4(6) could be replaced by the following text:

> The user can request the data holder to conclude an agreement on the use of non-personal data generated by the use of a product or related service. As part of such agreement, the user can limit the data holder's use of any such non-personal data.

(54) Still the Institute recommends deleting the first sentence without any replacement. The reasons are as follows: First, it seems that the second sentence of Article 4(6) already sufficiently takes care of the user's legitimate interests in restricting the use of data by the data holder. This second sentence can be applied without conclusion of an agreement on the use of the data with the user. Secondly, an obligation of the data holder to enter into a data sharing and use agreement raises the question about the appropriateness of the terms of such agreement and, hence, the question of whether Article 8 should not be applied to Article 4 as well. For very good reasons the Proposal seems to opt against the application of the FRAND system (relating to fair, reasonable and non-discriminatory contract terms) of Article 8 to Article 4. FRAND disputes are complex and burdensome for all parties. They should in particular be avoided where the user is a consumer. Thirdly, there can be scenarios where the user is the stronger party and therefore could impose inappropriate restrictions on the data holder's possibilities to use the data. Article 4(6) should not create the impression that the user has a right to impose any contractual restriction on the data holder. Whether a contractual relationship among the two parties is affected by an imbalance of bargaining power should exclusively be assessed under the rules of Chapter IV of the Data Act, which should also be applied to protect the data holder as the weaker party.

(55) This still leaves the question open how important it is to trigger a contract that can be controlled under Article 13. In this regard, one should note that Article 13 is designed to make unfair contract terms inapplicable. Hence, Article 13 presupposes the existence of a contract, while an 'unfair' refusal to enter into a contract cannot be sanctioned. This means that Article 13 is anyhow applicable where a contract on the use of data is concluded. The deeper reason for the Commission's intent to trigger a data sharing agreement between the data holder and the user in the context of Articles 4 and 5 is the incompleteness of these rules concerning the terms of data use. This argues for a duty to conclude such contract and, once such contract is concluded, Article 13 would be applicable. However, one wonders in which regard the statutory duties can be regarded as incomplete. What Articles 4 and 5 do not require are issues of liability for non-performance or insufficient performance of the statutory duties. Indeed, several clauses of Article 13(3) and (4) address contractual liability. However, it can seriously be questioned whether application of Articles 4 and 5 will be in need of 'contractual' liability rules. Where a data

holder does not sufficiently fulfil its statutory requirements under Articles 4 and 5 and causes harm to the user, the data holder can be held liable under the applicable national tort law. National private law rules on obligations and non-fulfilment of obligations will typically also apply where the obligations arise from statutory provisions. Hence, the Institute does not see why in case of a deletion of Article 4(6), 1st paragraph, the regime of the IoT data access and use rights should not fully and effectively function.

- **Definition of key concepts used in Chapter II**

(56) Article 2 defines certain concepts that are key for the application of Chapter II. The Institute is of the opinion that not all of these definitions are fully satisfactory. In addition to some amendments, the Institute wants to propose additional definitions that it finds missing.

(57) As regards the definition of 'data' in Article 2(1), it is not fully clear what 'compilation' in comparison to the term 'collection', the term used in the Database Directive to define a database,[28] means. This raises the question of whether the provisions of Chapter II can also relate to databases as such, meaning that a user could claim access to entire databases. The Institute does not see any argument against such understanding. The fact that a collection/compilation of data qualifies as a 'database' does not automatically mean that the database will also enjoy copyright protection or *sui generis* database protection pursuant to the Database Directive. Many databases are not protected at all. In addition, Article 35 guarantees that the *sui generis* database right will not hinder the exercise of the rights under Chapter II.

(58) In contrast, the term 'product' in Article 2(2) appears to be defined too narrowly. Here, the Institute recommends deleting the exclusion of items 'whose primary function is not the storing and processing of data'. As Recital 15 explains, the proposed exclusion is meant to exclude devices that are meant to display or play, record or transmit content. What the exclusion of such devices seeks to achieve is that digital content will not be covered by the rights under Chapter II. This seems justified for two reasons: first, such content is the direct result of human, oftentimes creative, activity the purpose of which is the very creation of this content. This distinguishes such content from typical IoT data that a product autonomously generates as a consequence of the use. Second, such content may often be protected under copyright law. Hence, the exclusion of respective devices from the definition of a 'product' will exclude potential conflicts with copyright law and the data access regime. However, all this reasoning only justifies the exclusion of the respective content from the definition of 'data' and not the definition of a 'product'. Devices that are meant to be excluded according to Recital 15 include in

[28] See Art 1(2) Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases, [1996] OJ L 77/20.

particular personal computers, tablets, smartphones, cameras and scanners. To exclude them completely would result in a considerable weakening of the intended protection as regards a most important category of devices that especially consumers use every day. There is no reason why a user of a smart watch can rely on Article 5 to get the watch repaired by a third-party service provider while such right would not be recognised with respect to a camera or a smartphone. Complete exclusion of such devices is not at all warranted. As a better solution, the Institute proposes that, first, the exclusion of such devices from the definition of a 'product' should be deleted and, second, 'content-related data, such as writings, music, photographs and films, that have been encoded by the use of a device whose primary function consists at least *inter alia* in assisting a person creating or recording such content' should be excluded from the notion of 'data generated by the use of a product or related service' (for including a specific definition of this term see paras 22-30 and 63).

(59) The definition of the 'user' in Article 2(5) is key to identifying the entitled holder of the IoT data access and use right. Here, while not suggesting a different wording, the Institute calls to mind that the interpretation should follow an interest-based approach. This means that only a person who has a legitimate interest in data access should be identified as the 'user' of a product in the sense of Articles 4 and 5. Hence, being the owner of the device or having rented or leased the product should not suffice *per se* to consider such person as a user. The proposed narrower interpretation correlates with the purpose-bound approach to the permitted uses. Only a person who is in need of using the data on her or his own behalf to generate additional value (so-called 'added value use') under Article 4 or who requests a making available of data to a third party to enable this party to provide an added value service under Article 5 should be considered as users. This would considerably limit the instances where a data holder has to deal with several users.

(60) Yet, in other regards, it is not clear whether Article 2(5) will cover all persons who should indeed be granted the data and access right. By referring to persons who own, rent or lease a product, the Proposal requires a legal title in the product. Conversely, Article 2(5) does not seem to require that this person is also personally using the product. Conversely, persons that use the product without having such legal title will not be vested with the right. Hence, use of a product by a family member of the owner will not grant access of that family member to the data. Data access can only be sought by the owner. This solution may make coordination with data protection rules, including the data portability right under Article 20 GDPR, more complex but not impossible. In sum, this approach deserves support to narrow down the group of persons who qualify as users. Otherwise, even mere by-standers from whom products produce data (especially images) in publicly accessible places could qualify as users.

(61) In other regards, Article 2(5) may not be broad enough to also cover all cases where a person is only the recipient of a service for which the service provider uses a product. This would in particular cover the case where a small farmer cannot afford to buy all the machinery that is needed to work the land and therefore enters into an agreement with a farming service provider who will provide such services using its own machines and personnel. Where such machinery collects data from the land of the farmer and the data will be controlled by the manufacturer, the farmer should also be entitled to request a making available of the data under Articles 4(1) and 5(1) to benefit fully from the data collected from her or his land. Article 2(5) could be read as covering such case to the extent that it also includes persons who 'receive a service'. However, this wording could be misinterpreted in the sense that it only refers to 'related services' in the sense of Article 2(3). Therefore, the Institute recommends making the application of definition clearer at least in Recital 18. The proposed wording of this recital is currently incomplete to the extent that it does not explain the additional case of 'receiving a service' mentioned in Article 2(5).

(62) The definition of the 'data holder' in Article 2(6) does not raise any concerns. The term 'data holder' is also used in Chapter III of the Proposal. There, the term is used as a generalisation of the person who is under an obligation to make data available pursuant to other legal instruments of EU and national law. In contrast, in the context of Chapter II, Article 2(6) lays down the substantive requirements for identifying the person who will have to make data available under this Chapter. In this regard, the provision relies on the 'ability' to make the data available. However, in the context of Chapter II, Article 2(6) additionally requires that this ability has to be based on the 'control of the technical design of the product and related service'. This should make sufficiently clear that it will typically be the manufacturer alone who has to fulfil the obligations of the data holder under Chapter II. This could however be made clearer in the Recitals. In addition, the EU legislature could clarify that a complete transfer of the data to another person will not exempt the manufacturer from the obligations under Chapter II. Hence, the manufacturer should be considered to be under an obligation to retain the right to order a person to whom the data was transferred to make the data available to the users of the products. In this way, the Data Act would guarantee that the manufacturer cannot evade the obligations under Chapter II by selling and transferring the data to another person.

(63) As already explained, the legislature should include an additional definition of 'data generated by the use of a product or related service' (paras 22-30 and 58 above).

(64) In order to implement the purpose-bound approach as recommended above (paras 16-19), the EU legislature should also define the concepts of 'added

value use' (as to be used in Article 4) and 'added value service' (as to be used in Article 5). As explained above, Article 5 is designed to enable users to overcome a vendor lock-in as regards added value services on the aftermarket level. The definition of 'added value service' should therefore be defined broadly, namely, in the sense of 'any service provided to the user that can be enabled or improved by access and use of the data generated by the use of the product or service'. The term 'added value use' should be defined along the same lines. Especially commercial users may not necessarily depend on third-party service providers to make full use of the data for the purpose of conducting their business. A manufacturer who has acquired connected machinery should have a choice as to whether it will take data-based maintenance services from the manufacturer of the machine, a third-party service provider or whether it prefers to organise maintenance through an in-house maintenance unit. Accordingly, 'added value use' should be defined as 'use of the data for the purpose of enabling or facilitating the satisfaction of the user's personal – including private and commercial – needs'.

(65) Articles 4(1) and 5(1) lack precision as to the concept of the 'making available of data', while Article 3(1) uses the concept of direct accessibility. Since there is neither a definition of 'making available of data' in Article 2 nor further explanation given in the recitals, it is not clear whether this concept only involves an obligation to grant access to the data in the form of *in situ* accessibility, whether the user should also be allowed to copy the data and to port the data or whether there is even an obligation to transfer the data. As regards the obligation to allow for direct accessibility of the data in Article 3, Recital 21 seems to limit the obligation to granting *in situ* accessibility. In this context, Recital 21 also uses the term of 'making available'. This could be understood as an indication that the concept of making available indeed does not go any further than requiring *in situ* accessibility. While the recitals only repeat the term 'making available of the data' in relation to Articles 4 and 5, the Impact Assessment Report describes the data access and use right as a 'data access and portability right'.[29] Moreover, the use of the term 'transmitting the data' in Article 5(7) raises the question whether the user can generally claim transmission of the data to a third party.

(66) In sum, there is a clear need to clarify the concept of making available in Articles 4 and 5. To guarantee that the rights can be exercised effectively, mere *in situ* accessibility may often not be enough. To remedy this shortcoming the Institute recommends the legislature to consider introduction of specific requirements of holders of IoT data to promote interoperability as part of Chapter VIII (see para 219 below). Moreover, the Institute recommends adding a definition of 'making available of the data generated by the use of a product or related service', which should go beyond *in situ*

[29] Impact Assessment Report, p 67.

accessibility. In particular, this definition should be coordinated with the data portability right under Article 20 GDPR. What a data controller is obliged to do pursuant to this provision as regards the portability of personal data should at least be recognised as the minimum standard under Articles 4 and 5. The legislature could consequently enact the following definition:

> 'making available of data generated by the use of a product or a related service' means the making accessible of data by a simple request through electronic means, enabling the user or a third party to copy the data and to receive the data in a structured, commonly available and readable format.

(67) This definition integrates the second sentence of Article 4(1) into the definition, though without the requirement of 'technical feasibility'. The Institute wants to stress that, for making data more accessible and reusable, data interoperability is key. In this regard, it is regrettable that in Chapter VIII on interoperability the Proposal does not contain obligations of data holders as regards objective requirements for interoperability, although such obligations are proposed for specific groups of other service providers in the data economy. If the legislature implemented such requirements also for data holders in the sense of Chapter II, the reservation regarding technical feasibility could be deleted. Provided that the requirements for interoperability are fulfilled, the data holder should be considered to fulfil its obligation to make the data available under Articles 4 and 5.

- **The triangular structure of the relationships among the data holder, the user and the third party**

(68) The conceptual approach to regulating the relationships among data holder, data user and third party is not intuitively apparent from the text and structure of the Proposal. A closer analysis of the proposed provisions however helps distinguish three different sets of provisions that specifically focus on the relationship between the user and the data holder (Articles 4 and 5), the relationship between the user and the third party (Article 6) and, finally, the relationship between the data holder and the third party (Articles 8 and 9). All three sets of provisions deal with the rights and obligations of the parties regarding access to and use of the data.[30] Equally, they are all characterised by statutory obligations, which however are closely intertwined with a contractual relationship between the respective parties.

(69) The most surprising element of this approach is the legal regime established by Articles 8 and 9 for the relationship between the data holder and the third party. One could indeed imagine a workable legal design without application

[30] This logic is not respected in Article 5. This provision also contains obligations of the third party vis-à-vis the data holder.

of Chapter III to the relationship between the data holder and third parties. As regards the data portability regime for personal data, Article 20 GDPR does not provide for any direct rights and obligations between the data controller and the 'other data controller'. The reason is that transmission of the data to another data controller under Article 20 GDPR is designed as a right of the data subject. However, the same holds true for the right of the user to request a making available of the data to a third person under Article 5(1) of the Proposal. This provision explicitly allows for another person than the user to make the request. This could even be the selected third-party service provider. However, such other party will only act 'on behalf of the user', which may also be an indication that this right of the user is to be considered a non-transferable right.

(70) The reason why, in contrast to Article 20 GDPR, the Proposal provides for a third legal relationship between the data holder and the third party lies in the decision of the Commission to require the third party to pay a reasonable compensation to the data holder according to Article 9(1) of the Proposal, while the making available of the data to the third party should remain free of charge for the user according to Article 5(1). Such approach is neither convincing from a legal nor an economic perspective.

(71) Legally, such an approach has to produce tensions that cannot be adequately resolved. As regards the relationship of the data holder to the user, the data holder has to provide the data 'without undue delay and free of charge', which immediately raises the question of how to coordinate the fulfilment of this obligation vis-à-vis the user with a potential FRAND conflict between the data holder and the third person. Allowing the data holder to retain the data until the FRAND dispute is resolved would lead to a violation of the obligation of the data holder vis-à-vis the user and seriously affect the effectiveness of the data access and use right of the latter. Conversely, if one considers the data holder under an obligation to provide access despite its failure to agree on FRAND terms, this would create a so-called 'hold-out' situation, where the third party can simply refuse or evade honest FRAND negotiations, as this will not hinder the provision of the service. Even more, one may wonder what the third party has to pay for if the data will anyhow have to be made available to the third party pursuant to Article 5(1). Article 8(1) and (2) is not completely blind to the problem since Article 8(2) explicitly provides that the contract that the two parties are supposed to conclude on FRAND terms must not 'derogate from or vary the effect of the user's rights under Chapter II.' However, this provision only applies to the terms of the contract and, hence, requires that the parties enter into such contract in the first place. For the case that the third party is unwilling to negotiate the contract, Article 8 does not offer any solution to coordinate the FRAND regime with the requirement of Article 5(1) to make the data available to the third party without undue delay and free of charge for the user.

(72) Moreover, the proposal that the third party should pay compensation while the user can claim a making available of the data to the third party free of charge cannot be justified for various reasons: first, Articles 4 and 5 seem to be grounded on the idea that the user can freely choose whether to organise the added value use internally or externally. If, for instance, data access is needed for repairing a manufacturing machine, the industrial user can either delegate the repair to its own maintenance unit (Article 4) or outsource maintenance to an external service provider (Article 5). The reasons why such user chooses to outsource maintenance are unrelated to the question of whether the data holder deserves a compensation or not. Hence, there is no reason to distinguish between the two cases. Secondly, the compensation that the third party has to pay to the data holder will increase the costs of providing the service to the user of the IoT machine. To recoup such costs, the third party will typically attempt to charge the user of the machine a higher price. Accordingly, in a situation where the user outsources the maintenance service, Article 5 creates the risk of undermining the policy decision in Article 4 according to which the user should enjoy the data access and use right free of charge. Furthermore, it varies the effect of the user's rights under Chapter II. It is not justified that a contract term that causes such variation should not be binding according to Article 8(2), while such variation caused by the payment of compensation will be ignored. Thirdly, the Proposal may lead to distortion of competition among commercial users of the same kind of product to the disadvantage of smaller users. Large commercial users will be more likely to organise efficient in-house maintenance units while smaller competitors are more likely to depend on external maintenance services; only the latter will run the risk of being indirectly charged for the data use. Fourthly, this argument applies even more to users who are consumers. They will typically not be able to repair the product themselves. There is no reason why consumers should be discriminated against in comparison to business users who can organise in-house maintenance. Fifthly, and most importantly, the need to negotiate a price and potential disputes about the appropriateness of the compensation increases the transaction costs, may delay data access and use and would ultimately undermine the effectiveness of Article 5. While the former reasons only advocate for the application of identical rules on compensation in the context of both Article 4 and Article 5, this latter reason argues in favour of excluding a right of the data holder to claim a compensation also in the context of Article 5. Finally, one should not overlook the fact that the manufacturer is anyhow able to recoup the cost for making the data available when setting the sales price for the product (see para 84 below). This should also sufficiently compensate the data holder where the data is made available in the context of Article 5. The Institute therefore proposes that the reference made to Article 5 in Articles 8(1) and 12(1) be deleted. As a result, the data holder would not be able to charge a price for the making available of data to a third party in the context of Article 5.

- **Data accessibility by default (Article 3)**

(73) The Institute supports the approach adopted under Article 3 to conceive access to IoT data as being part of the design of IoT products. Making data accessibility a fundamental feature of IoT products promotes the ability of the user to integrate IoT products as part of the connected infrastructure that the user controls, be it a factory, an administration or a household. However, the obligation under Article 3 is not without reservation. Direct accessibility is only required 'where relevant and appropriate'. The recitals do not explain how this proviso has to be understood. Recital 21 only clarifies that 'direct' availability relates to both availability from an on-device data storage and from a remote server. In addition, it is not clear why the proviso is only relating to 'direct' accessibility and not to easy and secure accessibility. If the Commission cannot explain the reasons, the wording 'where relevant and appropriate' should be deleted.

(74) Article 3(1) does not clearly state who the addressee of the provision is. It seems obvious that the obligation to enable data accessibility by design should be an obligation of the manufacturer. Yet this does not answer the question of who can be held liable if the product does not fulfil the requirement under private law. Making accessibility by design a feature of the product design indeed raises the question of how Article 3(1) interacts with contractual liability for defects under the law of sale contracts. In this regard, it is puzzling that neither the provisions nor the recitals of the Data Act mention the EU Sale of Goods Directive.[31] This Directive provides for liability for non-conformity of goods with the sales contract. In this context Article 6(a) of this Directive *inter alia* mentions 'functionality, compatibility, interoperability' as aspects to which conformity may refer. Moreover, Article 7(1)(a) states that, beyond what is agreed in the contract, the good needs to be 'fit for the purposes for which goods of the same type would normally be used', whereby any existing rules of EU and national law are to be taken into account. Therefore, it can easily be argued that the principle of 'data accessibility by default' as established by Article 3(1) of the Proposal would have to be considered when assessing the conformity of the product with the contract in the light of the Sale of Goods Directive. According to Article 10 of this Directive, however, it will be the seller of the device – and not the manufacturer – who is liable for non-conformity of the product vis-à-vis the consumer. According to Article 10(2), this liability also extends to non-conformity of related digital services, which are typically provided directly by the manufacturer to the consumer. The Proposal certainly does not intend to change the rules on contractual liability under the Sale of Goods Directive. Also, the general placement of Article 3 in Chapter II, which also includes

[31] Directive (EU) 2019/771 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the sale of goods, amending Regulation (EU) 2017/2394 and Directive 2009/22/EC, and repealing Directive 1999/44/EC, [2019] OJ L 136/28.

Articles 4 and 5 creating obligations on the part of the data holder, should sufficiently explain that Article 3 stipulates obligations of the manufacturer and not the retailer. Still, the legislature should explicitly mention the manufacturer as the person who has to fulfil the obligation under Article 3. Making this clear is also important so as to identify the manufacturer as the addressee of enforcement measures under Chapter IX. Equally, Article 1(3) should also mention that the Data Act does not affect the application of the Sale of Goods Directive.

(75) As regards the IoT data access and use right of Article 4, this Position Statement has already pleaded in favour of conceptualising the right as a purpose-bound right focusing on the objective of overcoming vendor lock-ins. This requires extending the right to cover derived and inferred data access to such data where this is needed to realise this purpose. This raises the question of whether this concept should also be adopted for Article 3.

(76) The Institute answers this question in the negative. Article 3 pursues very different objectives than Articles 4 and 5. Manufacturers have to implement the principle of data accessibility by default uniformly for all products. This rule can only establish the first level of accessibility of data, which should not extend to derived and inferred data (para 31 above). In contrast, Articles 4 and 5 have the very specific purpose of overcoming vendor lock-ins in individual cases. Accordingly, the Institute is in support of the general design of Article 3, which seeks to establish a general standard of data accessibility for all products.

(77) The Institute also supports the precontractual information obligations laid down in Article 3(2). Yet here as well the provision does not clearly name the addressee of these obligations. Again, it is most likely that the Commission's intention is to only create obligations of the manufacturers of IoT products, who is the only person who will be able to provide that information. However, in many instances, this information will have to go through the hands of many intermediaries before the information can reach the user. This raises the question of whether the manufacturer could also be exposed to sanctions for the failure of commercial customers to pass on said information to downstream users of the product. An alternative approach would consist in limiting the duties imposed on manufacturers to only informing their direct customers and establishing identical duties for all subsequent commercial customers acting as intermediaries in the distribution chain. This would, on the one hand, alleviate the regulatory burden on manufacturers and, on the other hand, increase the likelihood that said information reaches the user. In the case of commercial retailers such duties would complement the Sale of Goods Directive and mutually support the effectiveness of both legal instruments. However, end users who resell IoT products as used products should not be required to provide said information. Nor should the

manufacturer be held responsible if in such case of a resale the information does not reach the subsequent user.

(78) It should be noted that Article 3(2) does not stipulate whether beyond administrative enforcement under Chapter IX a failure to provide the information will also lead to private law sanctions.

- **The IoT data access and use right pursuant to Articles 4 and 5**

(79) As regards Article 4, the relationship with Article 3 is not quite clear. According to its wording, Article 4 would only apply where the data cannot be 'directly accessed by the user from the product'. This seems to cover two distinct situations: First, Article 4 would apply where the manufacturer fails to make the data directly available by default in the sense of Article 3. In this case, private enforcement of Article 4(1) would provide an immediate claim for data access and use where the manufacturer has failed to fulfil the obligation set out in Article 3(1). Secondly, Article 4 also seems to apply to cases where the data is only 'directly accessible' from a remote server, as explained by Recital 21, but not from an on-device data storage (product). In such latter case, Article 4(1) would complement Article 3 by also applying the detailed provisions of Article 4 in this case. Conversely, however, this would mean that neither Article 4 nor Article 5 would apply where the data is made directly available from on-device data storage.

(80) The Institute is of the opinion that such distinction of the scope of application between Articles 3 and 4 does not make sense. Rather, as already indicated above (para 76), the two provisions should be distinguished in functional regards. It is also to be noted that especially Article 5 concerning the right to share data with third parties should also apply where the data can be accessed 'from the product'. In a situation where a user can enable a third party to access the necessary data from on-device data storage without additional involvement of the user, it is still important that the entire provisions of Articles 5 and 6 apply. Accordingly, the Institute recommends changing the wording of Article 4 at the beginning in the sense that the data access and use right applies 'without prejudice to Article 3'.

(81) The Institute also recommends amending the wording of Article 4 to make clear that the user is vested with a non-exclusive right of data access and use against the data holder. The Proposal only mentions the 'right of users to access and use data' in the title of Article 4, while access is addressed in Article 4(1) in the form of an obligation of the data holder and use is only mentioned in Article 4(6) in the form of restrictions imposed on the data holder to use the data. Here, the Proposal's legal design could create the false impression that the Data Act distinguishes between a (non-exclusive) data access right and an (exclusive) data use right. The text of Article 4 should also make clear that this right is non-waivable and non-transferable.

(82) As regards the modalities of data access, Article 4(1) is quite rightly worded in an open manner. Following the purpose-bound approach as argued above, the concrete purpose should define whether the right will also cover access to and use of derived and inferred data and in what way the data should be made available, specifically continuously and in real time.

(83) Effective exercise of the right of Article 4(1) will critically depend on the form in which the data will be made available and whether interoperability will be enabled. In this regard, it has already been explained that the conditions for enabling the accessibility and usability of the data in technical regards need to be improved by additional requirements. This can partially be implemented as part of a definition of the 'making available of data generated by the use of a product or a related service' (see para 63 above).

(84) Article 4(1) provides for a duty to provide the data free of charge. However, additional technical requirements as regards the accessibility and usability of the data beyond *in situ* accessibility will not come without additional costs for the data holder. Still, the Institute supports the obligation to make the data available free of charge. The reasons are threefold: first, the charging of a (potentially excessive) price could prevent data holders from claiming their right of access and use. Secondly, a right to compensation of the data holder would require the extension of the application of the FRAND regime of Chapter III to Article 4. Whether the compensation is fair and reasonable in the sense of Article 8(1) will be fraught with uncertainties and would therefore not rule out strategic behaviour on the part of data holders in the form of claiming excessive compensation (in FRAND cases relating to standard essential patents (SEPs) this is known as 'hold-up'), ultimately leading to disputes that at least delay data access and use. Application of the FRAND regime therefore also conflicts with the obligation of the data holder to provide access without undue delay under Article 4(1). Thirdly, the user will anyhow have to pay a price either directly to the data holder (manufacturer) or indirectly when buying, renting or leasing the product from a third party or paying for a service that is delivered by using the product. Hence, the manufacturer should be able to cover the costs of making the data available under Article 4 by charging a higher price when bringing the product to the market.

(85) In sum, the Institute recommends reformulating Article 4(1) as follows:

> Without prejudice to Article 3, the user shall have a non-waivable and non-transferable right against the data holder to access and use data directly or indirectly generated by the use of the product or related service, including derived and inferred data. This right is limited to data to which access is required to enable added value uses by the user. The data shall be made available, without undue delay, free of charge and, where applicable, continuously and in real time.

(86) In the light of the purpose-bound approach in Article 4(1), it is important that Article 4(2) enables the data holder to verify whether the request is legitimately made by a user in the sense of Article 4(3)

(87) In Article 4(4), the Proposal excludes the use of the data for the purpose of developing a competing product. This identifies the IoT data access and use right as a right that only strives to promote competition with the data holder in downstream (related) markets. Against the backdrop of the recommended wording for Article 4(1), Article 4(4) would only constitute a clarification.

(88) As explained above (para 54), Article 4(6), 1st sentence, should be deleted. The second sentence, in contrast, should be maintained – however, while clarifying that it only applies to non-personal data. This restriction on the data holder to use data relating to the user goes beyond what trade secrets law would provide for, but the provision appears indispensable to protect the legitimate interests of users.

(89) If the EU legislature follows the recommendation of the Institute on amending Article 4(1), Article 5(1) will need to be further coordinated with Article 4. In this regard it would suffice to add a reference to Article 4(1) at the beginning of the proposed text for Article 5(1) reading: 'In addition to the obligation to make the data available to the user, upon request by the user …'

(90) Article 5(2) includes a rule that seeks to exclude gatekeepers in the sense of the proposed Digital Markets Act (DMA) from benefitting from the application of Article 5(1).[32] In the larger context of Article 5, this provision constitutes a limitation of the right of the user to freely choose the third party to which the data should be made available for the provision of added value services. However, Article 5(2) also stipulates prohibitions directly addressing gatekeepers.

(91) The exclusion of gatekeepers may seem justified in the light of the particular challenges the business models of gatekeepers present for maintaining competitive and contestable markets. Since access to large volumes of data is key for the creation of the gatekeepers' digital ecosystems, it is understandable that the Commission proposes their exclusion in Article 5(2).

(92) Yet the Institute also wants to mention a number of arguments against such exclusion that should be considered by the EU legislature. First and foremost, duties of gatekeepers should exclusively be regulated within the system of the DMA. The DMA identifies the Commission as the only authority to enforce the DMA, while the obligations of gatekeepers under Article 5(2)(a) through (c) would be enforced by national authorities as provided by Article 31.

[32] Proposal of 15 December 2020 for a Regulation of the European Parliament and the Council on contestable and fair markets in the digital sector (Digital Markets Act), COM(2020) 842 final.

Second, Article 10 DMA provides for a mechanism for 'updating' the obligations of gatekeepers. Hence, there is a possibility to integrate the gatekeeper obligations of Article 5(2) into the system of the DMA. Third, Article 5(2) may set a precedent for restricting gatekeepers' economic freedom to act in whatever context of future regulation. Fourth, Article 5(2) would considerably restrict the legitimate interest of the users of IoT products to freely choose the third party. Hence, exclusion of gatekeepers would result in being unfair to users by preventing them from receiving a service from gatekeepers, while the DMA seeks to preserve fairness in the interest of undertakings and persons who enter into a service relationship with gatekeepers. Fifth, where gatekeepers have to compete with providers, exclusion of gatekeepers could harm innovation to the disadvantage of consumers and society at large. Sixth, Article 5(2) may even turn out to be counterproductive. The Institute agrees that one should look suspiciously at all activities of gatekeepers by which they draw users within their digital ecosystems and increase their strong market positions by amassing increasing amounts of data. However, if Article 5(2) were enacted, this might incite gatekeepers to expand their business into multiple markets for IoT products, in particular in the form of acquiring manufacturers of IoT products. It should equally be noted that the Proposal does not prohibit data holders from directly sharing aggregated IoT data with gatekeepers.

(93) Following the example of Article 4(6), 2nd sentence, Article 5(5) protects legitimate interests of third parties and should therefore be enacted.

(94) Article 6 comprehensively regulates obligations of the third party. It is therefore recommended that, in line with the proposed amendment to Article 4(1) (para 85), Article 6(1) should clearly set out that the third party may use the data only for the purpose of providing added value services to the user. If the legislature decided to follow this recommendation, lit (d) and (e) could be deleted.

(95) In contrast, it is important to maintain Article 6(2)(c) and (f). Article 6(2)(c) in its proposed version is fully in line with the purpose-bound approach and therefore indispensable. Article 6(2)(f) would guarantee that the third party will not be able to tie additional secondary services to its service.

(96) The Institute is inclined to recommend deleting Article 7. This provision seeks to exclude micro and small enterprises from the scope of Chapter II. Here, the Commission seems to overlook the fact that Chapter II is not just a form of industry regulation. Rather, it provides for rules that are intrinsically embedded in contract and consumer law. If one accepts the view that accessibility of data by default should be regarded as an objective element of the conformity of IoT products in the sense of the Sale of Goods Directive (para 74 above), the exclusion of micro and small enterprises would not be justified. In addition, one should expect that competition would anyhow force

micro and small enterprises to provide users with the same degree of data access and use as their larger competitors are obliged to do. At least, Article 7 should not be enacted without an obligation of micro and small manufacturers to inform users that Chapter II does not apply to them. Otherwise, they would mislead users about the functionalities of the products and rights that can legitimately be expected. In addition, the legislature has to be aware that at a given time an enterprise may no longer qualify as a micro or small enterprise. For such cases, it should be clarified that Chapter II should not apply retroactively to products that a manufacturer has sold or otherwise made available to a user before the manufacturer lost its status as a micro or small enterprise.

III. Obligations of data holders under a legal obligation to make data available (Chapter III)

(97) Chapter III complements all EU and national legal instruments with an obligation of data holders to make data available. The Institute fully appreciates the creation of such horizontal rules. As regards the scope of application, the question is whether the rules of Chapter III are suitable for existing data access regimes. Article 12(3) takes sufficient care of this problem by limiting the application of Chapter III to only those EU and national legal instruments that enter into force after the date of application of the Data Act. With respect to prior EU legislation Recital 87 points out that Chapter III may still be used as a template for future amendments to existing rules.

(98) According to Article 12(1), Chapter III applies to Article 5 but not to Articles 3 and 4. The reason for this is to make Article 9 on compensation applicable in the context of Article 5. Recital 31 explicitly confirms that the data holder can claim reasonable compensation from the third party in the context of Article 5,[33] while under Article 4(1) the user of an IoT product shall be able to access and use the data free of charge. Above, the Institute has already argued that application of Chapter III to Article 5 should be excluded (paras 69-72).

(99) In Article 8(1) the Proposal provides for a system of FRAND licensing of data access and data use. Such a system is not without precedent in European legislation.[34] Here, the Commission has most likely taken inspiration from

[33] See also the Impact Assessment Report, pp 33 and 154.

[34] See, for instance, Regulation (EC) No 1907/2006 of the European Parliament and of the Council of 18 December 2006 concerning the Registration, Evaluation, Authorisation and Restriction of Chemicals (REACH), establishing a European Chemicals Agency, amending Directive 1999/45/EC and repealing Council Regulation (EEC) No 793/93 and Commission Regulation (EC) No 1488/94 as well as Council Directive 76/769/EEC and Commission Directives 91/155/EEC,

FRAND licensing of standard essential patents (SEPs).[35] FRAND is however a rather vague concept, especially as regards the appropriate royalty rate. Its advantage is that it allows for taking account of the specificities of the individual case. Such flexibility however does not dispense the law enforcers and the courts from developing general principles for assessing FRAND terms. Otherwise, FRAND would not be any more concrete than the general principle of freedom of contract. Indeed, the role of FRAND is to narrow down the range of acceptable solutions.

(100) With Article 8 of the Proposal, the EU legislature would adopt a FRAND system at the interface of statutory law and contract law, while in the case of licensing of SEPs, the basis for FRAND is contractual. In that latter field, standard development organisations (SDOs) as private organisations require the holders of SEPs to commit to FRAND licensing. Under the applicable national law, such commitment may be considered a (pre-)contract between the SEP holder and the SDO with the implementer of the patent as a third-party beneficiary. As regards EU law, only competition law seems to provide a means to limit the availability of intellectual property remedies, especially injunctions, in case the parties turn out to be unable to agree on a licensing agreement.[36] In the context of Article 8 the baseline is a different one. Article 8 makes use of the FRAND concept as part of the statutory text. More specifically, it only defines an obligation of the data holder.

(101) Against this backdrop, the concept seems to be that if a data holder is not willing to make the data available on FRAND terms, law enforcers, including the national authority in the sense of Article 31 of the Proposal, should be able to intervene and enforce the FRAND obligation. However, when it comes to

93/67/EEC, 93/105/EC and 2000/21/EC, [2006] OJ L 396/1. Articles 27 and 30 REACH Regulation implement a scheme for information sharing that pursues the particular objective of avoiding animal testing. More concretely, the potential registrant of a potentially hazardous chemical substance is under an obligation to request a sharing of information from previous registrants as holders of studies, whether these studies include tests with vertebrate animals or not. Thereby, the Regulation takes into account the interest of the previous registrant in fair compensation for the testing it has already undertaken. For that latter purpose, the owner of the existing study has to determine the costs of sharing the information in a 'fair, transparent and non-discriminatory way' (Arts 27(3) and 30(1)(2) REACH Regulation). On whether such system can be fruitfully used for modern data access and use regimes see Josef Drexl, 'Designing Competitive Markets for Industrial Data – Between Propertisation and Access' (2017) JIPITEC 257, paras 176-180.

35 The IP policies of many Standard Development Organisations (SDOs), such as the European Telecommunications Standards Institute (ETSI), often require holders of standard essential patents to commit to license their patents on 'fair, reasonable and non-discriminatory' (FRAND) terms. The need to require such FRAND commitment is included as a principle in the Commission's Horizontal Cooperation Guidelines as a means to 'ensure effective access to the standard'. See Communication from the Commission – Guidelines on the applicability of Article 101 of the Treaty on the Functioning of the European Union to horizontal co-operation agreements, [2011] C 11/1, para 285.

36 See Case C-170/13 *Huawei Technologies* ECLI:EU:C:2015:477.

deciding whether the claimed compensation in the sense of Articles 8(1) and 9(1) is reasonable, the authority will hardly be able to set any concrete standard beyond what is laid down in Article 9(2) through (4). In the field of SEP licensing, the FRAND concept has led to endless discussions and disputes on the appropriate royalty rate around the globe. In the field of data licensing under Articles 8 and 9, the potential for disputes can be expected to be incommensurably higher since the variety of cases of data access, the informational value of the data and the intended uses are unlimited, while SEP licensing almost exclusively concentrates on the licensing of telecommunications standards.[37] Hence, the test of reasonableness for assessing the appropriate level of compensation can hardly be expected to provide a useful standard, neither for administrative authorities nor private law courts. This explains why the Proposal seeks a procedural solution by relying on specialised dispute settlement bodies in Article 10.

(102) In the field of SEP licensing, the key function of FRAND may well consist in providing a framework for negotiation (FRAND as a process) that helps parties to finally agree on a fair royalty rate for the use of SEPs. Recital 39 of the Proposal seems to adhere to a similar idea by stating that parties should remain free to agree to negotiate the precise conditions. The same idea characterises the *Huawei* judgment of the CJEU concerning SEP licensing, in which the Court defined a list of procedural rules and mutual obligations of the parties for negotiating FRAND terms, while remaining silent on the substantive standards for FRAND.[38] However, these procedural rules for SEP licensing cannot easily be transferred to data licensing. In the field of SEPs, quite rightly, the CJEU did not take the side of one of the two parties. Rather, it sought to balance the risk of hold-up by the SEP holder (seeking an injunction so as to extract an excessive royalty rate) with the risk of hold-out (also 'reverse hold-up') by the implementer (seeking to implement the standardised technology without being willing to negotiate a price). SEP cases and data access cases differ as regards the position of both parties. Since the technical standard specification is publicly available, device manufacturers can implement the technology standard without seeking a licence first. Data holders, in contrast, can keep back the data. This creates a risk of hold-up exercised by the data holder, while there is no risk of hold-out based on the conduct of the data recipient. This indeed explains the formulation of a FRAND obligation of data holders in Article 8(1) of the Proposal.

[37] On the application of FRAND in Article 8 of the Proposal see already Peter G Picht, 'Caught in the Acts: Framing Mandatory Data Access Transactions under the Data Act, further EU Digital Regulation Acts, and Competition Law', Max Planck Institute for Innovation and Competition Research Paper Series No 22-05, available at <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4076842>.

[38] Case C-170/13 *Huawei Technologies* ECLI:EU:C:2015:4, paras 55-68.

(103) Still, the approach of Article 8(1), (2) and (3) to only formulate unilateral obligations of the data holder is not unproblematic since the different prongs of FRAND require a balancing of the interests of both parties, and also the data recipient should be considered under an obligation to negotiate with good faith and agree on FRAND terms. Nor can it be ruled out that the data recipient may dispose of superior bargaining power when negotiating the contract required pursuant to Article 8(2) and be able to negotiate a privilege that is not FRAND compliant. Therefore, the EU legislature is advised to formulate the FRAND concept in Article 8 as mutual obligations of both parties. This would call upon the competent authority in the sense of Article 31, private law courts and the dispute settlement bodies of Article 10 to enforce the FRAND concept also against the data recipient where this is needed. In contrast, imposing the burden of proof on the data holder in Article 8(3), 2nd sentence, can be considered appropriate. Here, the proposal reacts to an information asymmetry. The data recipient typically has no information about terms the data holder agreed upon as regards other data recipients.

(104) Non-exclusivity as provided for by Article 8(4) seems an appropriate default rule for data sharing since use of the same data by more persons will typically enhance welfare. On the other hand, where data recipients require exclusivity, they may strive to exclude competitors. Yet Article 8(4) should equally use a balanced wording, not only in terms of a prohibition addressed at the data holder but also a prohibition imposed on the data recipient from claiming an exclusive licence. The reservation made in Article 8(4) with regard to Chapter II should be deleted even if the EU legislature decided to follow the Proposal as regards the application of Article 8 in the context of Article 5. Similar to Article 4(6), 1st sentence, this reservation presumes an exclusive right of the user of the IoT product to decide on who is allowed to use the data. Since the Commission explicitly seeks to avoid an exclusive data access and use right, the data holder should be free to license the data to any other party.

(105) As regards Article 8(5), it is not clear who the recipient of the information will be, whether this is about mutual obligations of the parties to inform each other or whether this is about information to be delivered in the context of administrative enforcement or court proceedings. In the context of Article 8, the more likely function is the former, so as to bring further precision to the understanding of FRAND terms. Hence, this should be clarified by including the words 'to each other' to read: '…shall not be required to provide any information *to each other* …'.

(106) The Institute recommends deleting Article 8(6), which would invite data holders to strategically claim trade secrets protection to avoid the sharing of data (see in more detail para 284 below).

(107) The rules on calculating compensation in Article 9 seem largely acceptable. This is especially true for Article 9(3), which creates the necessary flexibility

for legislation and will protect existing national rules, as well as Article 9(4). The latter provision, stipulating an obligation of the data holder to provide information on the basis for the calculation, allows the data recipient to make a judgment on the fairness of the calculation.

(108) The Institute agrees that dispute settlement bodies as provided for in Article 10 are best equipped to solve conflicts between data holders and data recipients. However, Article 10(1) defines the scope of jurisdiction extremely narrowly, only empowering these bodies to determine FRAND terms for the given case. Disputes between the parties may also regard other aspects of the data access regime. Article 10 should avoid such carving-out of only some aspects of a broader conflict. Since parties have an interest in having their entire dispute decided by a single body, the proposed limited jurisdiction could considerably reduce the attractiveness of the dispute resolution before the new dispute settlement bodies. Accordingly, the legislature is recommended to extend jurisdiction of these bodies to the entire conflict of the parties.

(109) As Recital 48 explains, the dispute settlement bodies of Article 10 are proposed as an alternative venue to state courts for solving conflicts between the parties. Jurisdiction of state courts is indirectly confirmed in the *lis pendens* rule of Article 10(5). This provision also addresses the relationship to other dispute settlement bodies, and seems to refer to arbitration tribunals in particular. The application of the *lis pendens* rule as regards those other courts and bodies appears especially appropriate so long as the new dispute settlement bodies under Article 10 have not proven to be the better venue.

(110) Conversely, however, Article 10(5) is not clear as regards the opposite situation where the body first seised is a dispute settlement body in the sense of Article 10. At least Recital 50 clarifies that jurisdiction of the bodies under Article 10 does not deprive parties of the possibility to bring a claim before the competent tribunals and courts of the Member States. Accordingly, the *lis pendens* rule does not seem to exclude jurisdiction of a later seised state court. Yet this does not have to mean that parties cannot prorogate the jurisdiction of state courts in favour of bodies in the sense of Article 10. The latter may well make sense once the new bodies have proven to be better qualified and quicker venues for dispute resolution than state courts.

(111) Neither Article 10 nor the recitals explicitly address the issue of international jurisdiction, although Recital 48 specifically points out that the dispute settlement bodies could also help solve cross-border disputes. Referring to the *lis pendens* rule of Article 10(5), Recital 49 at least shows awareness of jurisdictional conflicts. However, in contrast to what Recital 49 argues, this *lis pendens* rule does not adequately solve conflicts between dispute settlement bodies established in different states. If Article 10 allowed a party to freely choose among the certified bodies across the EU, this provision

would open the door to unlimited forum shopping. In addition, in cross-border conflicts, a party will typically prefer to bring the dispute to the body in the country of its domicile. This however would conflict with the justice principles underlying Article 4(1) Brussels Ibis Regulation, according to which another party can in principle only be sued in the courts of the Member States of the other party's (the defendant's) domicile.[39] Application of the rules of the Brussels Regulation for delineating the jurisdiction of the dispute settlement bodies should be considered the more appropriate approach. However, direct applicability of the Regulation is by far not clear. Article 1(1) defines the Regulation's scope of application very broadly as encompassing 'civil and commercial law matters whatever the nature of the court or tribunal'. On the one hand, Article 10 certainly allocates an adjudication function to these bodies. On the other hand, however, Article 10 does not order the Member States to create such bodies as state entities. Rather, it seems that it is expected that those bodies will be established on private initiative. According to Article 10(2), these bodies' adjudication function will only be recognised based on certification by the respective Member State. Certification will only occur upon request by such body and if the body is able to demonstrate that it fulfils the conditions listed in this provision. In sum, these bodies seem to be placed between state courts and arbitration tribunals. They can be seised just like state courts for the purpose of adjudicating cases without the consent of the defendant. On the other hand, they remain private bodies, a feature they share with arbitration tribunals. Pursuant to its Article 1(2)(b), the Brussels Ibis Regulation does not apply to arbitration. Indeed, established and permanent arbitration tribunals, such as at certain chambers of commerce, are most likely to seek certification pursuant to Article 10.

(112) Delineation of international jurisdiction is further complicated by the fact that the certification system of Article 10(2) does not guarantee that such bodies will exist in all Member States.[40] Most likely these bodies will at best only be established and certified over time. One could of course consider applying the Brussels Ibis Regulation *mutatis mutandis*. However, how should this work if no such body is certified in the Member State of the defendant's domicile? In such case, the purpose of safeguarding the legitimate interests of a potential defendant in not being sued abroad argues against setting aside the principles of the Brussels Ibis Regulation. This would mean that a dispute settlement body should only be able to claim jurisdiction if it has jurisdiction according to the rules of the Brussels Regulation. Where this leads to a situation where no dispute settlement body exists in the respective Member State designated

[39] Art 4(1) Regulation (EU) No 1215/2012 of the European Parliament and of the Council of 12 December 2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters, [2012] OJ L 351/1.

[40] However, Article 10(2) does not prevent Member States from taking on an active role in the creation of such bodies.

by the Regulation, the case can only be brought before the private law courts of this Member State.

(113) The Institute would like to furthermore express its concerns about the privatisation of adjudication under Article 10(2). The requirement in Article 10(2)(b) that a body have the necessary expertise in relation to FRAND determination concerning the making available of data has to be considered insufficient. The problem lies not only in the vagueness of this requirement, which in itself would undermine a uniform standard of expertise across the EU. More importantly, it has to be expected that said expertise will probably not be available anywhere in the EU. Sufficient case-law on FRAND determination from state courts as a standard for expertise does not exist, especially considering that Chapter III will only apply to newly introduced data access regimes. Nor would judgments on the determination of FRAND concerning standard essential patents be sufficient to provide guidance for data-related cases. Furthermore, it will be hard to find members for such bodies who have particular experience in FRAND determination regarding data access. Apart from these concerns, Article 10 does not provide any standard for the professional qualification and selection of the members of these bodies. It is telling that the recitals do not elaborate on the reasons why the Commission chose the certification system and that Article 10 leaves key issues regarding the constitution of such bodies open. This shows that the discussion on the establishment of these bodies has not matured enough for implementing Article 10 as proposed by the Commission.

(114) Another blind spot in Article 10 is enforceability: It does not suffice that Article 10 recognises adjudication power of the dispute settlement bodies. No party will bring complaints to these bodies if the decisions are not enforceable by state courts. Since Article 10 is not clear as to whether these bodies qualify as courts, arbitration tribunals or even another *sui generis* dispute settlement body, it will not be clear pursuant to the applicable rules of international procedural law whether and under which conditions state courts will have to enforce dispute settlement decisions. Hence, Article 10 should at least clarify that the decisions of these bodies shall be enforceable by state courts under the same conditions as arbitration awards.[41]

[41] Typically, this would allow the losing party to request a review by the state court if the award is contrary to the public policy. Whether the fact that such bodies in the sense of Article 10 of the Proposal apply EU law suffices to justify such a review is however doubtful. The CJEU requires such a review in particular where the application of EU competition law is at stake. The CJEU explains this by two cumulative reasons, first, the fact that arbitration tribunals do not qualify as courts or tribunals of the Member States that could refer questions on the interpretation of EU law to the CJEU pursuant to Art 266 TFEU (the same may be argued for bodies in the sense of Article 10 of the Proposal) and, secondly, the central role of competition law in EU law and, in particular, for the functioning of the internal market. In this regard, the CJEU has also hinted at the fact that anticompetitive agreements are void pursuant to Article 101(2) TFEU. See Case C-126/97 *Eco*

(115) In sum, Chapter III has to be considered the Achilles' heel of the proposed Data Act. In cases where data access free of charge is not appropriate in the light of the interests involved, the reasonableness standard of Article 9(1) for assessing the royalty rate is too general to allow for legal certainty and expeditious litigation and adjudication. In a horizontal legal instrument such as the Data Act, where such rules are designed to apply to a multitude of data access regimes, application of the FRAND standard is probably unavoidable. However, this may well mean that the legislature should in the future focus on devising precise standards for the calculation of the compensation for data access in the framework of the legal instruments regulating the individual data access regimes. Chapter III is neither a model for such regimes nor will its effectiveness prove to be superior to the adoption of more focused rules applicable to the specific data access regimes.

(116) Article 11(1) confirms that the data holder can make use of technical protection measures (TPMs), which are an additional means to enable and safeguard *de facto* data control. This is not inappropriate. While it may seem that such control runs counter to the public interest in making data broadly available, *de facto* control allows the data holder to charge a price for the sharing of data which, in turn, can be used for improving the quality of data, which includes in particular their veracity, completeness and technical accessibility and usability. Those incentives for quality data also apply in circumstances where the data holder is under a statutory obligation to make data available.

(117) If the legislature followed the recommendation to delete the application of Chapter III in the context of Article 5 (paras 69-72), it would be possible to also delete the second sentence of Article 11(1). This provision confirms the problem that the FRAND system cannot be applied as sought in general under Chapter III in the case of Article 5, which provides for a right of the user to request a making available of the data to a third party.

(118) Article 11(1) seems in general appropriate. There is still a problem in situations where the application of TPMs is protected against circumvention in cases where TPMs seek to protect against the infringement of copyright law. Such protection is required both pursuant to the Information Society

Swiss China Time ECLI:EU:C:1999:269. Against the backdrop of these requirements, FRAND determination under Article 8(1) of the Proposal should be distinguished from the application of EU competition law. FRAND determination primarily regards the private interests of the parties. Moreover, Article 8 does not restrict the freedom of the parties to agree on terms that are not FRAND. This argues against the right of the losing party to request a review of decisions of bodies under Article 10 to deny enforcement.

(InfoSoc) Directive[42] and the Computer Programs Directive.[43] This raises the more profound question of how data access regimes are to be coordinated with intellectual property. As regards Article 11(1), one could at least argue that, if this provision allows for the application of TPMs in general, this should even more be permitted in case of protecting copyright-protected data. However, protection against circumvention, which may be sanctioned under criminal law in the Member States, could potentially restrict measures to establish interoperability with the datasets of data holders. In the context of Article 11 it would not be appropriate that, if a data holder does not fulfil its obligations under a statutory data access regime, a person entitled to data access who manages to establish interoperability with the relevant data by circumvention of TPMs will be held liable under the copyright regime for TPMs. This would argue for adding another sentence to Article 11(1) that clarifies that 'such technical protection measures should not be used as a means to prevent interoperability of the data which the data holder is under an obligation to make available'.

IV. Control of unfair contract terms between enterprises (Chapter IV)

(119) For many years, the Commission has promoted a debate on whether there should be rules to control the fairness of business-to-business (B2B) data-sharing contracts.[44] The fact that it has now decided to propose such rules in Chapter IV shows that it considers the development of model contract rules, which is still mentioned in Article 34, an insufficient alternative. The scope of application of Chapter IV differs from that of Chapter III. While Article 8(2) declares Article 13 (Chapter IV) also applicable to the terms of the contract that the parties conclude in the framework of statutory data access regimes, Article 13 also applies in cases of voluntary data sharing.

(120) European law on the control of not individually negotiated contract terms is so far limited to business-to-consumer (B2C) contracts.[45] While some national laws also apply the same rules to control the fairness of B2B contracts, the decision of the Commission to propose such application now under EU law is a paradigm shift in EU contract law. This may explain why the Commission proposes a less interventionist regime than exists for consumer contracts, raising the likelihood that a sufficient number of Member States will support

[42] Art 6 Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society, [2001] OJ L 167/10.

[43] Article 7(1)(c) Directive 2009/24/EC of the European Parliament and of the Council of 23 April 2009 on the legal protection of computer programs (Codified version), [2009] OJ L 111/16.

[44] See Commission Communication – Building a European Data Economy (n 24) p 12.

[45] Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts, [1993] OJ L 25/29. Recently amended by Directive (EU) 2019/2161.

Chapter IV. The Institute is in general in support of fairness control of B2B contracts in this context, since it cannot be denied that B2B relationships can be affected by unequal distribution of bargaining power where, for the purpose of conducting its business, one party crucially depends on access to data controlled by another party.

(121) In Article 13(1), the Data Act uses two cumulative requirements for identifying clauses to which the control mechanism should apply. Thereby, the Proposal follows the conceptual nature of the approach of the Unfair Contract Terms Directive for B2C contracts[46] but differs as regards the concrete requirements.

(122) First, the provision requires that the specific clauses be 'unilaterally imposed' by one party to the contract. The Unfair Contract Terms Directive, in contrast, uses the different term of 'not individually negotiated'. This difference in wording is not coincidental. Article 13(5) sets the benchmark for intervention higher by additionally requiring that the other party not have been able to influence the terms of the contract 'despite an attempt to negotiate it'.[47] This means that, in a case where the other party simply accepts the contract without showing any resistance, it will not benefit from Article 13. In contrast, Article 3(2) Unfair Contract Terms Directive would apply.

(123) The Institute considers this higher threshold inappropriate. In particular, contract clauses used by digital marketplaces for data sharing where a petitioner of data access only has the possibility to click an accept button without being able to 'attempt to negotiate' would fall outside the scope of control of Article 13. Moreover, the additional requirement of an attempt to negotiate would force parties to negotiate 'strategically' to safeguard protection under Article 13. This would turn the attempt to negotiate into a formality. The practical effect of the requirement would run counter to the objectives of Article 13, since the legally less well-informed businesses, which are particularly in need of and deserve protection, are more likely to overlook the need to make an attempt to negotiate the contract.

(124) Therefore, the Institute recommends replacing the words 'which have been unilaterally imposed' in Article 13(1) by 'which have not been individually negotiated', the standard used in the Unfair Contract Terms Directive. This would also be in line with national laws that already allow for fairness control of B2B contract terms following the example of this Directive without requiring any attempt to negotiate the contract.[48] Article 13(5) should be

[46] Ibid.

[47] The same requirement is mentioned by Recital 52. It is therefore puzzling that these last words do not appear in the Impact Assessment Report, p 156. There, the standard seems to be that the other party could not influence the terms of the contract.

[48] German law does so with regard to standard contract terms. See Section 305(1) German Civil Code. It is only in B2C contracts that German law accepts the rule of the Directive that non-

reformulated accordingly. More specifically, it should adopt the wording of Article 3(1), sub-paragraphs (1) and (2), of the Unfair Contract Terms Directive.

(125) The second requirement of Article 13(1) restricts the scope of application to the protection of micro, small or medium-sized enterprises. This limitation may be inspired by the belief that, following the example of the Unfair Contract Terms Directive, also for B2B cases an additional personal element restricting the scope of application should be required. However, such logic is not convincing. Whether a contract is influenced by an imbalance of bargaining power or not is not a matter of the size of the undertaking but – in the specific case of data-sharing contracts – of the degree of data dependence. In the data economy, a relatively small company may control very valuable data on which even large companies crucially depend for doing business. In such a case, even small companies may hold superior bargaining power over other market players. This insight played a critical role when the German Act against Restraints of Competition was reformed in 2021 with a view to strengthen its effectiveness in the digital era.[49] On this occasion, the rules on 'relative market power' in Section 20(1), which make downstream or upstream market foreclosure a violation of German competition law. were also amended. By requiring significant imbalance between the power of the parties involved ('relative market power'), German law addresses typical cases of unequal distribution of bargaining power, which Article 13 of the Proposal now also seeks to regulate. The German reform of 2021 consisted in two things. First, the reform – in a new Section 20(1a) – clarified that such significant imbalance of market power can also exist in a case of dependence on access to data held by another company. Secondly, and more importantly for the future design of Article 13 of the Data Act, the German legislature abolished the former requirement in Section 20(1) according to which only small and medium-sized undertakings benefitted from the application of the rule. Hereby, the legislature explicitly reacted to the – empirically based – insight that economic dependence does not need to require, even less in the data economy, a difference in size of the parties involved.[50] Thus, it can equally be concluded that the limitation of Article 13 of the Proposal to only protect micro, small and medium-sized enterprises does not correspond to the current state of research in the field. The EU legislature should therefore delete this limitation.

---

negotiated contract terms that are only used once suffice as a subject of control. See Section 310(2) No 2 German Civil Code.

49 10th Amendment Act of 18 January 2021 (n 23).

50 See the Explanatory Memorandum of the government bill of 19 October 2020: Regierungsentwurf der Bundesregierung. Entwurf eines Gesetzes zur Änderung des Gesetzes gegen Wettbewerbsbeschränkungen für ein fokussiertes, proaktives und digitales Wettbewerbsrecht 4.0 und anderer wettbewerbsrechtlicher Bestimmungen (GWB-Digitalisierungsgesetz), Bundestagsdrucksache 19/23492, 78-79.

(126) In addition, the limitation of the scope of Article 13 to agreements among 'enterprises' is not without doubt. This limitation may be influenced by Recommendation 2003/361/EC and the limitation of the protection to 'micro, small and medium-sized enterprises'.[51] Article 1 of Annex 1 of this Recommendation defines 'enterprises' in line with the understanding of undertakings in the sense of competition law. However, in the context of Chapter IV, the Data Act is not specifically regulating competition law. This limitation would leave many entities, including private and non-profit associations as well as state bodies that depend on data access to act in the public interest, without protection. Therefore, the Institute proposes that the scope of Article 13 should be extended to protect 'any legal or natural person except consumers in the sense of Article 2(b) Council Directive 93/13/EEC'. This scope of personal application will guarantee application of Article 13 whenever the Unfair Contract Terms Directive does not apply because the other party is not a consumer. Conversely, however, the scope of application can, as proposed, be limited to enterprises as regards the party that introduces the contract terms into the agreement.

(127) Furthermore, it may not be entirely clear whether Article 13 only protects data recipients or whether it would also apply in the interest of data holders. Article 13(1) explicitly mentions the application of the rules to 'remedies for the breach or the termination of data related obligations', which may be taken as an indication that the provision only protects data recipients. Likewise, the clauses listed in Article 13(3) and (4) are more likely to be relied upon by data recipients. However, the entire Article 13 is formulated neutrally by referring to 'parties'. Similarly, a term 'concerning the access to and use of data' or a term concerning 'the liability and remedies for the breach or termination of data related obligations' can deviate from the fairness standard of Article 13(2) in different directions, hence also to the disadvantage of data holders. Accordingly, Article 13 should be considered to protect both data recipients and data holders. This could however be made clearer in the recitals of the Act.

(128) Another problem regards the applicability of Article 13 in the context of statutory data access regimes under Chapter II. The reference made to Article 13 in Article 8(2) is unclear as to what is meant by the 'conditions' of Article 13. This could either include the general requirements of the applicability of Article 13 or only refer to the fairness standard of control in Article 13(2), (3) and (4). The legislature should clarify this issue in the text of Article 8(2). On substance, there are good arguments to apply the fairness standard of Article 13(2), (3) and (4) to all cases without requiring fulfilment of the conditions set out in Article 13(1). The data holder is typically in a stronger position than the other party. In addition, Article 8(2) should be understood as importing

[51] Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises, [2003] OJ L 124/36.

the standards of Article 13(2), (3) and (4) as part of binding FRAND standards whose application should not depend on whether the terms were individually negotiated or not and who the other party is. Accordingly, based on Article 8(2), dispute settlement bodies in the sense of Article 10 should be allowed to consider Article 13(2), (3) and (4) as binding FRAND requirements. As regards the personal scope of protection, Article 13(2), (3) and (4) would also apply where the recipient under the relevant data access regime is a consumer.

(129) In the latter regard, the Institute wishes to express its concerns that Article 13 only attempts to modernise European contract law in the light of the needs of the data economy only for B2B relations, while the standard of control in the Unfair Contract Terms Directive of 1993 remains unchanged as regards B2C contracts. There is no reason to believe that Article 13(3) and (4) is not appropriate to be applied to B2C contracts as well. The recitals do not explain why consumers should be excluded from protection. The explanation is probably historical. Article 13 has emerged out of a discussion on the legal tools to promote the sharing of non-personal data in a more industrial context. However, this underlines even more how urgent it is to also modernise the Unfair Contract Terms Directive. If this cannot be done now in the framework of adopting the Data Act, the Commission should quickly start work on proposing a revision of the Unfair Contract Terms Directive.

(130) As regards the standards of control in Article 13, only the criteria in Paragraph 4(c) and (d) are specific for data-sharing contracts. This is obviously due to the fact that there are no default rules on data sharing contracts in place that could serve as a benchmark for control. Still, in the Communication of 2019 the Commission considered introducing such rules.[52] While adoption of such default rules would considerably enhance the effectiveness of Chapter IV, inclusion of such rules in the Proposal would probably have considerably delayed legislation. It should however be noted that courts may also use model contract laws as a source of inspiration when applying the general control standard of Article 13(2). Work on such rules is going on in different fora. In particular, the Principles for a Data Economy jointly proposed by the American Law Institute and the European Law Institute should be mentioned in this regard.[53]

(131) Equally, the Institute welcomes the fact that the Commission paves the way for the development of model contract laws under Article 34. The Institute recommends shifting this provision to Chapter IV to make clear that such model rules could be used as a standard of fairness under this Chapter. The accompanying Recital (currently Recital 83) should explicitly mention that

[52] Commission Communication – Building a European Data Economy (n 24) p 12.

[53] ALI-ELI Principles for a Data Economy (n 17). The rules on contracts on supply and sharing of data can be found in Part II Chapter B of the Principles.

such model rules could also be taken account of for the assessment of the fairness of the contract terms under Chapter IV.

V. Business-to-government (B2G) data sharing (Chapter V)

(132) The Institute welcomes the introduction and harmonisation of rules on business-to-government (B2G) data sharing as provided in Chapter V. It agrees with the conclusion that the progress in these areas appears rather slow and diverse.[54] However, the Commission's proposal needs additional thought, public discussion and improvement. In the following it is suggested that the Data Act should more clearly delineate the scope of B2G data sharing, which in turn determines pre-emption of national legislation in this area, by strictly limiting it to situations of *ad hoc* data access. Moreover, the proposal falls short of its goals of integrating the existing legal regimes for public sector information (Data Governance Act[55] and OD PSI Directive[56]) and coherently accounting for private rights and interests. Ultimately, the effectiveness of the proposed procedure appears questionable, especially with regard to public emergencies.

(133) There is no justification for Article 14(2) to exclude small and micro enterprises from the scope of the Regulation. Public interest must prevail in case of an exceptional need for data, while undue burdens for such entities (Recital 56) can be mitigated by providing due compensation. Therefore, the exclusion of micro and small enterprises according to Article 14(2) should be eliminated.

(134) It is a political choice under which circumstances data holders can be obliged to make data available to public sector bodies (PSB). The Data Act introduces a *horizontal* regime, as the reference point for providing access is not related to specific data or sectoral purposes, but to the *circumstances* under which PSBs should be entitled to request data from private data holders. Within this horizontal legal framework, there is ample room for further improvement and specification.

---

[54] See Heiko Richter, The law and policy of government access to private sector data ('B2G data sharing'), in German Ministry of Justice and Consumer Protection and Max Planck Institute for Innovation and Competition (eds), Data Access, Consumer Interests and Public Welfare (Nomos: Baden-Baden 2021) 529, 537–539.

[55] Proposal of the Commission of 25 November 2020 for a Regulation of the Parliament and the Council on European Data Governance (Data Governance Act), COM(2020) 767 final.

[56] Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information, [2019] OJ L 172/56.

(135) The legal basis in the context of public emergency according to Article 15(a) and (b) appears straightforward.[57] In contrast, Article 15(c) is ambiguous and needs further consideration. It provides a general legal basis for data access requests beyond public emergency and follows different reasoning. Still, Article 15(c) is equally based on the idea of the 'exceptional need to use data',[58] so that the interpretation of this notion is decisive for the application of Chapter V.[59] In particular, Article 15(c) requires that the lack of available data prevents the PSB from fulfilling its tasks.[60] It remains unclear how strictly this criterion is to be understood, not least because Recital 58 speaks of '[preventing] it from *effectively* fulfilling a specific task'.[61] Should it be necessary that data access would enable the PSB to fulfil the public task, or should it be sufficient that data access would just improve the effectiveness of fulfilling the public task? Indeed, 'prevents' in Article 15(c) should be interpreted strictly. Otherwise, the provisions of Chapter V could hinder future data access legislation that would improve the effectiveness of fulfilling the public task, especially when considering potential pre-emption of national legislation (see paras 141-146 below). This view is supported by the Impact Assessment Report, which regards it as characteristic of the exceptional data need that the need for data cannot be easily foreseen in advance and use of the data is a necessary condition for a PSB to fulfil its statutory task.[62] Therefore, the additional requirements of Article 15(c)(1) and (2) have to be interpreted in this light. To eliminate doubts, the EU legislature should delete the word 'effectively' from Recital 58.

(136) Article 15(c)(1) requires that the PSB be unable to obtain such data by alternative means.[63] According to this subsidiarity, mandatory access is a means of last resort in non-emergency cases. As a matter of principle PSBs have to make an attempt to get the data by other means first. In detail, however, it remains unclear what efforts PSBs have to make. The general threshold appears high, but not too high, as the Impact Assessment Report states 'difficulties must be justified by objective reasons that make it impossible or very difficult to buy data on the market'.[64] In this light, all alternative means of getting the data as listed in Article 15(c)(1) have to be considered:

(137) 'Purchasing the data on the market at market rates' implies that the data is actually offered to the public. At the same time, the PSB should be required to have taken reasonable efforts to enquire into the market. This should be

57 See also Art 2(10) as well as the definition mentioned in the Impact Assessment Report, p 158.
58 See also Impact Assessment Report, p 158.
59 Ibid.
60 See also Impact Assessment Report, p 34.
61 Emphasis added.
62 Impact Assessment Report, p 13.
63 Ibid, p 34.
64 Ibid, p 158.

clarified in Recital 58. It should not, however, be required to individually negotiate with potential data providers if they have not offered the needed data before. If the data is available for purchase, the question remains how to determine the 'market rate'. Often a given dataset will constitute the only access point to the required information, which would mean the required data is single-source and therefore prone to monopoly pricing. To determine whether the price matches market rates, Recital 58 should declare the cost-based approach of Article 20(2) to be taken as the relevant benchmark, as this comes closest to the competitive 'as if' price.

(138) 'Relying on existing obligations to make data available' implies that even if obligations to make the data available existed, access based on such obligations would come too late or prove inefficient. In that case, Article 15 provides a means to request *ad hoc* access.

(139) In any case, Article 15(c)(1) requires that 'the adoption of new legislative measures cannot ensure the timely availability of the data'. This criterion is vague as it does not say anything about the perspectives of such legislation or whether legislative measures already have to be initiated. The criterion appears to be motivated by the Commission's belief that much of B2G data sharing is not likely to be addressed to a sufficient degree by legislative means in the future.[65] This logic, however, can lead to a deadlock: If Member States do not enact legislation, and if exactly this inactivity is a prerequisite for the legitimacy of requests under Article 15(c)(1), while at the same time Member States are pre-empted from implementing future legislation (see paras 141-146 below), this insufficient status of the legal framework will be perpetuated. Therefore, the legislature should delete this requirement, under the premise that the scope of Chapter V is narrowed down to *ad hoc* data access.

(140) Article 15(c)(2) sets out an alternative requirement to Article 15(c)(1), which is highly questionable. Basically, Article 15(c)(2) would allow the PSB to request data access under Chapter V even if it could actually obtain the data by other means. The precondition is that obtaining the data according to Chapter V 'would substantially reduce the administrative burden for data holders or other enterprises'. This criterion appears conceptually flawed. The Impact Assessment Report explains that there is an exceptional need for data where 'the different way of collecting the data would lead to substantial reduction of administrative burden for companies, replacing existing reporting obligations'.[66] However, this requirement contradicts Article 15(c), 1st sentence, according to which a lack of data prevents the PSB from fulfilling its public task. It is rather meant to increase the effectiveness of the means for fulfilling the public task (see para 135 above). Even if one takes an opposing view and does not see a logical flaw, requests based on Article 15(c)(2) could

65 Ibid, p 13.
66 Impact Assessment Report, p 34.

at best be issued only once, if one takes the 'exceptional need' criterion seriously, while it cannot provide a legal basis for regular and permanent data access. This would run against the nature of *ad hoc* data access (see para 143 below). In sum, the legislature should delete Article 15(c)(2).

(141) A crucial question regards the Proposal's pre-emptive effect on national legislation, specifically, to what extent Member States can impose legislation that would derogate from the provisions in Chapter V. At first glance, Article 15 extends the rights of PSBs vis-à-vis private data holders, so that the Proposal could be regarded to be in their interest. However, depending on its pre-empting effect with regard to national legislation, the Proposal might take away considerable legislative flexibility from the Member States in the future. This could run against the interests of the Member States in adopting sectoral regulation or even relax the requirements of Chapter V, for instance, to safeguard the interests of businesses.

(142) It is important to stress that the proposed Regulation neither applies to nor prohibits voluntary agreements or contracts that consider the exchange of data between private and public entities (Recital 59), even within the scope of the Regulation. The operational part of the Data Act should state this more explicitly (para 146 below).

(143) As for the scope of pre-emption, the Impact Assessment Report states that the law of the Member States should not expand the scope of the Data Act.[67] Article 40 confirms only that Chapter V leaves Union law (and therefore not Member States' legislation) unaffected. But what does this mean? Delineating the scope of Chapter V is crucial but not self-evident – it requires a contextual and more systemic view. For determining the scope of pre-emption, it is decisive that Chapter V only regulates *ad hoc* data access and not constellations of regular B2G data access.[68] The title of Article 15 supports this view: 'exceptional need' expresses that it is not about regular situations.[69] Also, Chapter V aims to reduce the duplication of similar requests to data holders, which is typical in *ad hoc* data access situations.[70] Moreover, the request mechanism under Articles 17 and 18 is designed as a one-off request mechanism and is not suitable for multiple requests that amount to a permanent and regular data transfer. Regular means of obtaining data, on the other hand, should therefore fall outside the scope of Chapter V. Such regular means are 'existing reporting or compliance obligations in sectoral legislation that establish ongoing or recurring data exchange mechanism between public institutions and the private sector.'[71] Such regular access regimes are

67 Impact Assessment Report, p 159.
68 This is explicitly stated in Impact Assessment Report, p 34.
69 See also Impact Assessment Report, p 34.
70 Impact Assessment Report, p 19.
71 Impact Assessment Report, p 158.

motivated by needs of non-exceptional nature, ie where the range of data holders is known and where data use can take place on a regular basis (Recital 59). Ultimately, this explains why the Regulation should be 'without prejudice to Union and national legislation obliging companies to share data in other situations and for other purposes (eg, reporting or monitoring regulatory compliance)'.[72] Article 16(1) reflects this and therefore confirms the *ad hoc* quality of the proposed Chapter V, which should not affect 'reporting, complying with information requests, or demonstrating or verifying compliance with legal obligations'.[73]

(144) The exception of Article 16(2)[74] proves this interpretation. It exempts requests for some *ad hoc* purposes. The Commission argues that, in these cases, B2G data use exists or will exist.[75] So in the listed areas, there cannot be pre-emption by Chapter V, allowing Member States to remain free to regulate *ad hoc* data access (see also Article 1(4)). *E contrario*, Chapter V can serve as a legal basis for *all* other purposes when it comes to *ad hoc* access and it pre-empts Member States from imposing respective legislation.

(145) As a consequence, Chapter V does not provide a legal basis for *regular* B2G data access, but only for data access on an *ad hoc* basis. Arguably, it can be challenging to draw the line between *ad hoc* and regular data access, such as when looking at the problem of repeated requests under Article 17 concerning the same data. If Chapter V enabled such requests, this would take away pressure from Member States to systematically enact desirable sectoral legislation for regular B2G data transfers. Accordingly, the envisaged limitation pre-emption of national law would then reach too far and perpetuate the current, unsatisfactory legal situation. As pre-emption should not prevent sectoral rules for continuous access (such as in the mobility or housing sector), it must be limited to *ad hoc* access, which needs to be interpreted narrowly (see para 135 above on the 'prevention' v 'effectiveness' argument). One exception to *ad hoc* access in sectoral legislation concerns specific conditions on compensation, which the Member States are free to define, provided that they do not exceed the limits set by the Proposal (eg, the free-of-charge provision).[76] However, as this is envisaging a limitation on pre-emption, the law has to address this more explicitly.

(146) Against this background, the EU legislature should consider the following amendments:

[72] Impact Assessment Report, p 34.
[73] See also Impact Assessment Report, p 34.
[74] See also Recital 60.
[75] Impact Assessment Report, p 159.
[76] Ibid.

- The Data Act should make more explicit that Chapter V only regulates *ad hoc* access, which requires the Regulation to delineate more clearly the scope of application in the context of pre-emption. For this purpose, the following wording should be added in Article 16(1): 'This Chapter only regulates *ad hoc* data access and …'.

- Include a new provision as Article 20(3) allowing for specific rules on compensation even within the scope of Chapter V (meaning for *ad hoc* data access).

- Include a new provision as Article 16(3), according to which the Regulation leaves voluntary data-sharing agreements between PSBs and private data holders unaffected as long as such agreements do not explicitly rule out the application of the rules under Chapter V. Article 16(3) should declare such clauses void *ex lege*. The title of Article 16 should be amended accordingly ('Relationship with data sharing agreements and other obligations …').

(147) The Institute welcomes that the Commission takes transparency and proportionality as guiding principles for the proposed data request mechanism in Articles 17 and 18 (see also Recital 61). To ensure transparency, Article 17(2)(f) obliges PSBs to make all requests publicly available online without undue delay. However, Article 31(3)(g), which designates competent authorities and tasks, is narrower as it only concerns the online public availability of requests in case of public emergencies. In order to maximise transparency, Article 31(3)(g) should cover all requests and therefore be changed to 'in case of exceptional need to use data'.

(148) The Proposal does not solve a factual challenge that PSBs face: According to Article 17(1)(a), it is necessary that PSBs specify the required data in their request. However, often PSBs do not know exactly what data private entities hold. If the request is not framed precisely, the data holder may legitimately decline the request due to an 'unavailability' of the requested data pursuant to Article 18(2)(a). Therefore, a systemic information asymmetry can hamper the effectiveness of the proposed data access right. The legislature could consider two options to address this concern. One would be to provide the PSBs with a more differentiated access right according to a three-step logic: (1) right to access information about the available datasets; (2) access to (sample) datasets for assessing their usefulness with regard to fulfilling the desired purpose; and (3) access to datasets for using them in accordance with the purpose.[77] Another way would be to at least require best efforts on the part of the data holders to provide information about available datasets and ultimately provide data that are best suited to fulfil the public interest purpose.

[77] See Richter (n 54) 547.

In any case, data holders should not be able to decline a request too easily on the grounds of data unavailability.

(149) Article 18(3) implements the 'once-only principle',[78] which aims to avoid burdening companies with multiple requests.[79] This principle obliges PSBs to keep track of and publish data requests (Article 17(2)(f)) and to destroy the data when no longer needed (Article 19(1)(f)), and it may also incentivise a better cross-border coordination between PSBs. However, the 'once-only principle' is limited to situations of public emergency (Article 18(3) and (4)) – and particularly in this context the design of the proposed procedure can be counterproductive: The proposed rules allow the data holder to legitimately decline the request (and therefore effectively prevent the PSB from obtaining the desired data) not only (a) if the PSB that made the first request forgot to notify the data holder of the destruction of the data, but also (b) if this PSB is no longer in possession of the data, or (c) if it cannot provide the data in a timely manner to the PSB in exceptional need. In case of emergency, the public interest in effectively responding to the emergency should prevail – at least in cases (b) and (c). Hence, the legislature could consider applying the 'once-only principle' only to exceptional cases of need for data under Article 15(1)(b) and (c) but not Article 15(1)(a). Arguably, however, the practical relevance may become limited as the requests then covered are probably less likely to serve exactly the same purpose in multiple cases. A preferable alternative solution would consist in providing for a 'backdoor' provision in Article 18(4), according to which the data holder still has an obligation to make the data available if the requesting PSB – after making reasonable efforts[80] – cannot obtain the data from PSBs that made previous requests.

(150) As for the procedure on challenging requests, Article 18(6) refers to Article 31. However, Articles 31-34 do not further specify the procedure (eg, deadlines or interim decisions). This appears particularly insufficient in case of public emergency: While Article 18(2) recognises the urgency by shortening the period for declining or seeking modification of the request, it remains entirely unclear and therefore left to the Member States to decide what happens if the data holder declines the request and the PSB wants to challenge it. The enforcement of Chapter IX should install a more specific procedure on challenging requests and redress. Moreover, Article 17(2)(e) should require the PSB to include a reference to the means of redress where the applicant wishes to challenge the request (see, for example, Article 4(4) OD PSI Directive).

(151) As regards the use and re-use of the obtained data in question, the proposal falls far short of unleashing the potential for data-related societal benefits.

[78] Impact Assessment Report, p 160.
[79] Ibid.
[80] This would also have to consider the urgency of the request.

Also, it lacks sufficient coherence. As for the use of the obtained data by the PSB itself, Article 19(1)(a) allows use only in a manner compatible with the requested purpose, but the data holder should be able to agree on uses beyond that purpose (see para 153 below).

(152) Article 17(4) addresses the exchange of the obtained data between PSBs and transfer to third parties who fulfil the public task. This is held legitimate as long as it is in compliance with Article 19. However, Article 17(4) requires that the outsourcing agreements be made publicly available.

(153) The legislature should re-consider the Proposal's handling of re-use according to open data principles. Article 17(3) prohibits the PSB from making obtained data available for re-use under the OD PSI Directive. However, there is no convincing justification for this *per se* prohibition. Recital 62 still aims to explain this by stating that the data 'may be commercially sensitive'. However, such sensitive data only amounts to a portion of all data shared under the Regulation and would be excluded from the scope of application of the OD PSI Directive anyway,[81] while it may fall under the scope of Articles 3-8 DGA. Due to the potential positive externalities of data re-use, the PSB should be able to make the obtained data available under the OD PSI Directive as long as legitimate interests of businesses as data holders are not negatively affected.[82] One solution would be to delete Article 17(3) so that re-usability would be entirely governed by the OD PSI Directive, which anyhow adequately balances private and re-use interests. However, the OD PSI Directive may not provide sufficient legal certainty, not only because Member States have chosen different levels of implementation, but also – what is more important here – because the Directive was not designed to fully account for the incentives for data creation by the businesses that are subject to mandatory data sharing. Therefore, it appears preferable that the proposed Regulation should reconcile the involved interests by ultimately leaving the decision of re-use to the businesses. For this purpose, Article 17(3) should be amended in such a way that it takes the application of the OD PSI Directive as the default rule and provides private data holders with (a) the possibility to object to the re-use without the need for justification, and (b) the explicit option to designate purposes beyond the requested purposes. This is already reflected in Recital 65, which states that the data holder who made the data available can expressly agree for the data to be used for other than the requested purposes – but surprisingly, the Regulation does not echo this possibility in the provided request mechanism. Also, the legislature could consider incentivising businesses to consent to re-use by providing additional compensation in such cases under Article 20, which would then have to be provided by the re-user and not the PSB itself.

81 See Art 1(2)(c) OD PSI Directive.
82 See Richter (n 54) 554.

(154) As a side note, the OD PSI Directive does not provide access to data, but only regulates re-use of data. For access to data, national rules (eg, access to information regimes) or sectoral EU or national legislation (eg, access to environmental or geographic information) are key. The Proposal does not affect, let alone exclude, access of third parties under current access rules to data which a PSB has obtained under Chapter V – even though it appears that this is what the Proposal is ultimately aiming for.

(155) While the Proposal would rule out the possibility to provide data under the OD PSI Directive, providing the data for re-use under Articles 3-8 DGA would be possible. This is to be welcomed, as Articles 3-8 DGA provide a differentiated regime for data re-use, which also accounts for the legitimate interests of the data holder and provides safeguards. However, Articles 3-8 DGA only apply to data that are protected on the grounds of secrecy, confidentiality, intellectual property or data protection, while Chapter V of the Proposal covers a much broader scope of data, which would not be re-usable under the current Proposal (see para 153 above). This means that with regard to an optimal level of re-use, relying on the application of the DGA alone appears insufficient.

(156) Article 21 allows use of the obtained data for scientific research or analytics and compilation of official statistics. However, the research must be compatible with the purpose for which the data was originally requested; and there may be grey zones (eg, as regards the questions of whether the research has to relate to addressing the concrete emergency or whether the data can be used for general research on emergency prevention).[83] Article 21 appears overly narrow with regard to the legitimate research purposes, not least because scientific research is an open-ended process. Regarding Article 21, the legislature should consider whether there are reasonable means to broaden the purpose or install a more flexible regime, while safeguarding the interests of the data holder. In fact, the legislature has already installed a mechanism in Articles 3-8 DGA that carefully balances such involved interests. The legislature should consider potential benefits of systematically referring to the DGA or at least borrowing from its concepts, not least because Article 21 remains silent on conditions, non-exclusivity and technical and legal safeguards (except for Article 21(3)) etc. – all aspects which the DGA explicitly addresses.

(157) As for the further obligations of PSBs, Article 19(1)(c) should include a corresponding right of the data holder to request information on whether the data is still stored (see also the request right under Article 20(2)).

(158) It is welcomed that Article 20(1) obliges data holders to make data available free of charge in case of public emergency (see also Recital 67). As it has been

[83] See also Recital 68.

argued that micro and small enterprises should be included in the scope of the Regulation (see para 133 above), the legislature might consider providing compensation to them. In other cases of exceptional need for data, Article 20(2) provides compensation, which should also include the costs for pseudonymisation (see para 160 below).

(159) It remains unclear how to calculate the reasonable margin as required in Article 20(2). The provision already implies that this should be calculated on a cost-based and not on a benefit-based approach,[84] but for the sake of legal certainty, the cost-based approach as a reference point for calculating the reasonable margin should be made more explicit in Recital 67. In substance, the legislature could borrow from the OD PSI Directive, which allows for a 'reasonable return on investment' in some cases and specifies that this is to be 'understood as a percentage, in addition to marginal costs, allowing for the recovery of the cost of capital and the inclusion of a real rate of return', which 'should not be more than 5% above the ECB's fixed interest rate'.[85] As the scope of the access right is limited to *ad hoc* situations (see paras 143-145 above), it is unlikely that access requests would negatively affect the data holders' ability to collect/create the data,[86] which could justify a full-cost-recovery approach.

(160) The Proposal could be made more precise on the relationship to personal data protection. Article 1(3) states that the Regulation leaves the application of data protection law unaffected. But what this means depends on the specific case and context. In particular, Article 18(5) requires data holders to take reasonable efforts to pseudonymise the data if such data are needed. An extension of this obligation to anonymisation is implied in Recital 64.[87] Therefore anonymisation should be explicitly mentioned in Article 18(5) as well. Conversely, the provision on compensation only mentions compensation for anonymisation, while there are no reasons to exclude the compensation for pseudonymisation. Hence, Article 20(2) should equally provide compensation for pseudonymisation. As anonymisation and pseudonymisation constitute data processing under Article 4(2) GDPR, they must be lawful according to Article 6(1) and (2) GDPR. For this purpose, the legislature should clarify (eg, in Recital 64) that Article 18(5) itself provides a legal basis for anonymisation and pseudonymisation according to Article 6(1)(c) and (3)(a) GDPR.

---

84 See Richter (n 54) 549; on pricing of the data see also Bertin Martens and Néstor Duch-Brown, 'The economics of Business-to-Government data sharing' (European Commission: Seville 2020) 12-16.

85 See Recital 37 OD PSI Directive.

86 See Richter (n 54) 549.

87 Where anonymisation proves insufficient, Recital 64 requires pseudonymisation.

(161) Chapter V leaves intellectual property unaffected[88] with one exception: As for *sui generis* database protection, Recital 63 states that 'data holders should exercise their rights in a way that does not prevent the public sector body and Union institutions, agencies or bodies from obtaining the data, or from sharing it, in accordance with this Regulation'. This provision is necessary to enable B2G data sharing,[89] and it resembles Article 1(6) OD PSI Directive as well as Article 5(7) DGA. However, due to its substantive effect to limit the businesses' exercise of intellectual property rights, a Recital is not sufficient; the subsidiarity of *sui generis* database protection in the context of B2G data sharing must be made explicit in the operational part of the Regulation (eg, included as a new Article 35(2)). In fact, should the concerned data be the content of a protected database, Chapter V makes it compulsory for data holders to license the *sui generis* database right to the requesting PSB. At the same time, Recital 63 implies that businesses will not be prevented from invoking *sui generis* protection for any sharing that is not in accordance with the Regulation and therefore will have some control over illegitimate (re-)use.

(162) Chapter V has another blind spot: What about cases in which the data holder is prevented from making the data accessible to the PSB due to mere contractual restrictions with third parties (and not due to trade secrecy or intellectual property)? Recital 66 implies that such contracts trump and may therefore prevent data access under Chapter V *per se*. Again, such a strict consequence must be reflected in the operational part of the Regulation (eg, by including a new Article 19(3)). In substance, the approach appears questionable: It is hardly justifiable to let contractual restrictions prevent access *per se*, not least because Chapter V would allow the PSB to request access to the data from the original data holder as well. Moreover, such precedence of contract could incentivise data holders and third parties who supply data to data holders to insert clauses in their contracts with the aim of derogating access obligations pursuant to Chapter V. To enhance B2G data sharing, the Regulation should render mere derogation clauses void and include a balancing test for cases in which contractual restrictions would prevent data access.

VI. Switching between data processing services (Chapter VI)

(163) The Institute welcomes the emphasis Chapter VI of the Proposal puts on the special regulatory framework for data processing services. Being rather reluctant in the past to come up with regulation in this regard,[90] it is welcome

88 Impact Assessment Report, p 160.
89 See Richter (n 54) 570.
90 Cf. The Commission rather preferred sector-specific regulatory approaches that build more on privately ordered solutions like the SWIPO codes of conduct established under Regulation (EU)

that the Commission now wants to address existing issues in the cloud and edge markets defining a horizontal legal framework for switching service providers. This Chapter is closely linked with Article 29 in Chapter VIII on interoperability. Both policy fields are key for quickly unlocking the value of readily available high-quality data across sectors and data-driven technologies. The future regulatory framework must be conducive to innovation, facilitate better data portability as well as fair access to data, and ensure interoperability.

(164) Indeed, creating a cross-sectoral governance framework for data access also depends on the next-generation cloud for businesses and the public sector. As a lot of data is externally and, in some cases, exclusively stored and processed with cloud and edge providers, such data has to be unlocked in order not to render data sharing obligations under Chapter II *de facto* impossible. Together with Chapter VIII, Chapter VI must provide the legal basis for horizontal data sharing across sectors. Such endeavour, however, requires targeted solutions guided by a market-functional approach that builds on market realities, already existing sector-specific interoperability frameworks and privately ordered solutions. It has to strike a balance between safeguarding the innovation incentives of firms and creating feasible, well-balanced and inclusive regulatory answers. These answers have to be technologically neutral, well-designed for digitally fit and non-fit companies and public institutions alike and effectively enforceable by a combination of a centralised and decentralised enforcement mechanisms.[91]

(165) The Institute wants to highlight the need for making a clear distinction between the regulation of data processing services, the design of the regulatory interoperability framework for data spaces and the interoperability provisions regarding smart contracts – or better: distributed ledger technology (DLT).

(166) Data processing services require a different regulatory intervention than a horizontally designed data interoperability framework. The specific lock-in scenarios and potential data-specific exclusionary effects of some big platform undertakings' strategic conduct present in the cloud and edge markets may justify legal intervention that goes beyond the existing

2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union, OJ L 303/59.

[91] On a sector-specific regulatory approach for data-driven financial services that already provides for sector-specific solutions but will cause challenges for the horizontal design of an interconnected cross-sectoral interoperability framework in the Proposal see Jörg Hoffmann, 'Safeguarding innovation in the framework of sector-specific data access regimes' in: German Federal Ministry of Justice and Max Planck Institute for Innovation and Competition (eds), Data Access, Consumer Interests and Public Welfare (Nomos: Baden-Baden 2021) 343.

competition law framework.[92] In addition, the interdependences between the legal framework for data processing services and the specific access rights and obligations for data holders, data generators, third parties and data recipients outlined in the previous Chapters are obvious and call for a holistic solution that addresses centralised and decentralised legal and regulatory solutions. The same applies to DLT applications – wrongly described as smart contracts – that need tailored solutions to match their technological interoperability specificities. This is vital for properly addressing the role of DLT for making data sharing more feasible.

(167) Chapter VI imposes obligations on the providers of data processing services by outlining minimum requirements for contractual switching and porting obligations. The regime for switching between data processing services corresponds with the exercise of a contractual data portability right that entails both switching and portability obligations. Making interoperability obligations a contractual obligation, for which parties may still negotiate the details, provides a more targeted, desirable solution despite potentially higher transaction costs.

(168) This is in line with the aim of EU Member States to establish the next generation of cloud services that reach the highest standards in portability and interoperability.[93] Yet it does not differentiate between different services and respective competition issues. This is surprising since the Commission itself outlined the need to differentiate various complex cloud computing services.[94] However, by outlining different degrees of interoperability in the technical switching provisions, the Proposal balances the all-encompassing, technologically indistinct and non-market-functional approach, thereby pursuing the objective of introducing more competition in the cloud services market. The latter – at least – is a welcome approach.

(169) As regards the proposed rules, Chapter VI needs certain amendments and clarifications. The first relates to the scope of application. The definition of ‘data processing service’ is not clear, to some extent overly broad and at the same time too narrow regarding the regulatory goals the Proposal wants to achieve. The definition in Article 2(12) is to be read in conjunction with

[92] Cf Björn Lundqvist, ‘Cloud services as the ultimate gate(keeper)’ (2019) 7 Journal of Antitrust Enforcement 220.

[93] Joint Declaration on Building the Next Generation Cloud for Businesses and the Public Sector in the EU, 15 October 2020, available at <https://digital-strategy.ec.europa.eu/en/news/towards-next-generation-cloud-europe>.

[94] European Commission, Commission Staff Working Document Impact Assessment, Accompanying the document Proposal for a regulation of the European Parliament and of the Council on a framework for the free flow of non-personal data in the European Union, SWD(2017) 304 final 4 and 11 et seq.. The Commission itself uses the term ‘data processing of different levels of intensity’ already in the context of clouds. It further acknowledges that there are different levels of complexity within the cloud that impact switching options.

Recital 71. This Recital however is extraordinarily technical and does not help to understand what a data processing service under the Proposal is. By comparing this definition with the National Institute of Standards and Technology's definition of cloud computing (NIST definition)[95] and taking account of the references to 'cloud' in Article 29(2), one could be tempted to conclude that Chapter VI only refers to cloud computing service providers. In this case, web services, such as for edge computing, would not be covered, while the Commission – both in Recitals 69 and 71, last sentence, and in the Impact Assessment Report[96] – seems to use the term 'data processing services' to specifically designate cloud *and* edge computing services. Even if only cloud computing services fell under the notion of data processing services, the definition is so broad that it may include any existing '-as-a-service' (XaaS) business model.[97] All of these XaaS models entail a digital service provided to a customer that enables on-demand administration and broad remote access to a scalable and elastic pool of shareable computing resources of a centralised, distributed or highly distributed nature. Thus, they would fall under the definition of Article 2(12) and, hence, under the scope of Chapter VI. This is again surprising as the Commission itself explicitly refers to cloud and edge markets only in the Explanatory Memorandum when justifying the encroachment on the providers' fundamental rights.[98]

(170) On the other hand, it is also not clear why under Article 2(12) online content services as defined under Article 2(5) 2017/1128 of the Regulation on Cross-Border Portability of Online Content Services are excluded.[99] Following the twofold rationale of Chapter VI, namely enabling better data sharing and increasing customer choice by tackling vendor lock-in scenarios,[100] it does not make sense under the latter reasoning to exclude online content service providers upfront. The recitals should therefore better explain why online

95 National Institute of Standards and Technology definition of Cloud Computing, 'The NIST Definition of Cloud Computing' (2011): 'Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics, three service models, and four deployment models.'

96 Impact Assessment Report, pp 35 and 160.

97 'As a Service', or XaaS (Anything as a Service) offerings provide endpoints for customers and consumers to interface which are usually API-driven but can commonly be controlled via a web console in a user's web browser.

98 Explanatory Memorandum, p 14.

99 Regulation (EU) 2017/1128 of the European Parliament and the Council of 14 June 2017 on cross-border portability of online content services in the internal market, [2017] OJ L 168/01. The Commission's press release announcing Regulation (EU) 2017/1128 mentioned video-on-demand platforms (Netflix, HBO Go, Amazon Prime, Mubi, Chili TV), internet TV services (Viasat Viaplay, Sky Now TV, Voyo), music streaming services (Spotify, Deezer, Google Music) or online games marketplaces (Steam, Origin) as examples.

100 Recitals 69 and 72 Regulation (EU) 2017/1128.

content service providers that fall under Article 2(5) Regulation 2017/1128 on the Portability of Online Content Services should be excluded.[101]

(171) Additionally, the broad definition of data processing services providers under Article 2(12), together with the exclusion of online content services providers, may lead to uncertainty regarding the scope of the legal obligations under Chapter VI. Such uncertainties would arise if a digital service provider offers both data processing services that fall under Chapter VI *and* online content services as defined in Article 2(5) of the Regulation on Cross-Border Portability of Online Content Services that are excluded under Article 2(12). The Proposal makes clear that online content service providers should not fall under the porting and switching obligation. Yet in cases of duality, ie businesses providing both sorts of services, Article 23(1)(c) and Article 24(a) do not make clear whether online content falls under the porting obligation related to '*all* data, applications and digital assets'.[102] This would increase legal uncertainty for both sides, which in turn would lead to unnecessary disputes and hinder the effectiveness of Chapter VI. We therefore suggest – should the exclusion of online content providers remain – clarifying that online content, as defined under Article 2(5) of Regulation 2017/1128, is not covered under Article 23(1)(c) and Article 24(a) of the Proposal.

(172) Another example where the scope of application is not clear regards data sharing service providers (data intermediaries) as regulated in the Digital Governance Act (DGA).[103] Due to the broad definition of 'data processing services' in the Data Act, this would lead to imposing switching and portability obligations on all data intermediaries, regardless of whether conducting a business (data brokers) or providing data sharing services meant to be used by a closed group of data holders and users. However, Recital 22 DGA explicitly excludes the application of the DGA to data processing services. Although the Data Act and the Data Governance Act are both regulatory tools aiming at fostering data sharing, Chapter VI of the Data Act Proposal specifically seeks to overcome vendor lock-in situations. Data intermediaries, however, do not necessarily create such situations, comparable to those of the cloud and edge markets. Hence, intervention under Chapter VI only seems justified for cloud and edge service providers.

(173) In sum, these observations on the uncertainties concerning the application of Chapter VI to services other than cloud computing services should be reason enough for the legislature to specifically consider the appropriateness of the application of Chapter VI to individual subcategories of 'data sharing services'. This should especially be done in the light of the question of whether the rules are appropriate and proportionate as regards both the content

[101] See Recitals 1, 5 and 8 of Regulation (EU) 2017/1128.
[102] Article 23(1)(c), Article 24(a) of the Proposal. Emphasis added.
[103] Proposal for a Data Governance Act (n 55).

of the mandatory contract rules and the degree of intensity of regulation for the individual sub-categories of services.

(174) Article 24(1) imposes minimum obligations on data processing service providers in the sense of mandatory contract law regarding both B2C and B2B relations. In addition, these obligations apply across all sectors. Article 26 of the Proposal only allows for differentiating between various data processing services to the extent that the concrete technical specificities (interfaces) of the switching and porting obligation are concerned. While the Institute welcomes the gradual approach regarding different levels of interoperability, it is questionable whether it is justified to apply such a broad regime to all kinds of data processing service providers from a market-functional perspective.

(175) There are doubts whether the broad exclusion of freedom of contract under Article 24(1) and (2) can be justified. On the one hand, the exclusion of freedom of contract for all market participants is in conflict with the goal of the Data Act to introduce more competition in the market.[104] The use of mandatory contract law could reduce investment incentives for competitors and ultimately harm innovation. On the other hand, however, Article 24(1) and (2) seeks to enhance competition among service providers by overcoming vendor and data lock-ins. Thereby it may indeed enhance potential competition and create incentives for especially innovative newcomers to enter the market. Specific features of the current market structure may equally argue in support of the Proposal. The market for cloud services in particular is dominated by big players of the platform economy (especially Amazon, Microsoft, Google), who will be addressees of the upcoming Digital Markets Act (DMA). As a primary goal, the DMA aims to preserve the contestability of the relevant markets. By promoting switching between service providers, the Data Act may well complement the regulatory approach of the DMA.[105] However, it should be noted that the DMA does not generally limit the freedom of contract of gatekeepers and that, even more, the applicability of mandatory contract terms under Article 24 Data Act is not limited to gatekeepers.

(176) A justification is also difficult to find against the backdrop of European contract law. The Digital Content Directive (EU) only provides consumers with a right to get access to their provided or created digital content in case of contractual termination after the provider's non- or poor performance,[106] while failure to provide the service appropriately is not a requirement for

[104] See also Recital 87, referring to this goal in the context of Art 24 of the Proposal.
[105] The interface with the DMA is also noted in the Impact Assessment Report, p 35.
[106] Article 16(4) Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services, [2019] OJ L 136/1.

switching providers and porting data under Article 24(1) of the Proposal. In addition, the rationale of data portability in the Digital Content Directive is not that different. It also seeks to overcome data lock-ins, albeit for the particular purpose to make the right to contract termination operational.[107] Furthermore, the Digital Content Directive balances conflicting interests in more detail by excluding specific digital content[108] and exempting specific services and sectors from the application of the Directive.[109] These considerations show that the legislature should reflect further on the appropriateness of the regulatory approach of Article 24(1) of the Proposal. This is especially true as regards its application to B2B constellations. Here, it should also be noted that the extension of fairness control of contract terms in such constellations pursuant to Article 13 of the Proposal is a bold step towards reducing the freedom of contract beyond consumer contract law (paras 119-133 above). Therefore, against the backdrop of the proportionality principle, the EU legislature should recognise the need to clarify the reasons why intervention is needed even in cases where parties negotiate their contract terms freely.

(177) Moreover, the legislature should explicitly clarify the applicability of Chapter VI where it overlaps with the application of the Digital Content Directive. Indeed, parallel application of the two legal instruments may well lead to conflicting outcomes. Digital content in the sense of the Digital Content Directive qualifies as 'data, applications or digital assets' in the sense of Article 24(1)(a) of the Data Act Proposal. Although the Proposal gives room for negotiating the concrete terms and conditions of the porting obligation, it establishes a more interventionist and ambitious porting regime. It establishes a higher degree of interoperability and requires more technological governance mechanisms. In contrast, the Digital Content Directive provides for specific limitations to the right of making digital content available. Accordingly, if it does not address the applicability of the Digital Content Directive in Article 24(1)(a), the Proposal would create conflicting provisions and outcomes if applied in parallel. Since the provisions of Article 24 can more easily be justified in B2C relations, the legislature should explicitly state that Article 24 prevails over the Digital Content Directive. There is no need to apply the less ambitious regime of the Digital Content Directive[110] to data processing services that fall under Chapter VI of the Data Act.

(178) Conversely, the requirement of 'technical feasibility' of switching in Article 24(1)(a)(1) and Article 24(2) Data Act would undermine the effectiveness of

[107] Recital 70 Digital Content Directive.

[108] Namely digital content that has no utility outside the provided service supplied by the trader or relates to the consumer's activity when using the digital content or a digital service supplied by the trader or that has been aggregated with other data by the trader and cannot be disaggregated or only with disproportionate efforts. Art 16(4) (referring to Art 16(3)) Digital Content Directive.

[109] Art 3(5) Digital Content Directive.

[110] Art 16(4) Digital Content Directive.

the switching and porting right. In practice, service providers could strategically rely on this requirement to escape the switching and porting obligation. Negative experience with Article 20(2) GDPR, which uses a similar restriction for the exercise of the data portability right regarding personal data, shows that the technical feasibility exception should be deleted or at least concretised in the sense that technical infeasibility can only be affirmed if a higher level of interoperability than outlined in Article 26 and 29 of the Proposal cannot be achieved.

(179) Maintaining the proposed technical feasibility standard would indeed run counter to the interoperability-by-design concept established under Articles 26 and 29 of the Proposal. The latter gradual interoperability approach has to be supported, as it not only creates predetermined obligations and by-design concepts of interoperability, but also reduces legal uncertainty in the enforcement of the provisions of Chapter VI and guarantees the effectiveness of the switching and porting provisions. The technical feasibility exception, in contrast, would give the provider of data processing services the option to limit its obligations to complete the switching process. While it is a worthy goal that data service providers should not be overburdened with IT- and data-specific compliance costs, the technical feasibility exception does not seem to be justified. The envisioned current transition period of 12 months between the entry into force of the Data Act and its applicability as outlined under Article 42(2) of the Proposal should be sufficient for service providers to comply with Chapter VI, even if the technical feasibility exception were deleted.

(180) While the Institute supports a more differentiated approach regarding different data processing services providers, it is questionable why Article 26 establishes a dual regime with regard to the appropriation of intellectual property rights essential for the implementation of interoperability specifications (interfaces). Article 26(2) requires certain service providers (PaaS and SaaS) to enable interoperability by making open interfaces 'publicly available and free of charge'. This is generally welcome as any intellectual property right essential for the technical means of switching should not jeopardise the feasibility of switching. Article 26(3), however, leaves other data processing service providers (mostly IaaS) with an option to appropriate their intellectual property essential for the implementation of interoperability specifications. This is because according to Article 29(3) the open interoperability specifications and European standards shall comply with paragraphs 3 and 4 of Annex II of the European Standardisation Regulation.[111] Under this regime, whenever intellectual property rights are essential to implementing specifications, their rightholders can choose between FRAND

[111] Regulation (EU) No 1025/2012 of the European Parliament and of the Council of 25 October 2012 on European standardisation, [2012] OJ L 316/12.

licensing and licensing without compensation.[112] Under Article 26(2) such an option does not exist. This would lead to comparative grievances as open interfaces are standards and typically fall under the European Standardisation Regulation. Such a dual regulatory approach needs justification. This holds particularly true against the backdrop of the very complex technical specificities of SaaS interfaces that have already raised concerns in previous assessments of cloud and edge markets by the Commission.[113] The Institute proposes that in line with Article 23(1) any technical obstacles that inhibit customers from switching and porting should be removed regardless of the type of data processing service. This includes that intellectual property rights that are essential for technical switching should be dismissed in this constellation. The differences and also interests of data processing services (eg, investment interests) should rather be addressed and safeguarded under the mandatory provisions regarding contractual obligations for data processing services within the scope of application of Chapter VI (see paras 169-170 above) and various remuneration models.

(181) The Institute further recommends moving Article 29 from Chapter VIII to Chapter VI, since Article 29 specifically addresses interoperability for data processing services. Both Articles 26 and 29 regulate technical aspects of switching in the context of Chapter VI. Furthermore, Article 29 explains the concept of 'open interoperability specifications and European standards for interoperability', which is first mentioned (but not explained) in Article 26.

(182) In the field of interoperability, the Institute agrees that public enforcement should play a major role. This is due to the information asymmetries that exist to the disadvantage of customers, who can hardly judge whether and under what conditions data sharing and portability can technically be implemented. The Proposal underlines the role of public enforcement with regard to Chapter VI in Article 31(2)(c). Still, it is not clear which rules will be enforced by the competent authority under Article 31 and which rules will be enforced by private law courts.

(183) Especially in Chapter VI, the Proposal adopts a hybrid regulatory approach, including various provisions that may individually be characterised more as an expression of private law or of administrative law. This makes the delineation of two enforcement regimes difficult and causes legal uncertainty and may *de facto* hinder the effective implementation and application of the Data Act. Some rules relating to and arising from contracts may be better enforced by private law courts. Yet the mandatory contract rules in Article 34 are also public-interest based, as is competition law. Hence, such rules may

[112] Sec 4(c) Annex II of the Standardisation Regulation.

[113] Impact Assessment Report, pp 11 et seq.; Douglas Hayward et al, 'Switching of Cloud Services Providers', Study of IDC and Arthur's Legal on behalf of the European Commission (2018) SMART 2016/0032, pp 10 and 29.

be enforced through both private lawsuits and the administrative authorities. The EU legislature could enhance legal clarity by being more explicit on the distribution of enforcement tasks.

(184) More specifically, the legislature could clarify that the technical aspects of switching are to be considered part of the contractual obligations and hence aspects that need to be considered for assessing the conformity of the service with the contract so that the respective rules can be enforced by private law courts as well.

(185) Article 31(3)(i) explicitly gives the competent national authorities the power to ensure that charges for the switching of service providers are withdrawn in accordance with Article 25. However, the latter provision, which explicitly empowers the Commission to adopt delegated acts in Article 25(4), is not clear as regards the distribution of power between the competent national authorities and the Commission.

(186) Another open question relates to the application of Chapter III to the obligations of data processing service providers under Chapter VI. The wording, especially of Article 12(1), as well as a purpose-based interpretation of the provisions of Chapter III seem to argue against such application. Conversely, providers of data processing services may fall under the definition of a 'data holder' in the sense of Article 2(6) and therefore could also qualify as data holders for the purpose of Article 8. Hence, the legislature is advised to clarify the situation.

VII. Non-personal data safeguards in the international context (Chapter VII)

(187) The Institute considers Chapter VII (Article 27) as perhaps the most problematic Chapter of the Proposal. The Institute is aware that Article 27 proposes to import the provision of Article 30 Data Governance Act into the Data Act. To justify this rule, the Commission explicitly points out that Article 30 DGA has found wide support in the European Parliament.[114] However, referring to a past mistake does not justify committing the same mistake again.

(188) Article 27 addresses three situations in the first three paragraphs that need to be evaluated separately. Yet all three paragraphs share three normative elements that individually raise concerns and should therefore be identified at the outset.

[114] Impact Assessment Report, p 35.

(189) First, Article 27 only applies to providers of data processing services, which are the addressees of the switching obligations in Chapter VI. In addition, the provisions should probably be read in the sense that they only apply where data are transferred to a non-EU country in the context of providing a data processing service. Hence, data transfers related to other activity of a company that is active in multiple fields of commerce, such as Amazon as the world's largest cloud service provider, will not fall under Article 27. The limitation to data processing services is explained by the fact that these services are exempted from the application of the DGA, including Article 30.[115] Hence, the logic of Article 27 is exactly to establish the same regime for data processing services that has been chosen to apply to 'data sharing services' under Article 30 DGA. Hence this rather limited scope of application does not alleviate any concerns. Quite to the contrary, there is a risk that the EU legislature will repeat the errors that it committed when it gave its approval to Article 30 DGA. Although both Chapter VI and Chapter VII of the Data Act Proposal regulate the same services, the concrete rules pursue very different, even opposing objectives. While Chapter VI seeks to promote switching between the providers of said services, which necessarily comes with a transfer of data, Chapter VII (Article 27) restricts data transfers, albeit in the direction of non-EU countries. This means that the legislature should pay particular attention to Article 27 to evaluate whether it achieves an appropriate balance between the conflicting objectives, and in particular to make sure that the principal objective of the Data Act to enhance data sharing will be sufficiently respected. More concretely, this requires a thorough analysis of the impact of Article 27 on the provision of data processing services where they entail a transfer or making available of data to third parties. This means *inter alia* taking account of Article 27 when the legislature reconsiders the definition of 'data processing services' as recommended above (paras 169-173).

(190) Second, Article 27 only applies to non-personal data. In this regard, particular questions of justification necessarily arise. This provision recalls similar provisions of the GDPR (Articles 44-50) that restrict the transfer of personal data to third countries. Indeed, a clear path dependence can be observed: the regulatory concept was first developed for the GDPR and then travelled to the DGA, and is now proposed for the Data Act. However, in the GDPR, the reason for restricting the transfer of data to third countries lies in the very nature of personal data and is hence in line with the general objectives of the GDPR. The logic is easy to understand: Data protection rules seek to protect the fundamental rights and freedoms of the data subject; these rights must not be restricted by data transfers to countries where the law fails to grant

[115] See Recital 22 DGA. See also Impact Assessment Report, p 35 (referring to both cloud and edge service providers).

equivalent protection.[116] In the case of non-personal data these arguments do not apply. Quite to the contrary, the argument that there are no personal interests argues in favour of promoting data-sharing across borders. This objective characterises all other Chapters of the Proposal. Hence there is tension between Article 27 and the other rules of the Data Act Proposal. This distinguishes the function of the rules on cross-border data transfers in this Proposal from their counterparts in the GDPR. In the GDPR the restriction on cross-border data transfers complies with the general objectives of that Regulation, whereas Article 27 stands in opposition to the data sharing goals of the Data Act. These arguments should also have been considered before the adoption of Article 30 DGA. Both Article 30 DGA and Article 27 of the Data Act Proposal only ostensibly create a more coherent data law, with identical principles applying to both personal and non-personal data. In this context, however, it would be important to understand that very different policy considerations have to apply to the two categories of data when it comes to international data transfers. Thus, to what extent the same or similar regulatory regimes can apply to personal and non-personal data requires thorough consideration by the legislature.

(191) Third, the provisions seek to safeguard interests that are protected by other parts of the law of the EU or the law of the relevant Member State. A conflict of other parts of the law with the objective of the Data Act to promote data sharing should typically lead to a weighing exercise. It is questionable, however, whether Article 27 reaches an appropriate balance. Doubts relate in particular to the fact that Article 27 makes identical rules applicable to enforce the respect of the law in all fields on the EU and national level, while the interests protected under the various laws are largely diverging.

(192) As regards the assessment of the provisions of Article 27, a clear distinction has to be made between Article 27(1), on the one hand, and Article 27(2) and (3) on the other hand. The latter two provisions react to a foreign judgment or administrative decision that requires the service provider to transfer data or make data accessible, while Article 27(1) is a regulatory rule that tends to attribute to the provider of a data processing service the role of a law enforcer. The introductory concerns set out above regard Article 27(1) in particular. For this reason, in the following, the less problematic rules of Article 27(2) and (3) will be discussed first.

(193) Article 27(2) and (3) addresses situations where a foreign judgment or administrative decision requires a provider of a data processing service to transfer or give access to non-personal data this provider holds in the European Union. Article 27(2) is unproblematic, since it establishes the principle that such judgment or decision will be recognised and enforced

[116] See C-311/18 *Data Protection Commissioner v Facebook Ireland and Schrems* (‘*Schrems II*’) ECLI:EU:C:2020:559, paras 101-103.

based on an international agreement. Such an agreement not only sets a clear standard to solve the conflict within the legal order of the EU. It will also protect the service provider against additional enforcement actions and sanctions in the foreign state.

(194) Article 27(3) addresses the more critical situation where there is no international agreement with the other state and where compliance with the foreign judgment or decision would risk putting the service provider in conflict with EU law or the national law of the relevant Member State. For this case the provision establishes cumulative requirements that need to be fulfilled to allow the service provider to transfer the data or grant access to the data. In principle, the service provider itself has to assess whether these conditions are fulfilled. However, this burden is alleviated by Article 27(3)(2) where the Proposal provides that the service provider 'may' request the 'relevant competent bodies or authorities' to determine whether the requirements of Article 27(3)(1) are fulfilled.

(195) Several critical questions need to be asked regarding Article 27(3)(2). Does this provision only refer to the balancing requirements in Article 27(3)(1)(a)-(b), or also to the assessment of the EU or national law as to whether a conflict exists? The latter seems to be the case, since Article 27(3)(2) refers to 'these conditions' without any further specification. This should also be in the interest of the service provider who may have particular problems to correctly assess the legal situation. Such reading however raises additional questions. Article 27(3)(2) does not specify which is the 'relevant competent board or authority'. Since all the conditions of sub-paragraph 1 are related to issues that regard the specific law that may be violated, preference should be given to the body or authority that is competent for the specific subject-matter of that law and not the authority or court that deals with mutual legal assistance with third countries. Yet this in turn raises the question of how to deal with private law cases, for which administrative authorities will not exist. There can be no doubt that Article 27 also applies to private law – Recital 77 even explicitly mentions trade secrets protection and intellectual property rights. In such cases, to solve the problem of legal uncertainty, the service provider would have to convince the trade secrets holder or the holder of the intellectual property right to consent to the transfer or bring a court action against the other private party concerned. In the fields of trade secrets protection and intellectual property law this would have to be requested for a declaratory judgment of non-infringement. Since Article 27(3)(2) refers not only to authorities but in a very generic manner to 'relevant competent bodies', private law courts may also be covered. However, should this mean that, if the other party refuses to give consent to the data transfer, the service provider will then have a right to bring such action? If this were so, Article 27(3)(2) might even change the national procedural laws of the Member States, especially as regards the admissibility of declaratory actions. More

importantly, should EU law really trigger burdensome litigations before courts that would otherwise not take place? Not to mention that these proceedings can last many years. In practice, these latter issues may never matter, because, being under the threat of foreign enforcement measures and sanctions, no provider will bring such cases to the courts given the fact that such proceedings will not be efficient and expeditious enough to produce a court determination. To solve such problems, Member States could create 'competent authorities' to determine whether there is a conflict even in the field of private law. However, this would create a risk of illegitimately restricting the interests of the other private party. Trade secrets and intellectual property cases can be highly complex, and the determination of such cases should not occur without equal opportunities of the parties to plead their case in application of all the safeguards of the rules of civil procedure. To conclude, the legislature should seriously consider excluding conflicts with private law from the application of Article 27(3). This would at least have the result that, if the service provider follows the foreign judgment or decision, the service provider cannot be held accountable by the competent authority in the sense of Article 31. The service provider may still be sued for infringement by the other party. But it is more than appropriate to leave it to the private law courts to solve such conflict. To protect the interests of other parties in private law cases, Article 27(5) already includes an obligation of the service provider to inform the data holder about the request of an administrative authority before complying with the request. This provision adequately enables the data holder to seek interim injunctions against the service provider, especially in private law cases. However, this provision is too narrow, since it does not cover requests by foreign courts. Moreover, it should be extended to other third parties, such as third-party holders of IP rights and trade secrets holders.

(196) In the context of Article 27(2) and (3), the legislature is also advised to consider amending Article 27(4). This provision contains a data minimisation rule as regards the sharing of data in response to a third-country judgment or decision. It is understandable that in the context of Article 27(2) and (3) the service provider should not provide more data than necessary. However, this is not a matter of the 'amount of data' but of their informational content. To make this clear, the wording should be changed accordingly.

(197) Compared to Article 27(2) and (3), the obligation laid out in Article 27(1) is of a very different nature. In a situation where there is no foreign judgment or decision, Article 27(1) imposes an obligation on the service provider to take '*all* reasonable technical, legal and organisational measures, including contractual measures'[117] to prevent international transfer or government access where such transfer or access would create a conflict with Union law or the national law of the relevant Member State. The Institute is concerned

[117] Emphasis added.

that this rule will create an effect similar to that of a data localisation rule, since this obligation may well force data processing service providers to completely refrain from transferring data to countries outside the EU and granting access to data from such countries.[118] Several features of Article 27(1) contribute to this effect:

(198) First, as in Article 27(3), Article 27(1) is designed to safeguard the respect of any law on the EU and national level. This would require the service provider to set up a special system of legal compliance with all laws that one may think of. This contrasts with the situation under the GDPR, which only requires the data controllers to monitor compliance with one field of the law.

(199) Second, while Article 27(3) only applies in the hopefully rare event that a service provider is addressee of a foreign judgment or decision, Article 27(1) affects the entire business of a service provider that operates globally.

(200) Third, many of the laws will require a monitoring of the (semantic) content of the data. A provider of data processing services, such as cloud services, however, is not a content provider. Still, the obligation of Article 27(1) applies to such a provider. This may well mean that the provider has to monitor all the data that are transferred to, or made accessible from, third countries as part of its service. In this regard, three concerns arise: (i) such monitoring is not required as part of the service. Hence, an obligation to monitor the content would create considerable costs for the service provider, which would then have to charge a higher price. This would in turn considerably reduce the capability of internationally operating providers to compete with other providers that stick to the principle of localisation of the data within the EU. (ii) Monitoring needs to be legal in relation to the customer. This would require the provider to impose a contractual obligation on the customer to agree to the monitoring. Indeed, Article 27(1) includes mention of contractual obligations to guarantee compliance. However, such monitoring will be another reason why customers may prefer competitors that practice data localisation within the EU. Where the data consists in trade secrets of third persons, customers under a confidentiality obligation will not even be allowed to disclose the data to the service provider. (iii) Given the immense amount of data that is processed, it is most likely that it will not be technically possible to monitor all the data.

(201) Yet the result remains the same. To guarantee compliance, any legal counsel to such service provider will recommend avoiding any transfer of data to countries outside the EU, if the company wants to offer its services within the

[118] For clarity on what data localisation requirements are, see Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union, [2018] OJ L 303/59. This Regulation focuses on eliminating intra-EU data localisation.

EU. The data will be localised in the EU. Economically, data localisation has specific effects on both the service provider and its customer. On the one hand, service providers from third countries who want to extend their business to the EU need to store the data in the EU. This puts these service providers at a competitive disadvantage vis-à-vis their EU-based competitors. Hence, Article 27(1) has a protectionist effect. Secondly, the price for this lessening of competition will have to be paid by EU customers. More importantly, customers located within the EU may suffer much more in another regard. To a large extent, representatives of EU-based companies, public sector bodies and research institutions are located in different parts of the world, communicate with their colleagues of the same institution globally and travel around the world. Cloud service providers that localise all the data in the EU will not be able to cater for their needs. To address these needs, such entities will have to use closed digital systems that only grant access to a defined group of persons. While the Commission argues that erecting safeguards against unlawful transfers of data to non-EU countries will promote trust in cloud and edge services and thereby promote the development of this sector,[119] it may be more likely that Article 27(1) could create considerable impediments to data sharing.

(202) Beyond these economic concerns there are a number of legal concerns regarding Article 27(1). In the following, a few uncertainties concerning the wording will be addressed. In addition, particular attention should be paid to the interface with international trade law, on the one hand, and private law, on the other hand.

(203) The measures required from service providers under Article 27(1) are very far-reaching. It is only the test of 'reasonableness' that limits the scope of what the service provider is requested to do. Reasonableness requires a balancing. In particular, the provision does not include a 'technical feasibility' test. Whether lack of 'technical feasibility' can be considered as part of the assessment of reasonableness is an open question.

(204) Particular uncertainties arise from the requirement that the risk of conflict with EU or national law has to arise from 'international transfer or governmental access'. Here, inclusion of the term 'governmental', which only relates to 'access', is extremely puzzling. The most obvious explanation may be that the Commission is particularly concerned that governments of non-EU countries may seek access to non-personal data by exerting pressure on cloud service providers. However, such case would also be covered without the word 'governmental' in the text. Quite to the contrary, a literal understanding of the wording would lead to the conclusion that, as regards governments, mere access to the data can suffice to trigger the application of Article 27(1) of the Proposal, while the service provider does not have to

[119] Impact Assessment Report, p. 31.

prevent mere access of other third parties located outside the EU. However, it cannot be assumed that the Commission intends such a literal reading. Therefore, the legislature is advised to delete the word 'government' in the provision and to mention the specific case of government access in the recitals.

(205) Moreover, the wording of Article 27(1) differs from that of Article 27(3) in that the latter prohibits any data sharing that would result in a 'risk of conflict' with EU law or national law, while Article 27(1) seems to require – since the term 'risk' does not appear – an actual conflict. Setting the bar of intervention higher in Article 27(1) corresponds to the higher intensity of regulation this provision pursues. However, whether there is only a risk of conflict or an actual conflict cannot be distinguished with legal certainty. At least as long as there is no case-law that identifies the test for actual conflict compared to a risk of conflict, the higher benchmark will not alleviate the regulatory burden for providers of data processing services under Article 27(1).

(206) The major problem however regards the term 'conflict', which is used in both provisions of Article 27(1) and (3). This term is puzzling, since it would be clearer to stipulate that the transfer of data to a third country or granting access to data from such countries constitutes a violation of the law for which the service provider could be held liable. If this were the interpretation, Article 27(1) would not add anything to the already existing law. Hence, the concept of a conflict has to require less than a violation of the law by the service provider. Taking into account that Article 27(1) requires the service providers to take measures to prevent a conflict with the law, and since the provision does not require that without such measures the service provider would be held liable for infringement of the law, it seems almost mandatory to understand Article 27(1) as a rule that establishes a form of 'contributory liability' of the service provider. This would especially be relevant in cases where under the relevant EU or national law only the customer would be held liable for the sharing of data with a non-EU country. In such cases, Article 27(1) would create additional obligations of the service provider to prevent an infringement of the law by its customer. Whether this is appropriate is however very questionable. Many fields of the law draw the line between who is and who is not liable based on a specific balancing of interests. For instance, where the transfer of a trade secret to a third country would constitute a violation of trade secrets protection by the user of the service, as a matter of EU trade secrets protection, the provider of the data processing service should only be held liable if it knew or ought to have known that the transfer was illegal.[120] This guarantees that anyone who is not aware or should not be expected to be aware of the infringement should be allowed to use the protected information. This is a conscious decision of the EU legislature as a result of a weighing of the interests of parties concerned against the backdrop

[120] Article 4(4) Trade Secrets Directive.

of the fairness principle. There is no reason why Article 27 should put this weighing aside. The same applies in the context of intellectual property law, which similarly recognises principles of liability of third parties, especially intermediaries, that contribute – by aiding and abetting – to the infringing acts of others. In the same sense, one may question whether Article 27(1) is in line with the rules of liability of intermediaries in the digital economy laid down in Chapter II of the Digital Services Act (DSA).[121] In certain cases, providers of data processing services may also fulfil the requirements of a hosting service in the sense of Article 2(f) DSA and, hence, benefit from the limited liability under Article 5(1) DSA. In such cases, Article 27(1) seems to be in conflict with the prohibition of a general monitoring or active fact-finding obligations.

(207) As mentioned above (para 201), Article 27(1) may have the effect of discriminating against service providers from third countries that seek to offer their services in the EU. This raises the question of whether this is compliant with the obligations of the EU under the WTO/GATS Agreement and bilateral trade agreements concluded between the EU and third states. Although these agreements do not have direct effect within the legal order of the EU and the EU legislature is therefore free to adopt legal instruments that do not observe the obligations from these agreements as a matter of internal EU law, the EU legislature should not blindly adopt rules that violate obligations of the EU under international law. The Institute refrains from an analysis in this regard but recommends that the EU legislature examine the compliance of Article 27(1) with international law before adopting this provision.

(208) Particular legal issues arise in the context of private international law. In this regard, the Institute is particularly concerned about the explicit Proposal in Recital 77 that Article 27(1) should also apply to trade secrets and intellectual property protection. Here, the question arises when there is indeed a conflict with these laws. The point of departure for answering this question is the universally recognised principle that the territorial reach of private law is to be defined by choice-of-law rules as part of private international law. As regards intellectual property law, Article 8(1) Rome II Regulation establishes that the question of whether there is an infringement will be governed by the law of the state for which protection is thought (so-called 'country of protection').[122] This would allow any rightholder to seek protection under EU law or the law of a Member State. However, to successfully argue an infringement under that law, as an expression of the principle of territoriality,

[121] Proposal of the Commission of 15 December 2020 for a Regulation of the European Parliament and of the Council on a Single Market for Digital Services (Digital Services Act) and amending Directive 2000/31/EC, COM(2020) 825 final.

[122] Regulation No 864/2007 of the European Parliament and of the Council of 11 July 2007 on the law applicable to non-contractual obligations (Rome II), [2007] OJ L 199/40.

which is equally recognised globally in the field of intellectual property, the infringing act also needs to occur in the country of protection.

(209) Against this backdrop, it must be asked whether Article 27(1) is supposed to change or set aside existing choice-of-law rules. The text of the Proposal does not provide any answer, since it does not address the private international law dimension of its rules. Still, it cannot be ignored that choice-of-law rules as part of the private international law of the EU may apply in these cases, such as in cases concerning intellectual property rights and trade secrets protection.[123]

(210) Hence, assuming that a conflict with private law can only be confirmed under Article 27(1) where EU law or the relevant law of an EU Member State is also applicable under the general rules of private international law, this would necessarily limit the cases where a service provider would have to prevent cross-border data flows. To take again intellectual property law as an example, one could still argue that national authorities are competent pursuant to Articles 31(1) and 1(2)(e) as regards the question of whether the cross-border transfer or making accessible of the data infringes intellectual property rights where an EU customer initiates such data sharing.[124] In contrast, neither EU law nor the law of the Member States would apply where the data sharing enables an infringement by another person acting outside the EU after having received access to the data.

(211) This latter limitation is important to note, since the situation is quite different under Chapter V of the GDPR. As regards personal data, Article 44, 2nd sentence, and Article 45(1) GDPR seek to guarantee that a transfer of data to a third state will not occur if the law of this state does not provide adequate protection to ensure that the level of protection of the GDPR will not be undermined. This rule is very much inspired by the fact that particularly at the time of the adoption of the GDPR many states around the globe did not provide for adequate data protection. Consequently, the legislature opted for far-reaching extraterritorial application of the GDPR.

(212) Since the regulatory model of controlling data transfers to non-EU countries originates from the GDPR, the question may well be asked whether Article 27(1) should be interpreted in a similar way, namely, to require equivalence

[123] As regards trade secrets law, there is no doubt that the Rome II Regulation also applies. However, it is not completely clear whether Article 4, 6(2) or 8(1) Rome II Regulation should apply as the relevant choice-of-law rule.

[124] In cases of cross-border use of IP rights on the Internet it is generally recognised that countries have a legitimate economic interest to regulate such activity if the Internet can be accessed from their territory. However, this does not mean that there is no use of the right in the country where the alleged infringer has acted.

of legal protection under the law of the other state. Explicit statements in this regard are made in Recital 15 DGA, where it is argued that non-personal data

> should be transferred only to third countries where appropriate safeguards for the use of data are provided. Such appropriate safeguards should be considered to exist when in that third country there are equivalent measures in place which ensure that non-personal data benefits from a level of protection similar to that applicable by means of Union or national law in particular as regards the protection of *trade secrets* and the protection of *intellectual property*.[125]

(213) However, this reasoning relates specifically to Article 5(9) through (13) DGA and only regards the transfer of non-personal public sector information. Such requirement of equivalence is not mentioned in Article 27 of the Data Act Proposal. Nor does the Proposal contain a mechanism for assessing the equivalence of the foreign law with European standards as can be found in Article 45 GDPR and Article 5(9) DGA. Moreover, globally recognised principles of private international law, as regards intellectual property and trade secrets law in particular, argue against a requirement of equivalence. Private international law provides choice-of-law rules that are based on a general weighing of the interests involved in a cross-border case. As part of this logic, courts will in principle apply the designated foreign law without checking the appropriateness of that law in any regard. A general requirement of equivalence would be fundamentally opposed to private international law. It is only exceptionally that courts will refuse to apply the foreign law, namely, where the result of the application of that law would fundamentally collide with the public order of the *lex fori* (the law of the deciding court). As regards the international law on intellectual property and trade secrets protection, it has to be noted that there are various international agreements that guarantee high standards of intellectual property in practically all states. Moreover, the international agreements build on the principle of national treatment, according to which, apart from the substantive standards they contain, the contracting parties are only required to grant foreign rightholder the protection that their own nationals enjoy.[126] This excludes any additional reciprocity requirement. Hence, application of any equivalence test in the context of Article 27(1) would amount to nothing less than extraterritorial application of European standards in contradiction to the fundamental rules and principles of international IP law, namely, the principle of territoriality

[125] Emphasis added.

[126] See in particular Art 3 WTO/TRIPS Agreement. This agreement is also applicable to trade secrets protection. It includes a substantive provision in Art 39. The principle of national treatment has a long history going back to the 19th century. In particular, it was implemented in the Berne Convention concerning copyright and the Paris Convention concerning industrial property, both adopted in the late 19th century.

and the national treatment obligation. This analysis shows that one should not draw any inferences from data law, especially data protection law, for other fields of law. In intellectual property and trade secrets law, the analysis shows that the legal system governing cross-border cases has evolved to such a degree that there is indeed no need for applying Article 27. Yet it would not come as a surprise if the competent authorities specialising in data law (Article 31 of the Proposal) tended to look at international data sharing from a perspective that is strongly informed by data protection law. Equally, risk averse service providers, who may not easily understand the complexities of the operation of laws in a cross-border context, may overreact and stop data transfers that are neither in violation of intellectual property nor trade secrets law. Hence, Article 27(1) could have a disruptive effect on the traditional cross-border operation of important parts of private law, such as intellectual property law in particular.

(214) The main recommendations concerning Article 27 can be summarised as follows:

(a) Article 27(1) should be deleted. At the least this provision should not apply in the field of private law, where international private law provides for adequate rules to solve cross-border conflicts and where the applicable national law should conclusively regulate who is liable for law violations. This is even more true for the fields of intellectual property law and trade secrets protection, where international law has comprehensively established standards of protection in cross-border cases.

(b) Article 27(3) can in principle be maintained. However, the text should exclude the application of this provision as regards conflicts with private law. In the private law field, the enforcement should be left to the competent courts.

(215) To conclude on Chapter VII, it should be noted that the Data Act will certainly have a huge influence on the development of data law globally. The overall protectionist approach of Article 27(1) will not remain unnoticed by other states and may fuel a global trend towards requirements of localisation of non-personal data in the country of origin. Such a trend could considerably hamper the development of the digital economy globally to the disadvantage of all nations and regions, including the EU. The risk is real, since an increasing number of states are discussing and adopting policies of ‘data sovereignty’, and the policy debates, especially of countries of the Global South, such as India, are increasingly influenced by the emerging debate on ‘data colonialism’. While the EU should promote policies in favour of data sharing globally, Article 27(1) goes exactly in the opposite direction. This provision could fuel the attitude to consider ‘domestic’ – personal and non-personal – data a natural resource, the use of which in third countries should not be

considered legal without authorisation from the governments of the data exporting countries.

VIII. Interoperability (Chapter VIII)

(216) Chapter VIII – together with the Regulation on the Free Flow of Non-Personal Data[127] and the Data Governance Act[128] – proposes a regulatory interoperability framework as the key legislative measure of the horizontal EU data governance framework. The Commission has long stressed the need for a legislative framework for establishing interoperability and rightly ruled out a 'one size fits all' approach.

(217) With its interoperability requirements, Chapter VIII strengthens the Commission's new policy approach of aspiring to a global leadership role for EU standards and enhancing the international competitiveness of the EU data economy.[129] Ultimately, standardisation has to be at the core of future policy considerations. Dynamic solutions in terms of data-driven innovation are crucial to ensure the interoperability of products and services, reduce costs, improve safety and foster further innovation.

(218) This approach complies with the policy proposed in the Communication on a European Data Strategy.[130] As defined under Article 2(19) of the Proposal, the concept of interoperability builds on existing interoperability frameworks. These frameworks are designed as data governance regimes and reflect the complexity of the data interoperability they embody. The Proposal introduces different types of interoperability obligations beyond mere data-access-specific interoperability and encompasses technological data processing and potential data sharing infrastructure. More specifically, Chapter VIII contains three provisions that set up special interoperability requirements for three groups of addressees, namely, for operators of data spaces (Article 28), providers of data processing services (Article 29) and, finally, vendors of smart contracts (Article 30). Article 29 has already been considered in the context of Chapter VI, which equally applies to providers of data processing services. Accordingly, the following comments mostly concentrate on Articles 28 and 30.

(219) The very targeted approach of the three provisions of the Chapter also means that the Proposal does not include any obligations regarding interoperability

[127] Regulation (EU) 2018/1807 (n 118).
[128] Data Governance Act (n 55).
[129] See Communication from the Commission, An EU Strategy on Standardisation: Setting global standards in support of a resilient, green and digital EU single market, COM(2022) 31 final.
[130] Communication from the Commission – A European strategy for data, COM(2020) 66 final, 12-13

of other data holders that are required to provide access to data under Chapter II. This Position Statement has already submitted recommendations (see paras 66-67 above) to remedy this shortcoming. It is not clear why the Commission did not propose interoperability requirements as obligations in the context of Chapter II. Perhaps the Commission was concerned that uniform rules may not necessarily fit all sectors. Still, the Institute recommends considering whether more could be done in the framework of Chapter VIII (see also para 67). In particular, adopting the requirements contained in Article 28(1)(c) on operators of data spaces would also seem suitable in the case of data holders regarding IoT data. Where these and additional appropriate requirements are fulfilled, the legislature could stipulate that the data holder has fulfilled its obligation to make the data available to the user or the third party as required by Articles 4(1) and 5(1).

(220) As regards the specific statutory data access and use regimes in Chapter III, it is important that the legislature when adopting such regime in the future will also provide for sufficient regulation of the interoperability aspects.

(221) Generally speaking, the Institute welcomes the active role of the EU legislature and regulators in establishing a legal and regulatory framework for operators of data spaces, providers of data processing services and vendors of smart contracts. Yet there is still room for improvement of the design of the proposed provisions.

- **Operators of data spaces**

(222) Article 28(1) imposes interoperability obligations on operators of data spaces without defining them. This lack of definition could compromise the application and enforcement of the provision. In the Staff Working Document on Common European Data Spaces, the Commission only states that such definition is still on its way to being developed.[131] However, it will not make any sense to adopt a set of obligations and make them enforceable if the addressees are left in the dark about whether they are required to act and may have to expect enforcement measures and sanctions.

(223) In Article 28(1), the Proposal adopts a performance-based approach, listing several technical requirements for data access that data space operators are expected to meet. Among the technical means to enable data access, the Commission mentions application programming interfaces (APIs) as one example.[132] In this context, the Proposal leaves open how this provision should work, if the APIs are protected by intellectual property law.[133]

[131] Staff Working Document on Common European Data Spaces, SWD (2022) 45 final, 4.
[132] Art 28(1)(c) Proposal.
[133] On APIs and potential issues of IPRs see Jörg Hoffmann and Begoña González Otero, 'Demystifying the Role of Data Interoperability in the Access and Sharing Debate' (2020) 11 JIPITEC 252, para 49. On copyright protection for APIs in the US see *Google v Oracle America*,

Potential availability of intellectual property protection could seriously undermine the whole functioning of the interoperability concept for Common European Data Spaces. Article 28 should therefore resolve the tension between potential intellectual property protection and the interest in enabling data access.

(224) Yet Article 28(1)(c) is not the only place where the legislature could address this tension. Future intellectual property legislation could clarify, narrow or even exclude the availability of IP protection of APIs to favour dynamic competition. Intellectual property rights should not go beyond their purpose to create incentives for creativity and innovation and should not erect additional obstacles to access indispensable technical infrastructures.

(225) Competition law, in contrast, can only play a marginal role, as its concepts are rigid, and its enforcement tends to be slow. Only in exceptional circumstances can Article 102 TFEU be relied upon to overcome the exclusivity of intellectual property rights,[134] while reforms of national competition law have recently focused more on lowering the threshold for intervention where data access is hindered by *de facto* control of data.[135]

(226) Still, issues of IPRs can also be addressed within the rules of data access regimes. Preserving the exclusivity of intellectual property protection for the technical means of access jeopardises the functioning of data access rules and fails to reach the goal of the Proposal to establish interoperability. Such a rule, which follows the example of Article 35 of the Proposal concerning the *sui generis* database right, could be implemented as a new paragraph directly following Article 28(1). This provision could read:

> In order not to hinder data access in the context of paragraph 1(c), neither the rules of EU and national intellectual property law nor those protecting trade secrets pursuant to Directive (EU) 2016/943 apply to application programming interfaces.

(227) Article 28(3) proposes a presumption of conformity with the interoperability requirements of paragraph 1 under the condition that operators of data spaces comply with harmonised standards or parts thereof. These standards shall be published by the Commission. However, Article 28(3) does not specify these

593 U.S. __ (2021) (leaving open whether the API in the case at hand was copyrightable, arguing that the defendant Google could anyhow rely on the fair use exception). In Europe, the CJEU has at least clarified that data languages and data file formats are not protected under copyright law. See Case C-406/10 *SAS Institute* ECLI:EU:C:2012:259, paras 29-46.

134 Case C-418/01 *IMS Health* ECLI:EU:C:2004:257, para 35 (on refusals to license); Case C-170/13 *Huawei Technologies* ECLI:EU:C:2015:477, para 47 (on the competition law defence against the grant of injunctions for the enforcement of standard essential patents).

135 On the recent reform of German competition law, which aimed at facilitating data access in case of data dependence, see at paras 36 and 125 above.

standards any further, whereas on data processing services Article 29(3) is more precise, stating that the interoperability specifications shall comply with the open interoperability standards of Regulation No 1025/12, sections 3 and 4 of Annex II.[136] Taking into account that the definition of 'harmonised standards' in Article 2(1)(c) of Regulation 1025/12 would also apply as regards the provisions of the future Data Act, the omission of the reference to sections 3 and 4 of Annex II in Article 28(3) of the Proposal appears as questionable.

(228) Data spaces may also function as a means to enable data sharing across different industrial sectors.[137] This insight led to the concept of Common European Data Spaces,[138] whose interoperability the Commission has most recently deemed essential.[139] The Proposal, however, does not mention anything about interoperability across data spaces in Article 28. It just addresses interoperability requirements for data spaces in general. Indeed, the Common European Data Spaces are still under construction. Nevertheless, the recitals to the Data Act should mention the objective of achieving interoperability across data spaces as well.

(229) For achieving cross-sector interoperability, it is important to be mindful of a major challenge, which is that, as part of their vertical approach, existing standardisation initiatives address sector-specific realities. Each sector has its own data features, such as health, mobility or finance, and even within individual sectors it has been hard to achieve agreement on interoperability standards. Hence, a horizontal, one-size-fits-all approach to data spaces may encounter limitations, because it would fail to meet the particular needs of individual sectors.[140] For the future, it will be important to analyse how bodies in charge of establishing standards and interoperability manage to adequately address existing challenges of vertical standardisation and at the same time identify cross-sectoral commonalities.[141]

(230) An essential precondition for data spaces to work is the creation of functioning governance mechanisms. As part of this, institutions need to be established that implement, monitor and secure interoperability. However, in Article 28, there is not a single reference to institutions that will supervise interoperability. Only in the Explanatory Memorandum does the Commission indicate that the European Data Innovation Board (EDIB) and the Data Spaces

[136] Regulation (EU) No 1025/2012 of the European Parliament and of the Council of 25 October 2012 on European standardisation, [2012] OJ L 316/12.
[137] Commission Staff Working Document on the free flow of data and emerging issues of the European data economy, SWD(2017) 2 final, p 18.
[138] See Commission Staff Working Document on Common European Data Spaces, SWD(2022) 45 final, p 2.
[139] Ibid, p 43.
[140] Ibid, p 5.
[141] Ibid.

Support Centre will be the institutions in charge of advising the Commission on defining interoperability requirements and standards for data spaces.[142]

(231) In comparison, the Proposal for the Data Governance Act (DGA) is more precise on the governance model for interoperability. Articles 26 and 27 DGA establish the European Data Innovation Board (EDIB) as an advisory body to provide expert input on developing guidelines for European data spaces. The technical issues include the development of common standards and the securing of data interoperability. In contrast, the Data Act Proposal only mentions the advisory role of the EDIB in developing guidelines on the assessment of international data access and transfer (Article 27(3)(3)). There is, unfortunately, no specific mention of the EDIB in Article 28 concerning data spaces.

(232) On the role of the Data Spaces Support Centre, the Proposal is equally silent. This new institution has the task of coordinating aspects such as data infrastructure requirements, processes and standards that enable data to be re-used across sectors.[143] The Support Centre is also expected to assist the EDIB.[144]

(233) Consequently, in the context of Article 28, the legislature should recognise and define the specific role of the EBID and the Data Spaces Support Centre in attaining interoperability. This may be implemented in the recitals by reference to the DGA and the Staff Working Document on Common European Data Spaces. The advantage of prescribing the roles of these monitoring institutions in both the DGA and the Data Act is that this would help increase trust in the Common European Data Spaces initiative. It would likewise contribute to the uniformity and coherence of the different legal instruments that are adopted for the regulation of the data economy.

- **Vendors of smart contracts**

(234) Article 2(16) of the Proposal defines ‘smart contract’ as ‘a computer program stored in an electronic ledger system, wherein the outcome of the execution of the program is recorded on the electronic ledger’. This definition is very technical and raises some difficulties. This is the first time that smart contracts will be defined by EU law.[145] The definition refers to an ‘electronic ledger’ rather than a ‘distributed electronic ledger’. An electronic ledger could mean many things, while a distributed electronic ledger is commonly used as a synonym for ‘blockchain’.[146] In contrast to what Article 2(16) provides, the

[142] Explanatory Memorandum, p 14.
[143] SWD on Common European Data spaces (n 138), p 8.
[144] Ibid.
[145] There are numerous definitions for smart contracts in US law at state level, but none of them has been adopted in Europe.
[146] Blockchain is a particular type of DLT.

Data Act should prefer a definition of smart contracts that reflects on their real technological capabilities and that takes into account the guiding principles and definition used in the market. The most commonly used definition was provided by Szabo in 1994. He defined a smart contract as 'a computerised protocol that executes the terms of a contract.'[147] The Commission should consider that implementing a computerised protocol could occur with computer programs or in other digital electronic form, thus not necessarily encoded in the form of a computer program as Article 2(16) states. Hence, the proposed definition, not respecting the principle of technological neutrality for the design of the law, could limit the applicability of the requirements of Article 31.

(235) Article 30(1)(b) introduces a mandatory requirement to ensure a mechanism for terminating and interrupting the operation of a smart contract. One may wonder whether this requirement could render many existing smart contracts illegal, as one of the main characteristics of smart contracts is their immutability. The requirement to 'avoid future (accidental) executions' could even legitimise a kill switch that would make smart contracts unusable.

(236) Recital 80 explains the goals of addressing smart contracts in the Proposal. This includes 'promoting the interoperability of smart contracts in data sharing applications' and specifies that to 'facilitate the conformity of such smart contracts … it is necessary to provide for a presumption of conformity for smart contracts that meet harmonised standards'. However, Article 30 goes beyond these objectives. In addition to making clear what the goals are and reflecting them in the legal text, Article 30 fixes essential requirements for the specificities of smart contracts, their interoperability and their conformity with European standards.

(237) For promoting interoperability, a coherent centralised enforcement mechanism avoiding overlapping competences of various national and European authorities is key. To the extent that those overlaps exist, smooth and effective collaboration among the authorities is of primary importance.

(238) Against the backdrop of these requirements, the legislature should note that EU law, such as under the Digital Markets Act (DMA), has already adopted interoperability obligations, or is in the process of adopting such obligations, with regard to other specific platform providers.[148] The Proposal for the DMA envisions the Commission as the central regulator not leaving any role to national authorities, whereas Article 31 of the Proposal provides that national authorities are to guarantee compliance with the interoperability requirements of the Data Act. The legislature should consider whether such distribution of

[147] Nick Szabo, Smart Contracts (University of Amsterdam 1994). Note that this definition was not formulated for blockchain-based smart contracts.

[148] See, in particular, Art 6(1)(f) DMA.

competences is really required, and if so, how collaboration between the different authorities can be guaranteed. In addition, using different authorities does not need to exclude a 'one-stop shop'. For instance, the legislature could concentrate the enforcement of the interoperability rules in the hands of the Commission in cases where the addressees are gatekeepers in the sense of the DMA.

(239) In addition, centralised administrative enforcement has to be coordinated with parallel and robust private enforcement mechanisms. Information asymmetries regarding the technical details of interoperability justify centralised regulatory oversight and enforcement. But there is also a need to set out the right to access and use data as well as to switch between service providers as a matter of private law.

IX. Implementation and enforcement (Chapter IX)

(240) In Article 31, Chapter IX puts the focus on public enforcement. On private enforcement, in contrast, it remains silent, although many of the rules of the Proposal relate to contractual relationships and devise private rights among market players. Thus there can be no doubt that parties should also be able to enforce their rights by way of private litigation. In the following, the Position Statement will distinguish between the two enforcement regimes.

- **Public enforcement**

(241) With the exception of Chapter V, the Proposal seeks to regulate the rights and obligations between private parties in the data economy. Yet Article 31, including Article 31(3)(d) on enforcement by 'dissuasive financial penalties', seems to apply to all provisions. In this regard, it needs to be asked whether such enforcement system can be considered as proportionate taking into account the freedom of the regulated natural and legal persons to conduct a business under Article 16 EU Charter of Fundamental Rights.

(242) The legal nature of Article 31 is rather opaque. The rules of an EU regulation are directly applicable. However, the provisions of Article 31 mostly establish obligations of the Member States, including an obligation to designate the competent authorities in the first place. Article 31(3) should also be understood in the sense that it is for the Member States to 'lay down the [clearly defined] rules'[149] and implement the tasks listed in that provision in a clearer and more targeted manner. However, it is not

[149] As formulated in Art 33(1).

clear to what extent the Member States will enjoy flexibility when implementing these rules. In particular, it remains unclear whether Member States will be allowed to differentiate when they enforce the different obligations of actors as set out in the Proposal. In particular, the question arises whether and to what extent Member States are allowed to differentiate with respect to imposing financial penalties. Will Member States be free to impose such penalties only for the violation of some selected obligations or will they only be allowed to differentiate as regards the amount of penalties? Differentiation as such is indeed required in the light of the constitutional rights concerned. Also, Article 33(1) refers to the principles of effectiveness, proportionality and dissuasiveness for the design of penalties, which can be taken as a clear indication that differentiation is not only possible but even mandated. The authorities are equally in need of discretionary power, the boundaries of which national law will have to define with more legal certainty. In this regard, Recital 83 provides some guidance.

(243) Public and private enforcement have different advantages and shortcomings. This means that the principles of effectiveness and proportionality should also apply to the decision of whether certain rules are better enforced by administrative authorities, private law courts or both. Unfortunately, the Proposal does not provide any guidance in this regard. Rather, it seems to maintain that administrative enforcement should apply to all rules of the Proposal. In some cases, this may not be appropriate.

(244) Administrative enforcement is certainly appropriate with regard to the technical aspects of data sharing, including interoperability requirements in particular. Many holders of rights under the Act may lack digital literacy and therefore depend on effective public enforcement.

(245) Market regulation should in principle be justified in the light of identifiable market failures. Equally, the regulatory authority should only impose sanctions that adequately respond to such market failures and do not go beyond what is needed. In data protection law, it is the information asymmetry between the data controller and the data subject that makes it almost impossible for the latter to identify violations of data protection rules. This is why high financial penalties are justified in data protection law to deter violations of the law. As regards the Data Act Proposal, a very similar situation arises in the context of Article 4(6), sentence 2. Although this is clearly a private right, it should also be possible for the authority to act in case of violation of this rule and also impose financial penalties.

(246) While the Institute is concerned that Article 31 may give rise to the risk of over-enforcement, the Institute is in support of the right to bring a complaint before the competent authority as proposed in Article 32. However, it is to be noted that the wordings of Recital 82 and Article 32(1)

diverge as regards the rights of the complainant. Recital 82 explicitly states that natural and legal persons 'should be *entitled to seek redress*'[150] by lodging complaints with competent authorities. Article 32(1), on the other hand, only states a 'right to lodge a complaint'. In contrast to the latter wording, 'a right so seek redress' should make clearer that the private or legal person should also have a right to appeal to administrative courts if the competent authority rejects the complaint. However, there is nothing in Article 32 to indicate such right to an appeal. Only Article 32(2), which provides for an obligation of the competent authority to inform the complainant of the progress of the proceedings and the decision, could be interpreted in the sense that such appeal should not exist. Here, the legislature is recommended to follow the text of Recital 82. However, this should not only be realised by explicitly mentioning a 'right to seek redress' in the text of Article 32(1). The legislature should also add another provision, possibly as a second sentence added to Article 32(2), providing for a right to appeal to the competent administrative court in case the authority rejects the complaint in whole or in part. Such a 'right to seek redress' combined with a right to appeal to the courts would help guarantee uniform and effective enforcement of the Data Act across the Member States. It is of course true that such right should not restrict the authority too much in the assessment of individual cases, maybe even in prioritising cases. This concern should however be taken into account by the Member States when they design implementing rules that delegate discretionary power to the authorities.

(247) A particular shortcoming of Article 31 is that it does not address the delineation of the competences of the national authorities in cross-border cases. Article 31(4) only deals with coordination of competences among equally competent authorities on the national level. The Data Act cannot delegate the delineation of the competences of authorities of different states to the Member States since the same rules need to apply to all authorities in the EU. Such delineation is also important for the right to seek redress. Such right can only be sought against the competent authority.

- **Private enforcement**

(248) The legislature is recommended to make it explicitly clear that the Data Act can also be enforced before private law courts. The Proposal as it stands is silent on the matter. It is true that Recital 82 alludes to private enforcement by mentioning collective actions, and that Article 10(5) at least indirectly confirms that national courts could take cases on FRAND litigation. However, the possibility of private enforcement should be confirmed the same way as the entitlement to seek redress by lodging complaints to the competent authority. This should not only be done in

[150] Emphasis added.

Recital 82. Rather it is recommended to add another Article in Chapter IX that provides that '[t]his Chapter does not exclude the right of natural or legal persons to directly enforce their rights against other natural or legal persons before the competent courts'.

(249) Such provision would still not clarify what the remedies are and how the provisions of the Data Act interact with other parts of private law, including for instance the rules of contractual liability for non-conformity of a product or service with the contract, which particularly plays a role in the context of Chapter II, VI and VIII. In this regard, the Data Act should at least make clear that these rules, including the applicable rules of EU law concerning B2C contracts, will apply.

(250) The legislature should consider excluding public enforcement with regards to certain parts of the Data Act, namely, where private law enforcement is clearly superior to administrative enforcement. This is especially the case as regards the fairness control of contract clauses in B2B relationships under Chapter IV. The general clause on unfairness in Article 13 uses concepts that are inherently of a private law nature. Application of these concepts requires a balancing of the interests of the parties, who equally need to be protected in their interest in having equal opportunities to be heard by the court in private law proceedings. The reference made to collective actions in Recital 82 seems to refer in particular to Chapter IV and, hence, proves the relevance of this Chapter for private enforcement.

(251) The Commission is also recommended to consider whether the enforcement of Articles 4 and 5 in Chapter II should not be exclusively delegated to private law courts. As regards the IoT data access and use right, private law courts are better placed to assess the recommended purpose-bound approach, taking into account the particular interests of parties in proceedings that give equal opportunities to the parties to be heard. Still the Institute agrees that there are some rules contained in Articles 4 and 5 for which public enforcement should be allowed. This includes the enforcement of Article 4(6), 2nd sentence (para 50 above), and, if the recommendation is followed, the obligation to provide the data in a 'commonly available machine-readable format'. Finally, it is to be conceded that public enforcement of Chapter II in its entirety may generally increase the effectiveness of the provisions. Hence, the legislature will have to strike a balance, and in doing so it should also take account of the argument that exclusion of public enforcement would alleviate the regulatory burden for manufacturers. An alternative solution

could therefore exist in maintaining public enforcement, but exempting micro and small enterprises from such enforcement.[151]

(252) Under certain circumstances, administrative enforcement and even financial penalties may be needed to guarantee full respect of the law among private parties. This is for instance the case in consumer protection law, where the law imposes on businesses an obligation to refrain from certain practices vis-à-vis consumers, such as unsolicited commercial phone calls, and where individual consumers would not have sufficient incentives to claim injunctions before private law courts. This case of unsolicited phone calls shows that administrative fines may be needed and justified in cases where the infringement of the law is very much a general feature of doing business affecting all customers. This may make Article 3 a good candidate for public enforcement, since this provision typically addresses the general design of products and the information that should be delivered to users, while Articles 4 and 5 relate to individual cases where the user, or a third party authorised by the user, claims the right of data access and data use. However, availability of administrative enforcement for Article 3 should not exclude private enforcement. As explained (para 74 above), the principle of data access by default can also be enforced based on the private law rules establishing liability for the non-conformity of products or services with the contract.

(253) Finally, the same reasons for preferring private enforcement in the case of Articles 4 and 5 apply even more to Articles 8 and 9 in Chapter III. Both latter provisions require a weighing of interests of the parties concerned. To recognise administrative enforcement as a third route to enforcement in addition to actions before state courts and complaints before the dispute settlement bodies of Article 10 would even appear excessive and unnecessary. Yet it may make more sense to allow for parallel administrative and private enforcement of Article 11 relating to the use of technical protection measures. In the light of both the technical dimension of the rule and the rights and obligations this provision provides for, administrative enforcement, including the imposition of penalties, may seem appropriate.

X. Limiting the *sui generis* database right (Chapter X)

(254) While the Data Act does not pursue a reformulation of intellectual property rules, it is not blind to the fact that intellectual property rights (IPRs) will often constitute a major obstacle to access and use of data. In Article 35 (Chapter

[151] Art 7(1) currently generally exempts micro and small enterprises from the application of Chapter II. For the reasons to apply Chapter II also to these enterprises, see para 96 above.

X) the Proposal seeks to resolve the particularly vexing question of the applicability of the *sui generis* database right to IoT data.[152] To explain this, the Commission refers to the legal uncertainties about whether databases containing data generated from IoT products would benefit from such protection,[153] and the 'risk of an expansive interpretation of the *sui generis* right'[154] as extending to such data. To resolve such concern, Article 35 of the proposed Data Act stipulates that 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', 'in order not to hinder the exercise of the right of users to access and use such data … or of the right to share such data with third parties'. In other words, the database *sui generis* protection cannot be invoked by data holders as a defence for not fulfilling their obligations under Articles 4 and 5.

(255) As for the nature of Article 35, the Commission claims to clarify the application of relevant rules on *sui generis* database protection under Directive 96/9/EC.[155] At the same time, the Commission refers to the German *Autobahnmaut* case,[156] where the German Federal Supreme Court (*Bundesgerichtshof*) 'favoured the interpretation according to which machine-generated data would be included in the *sui generis* right'[157] and points out that this will no longer be the case.[158] Therefore, it can hardly be argued that Article 35 only provides a form of legislative interpretation of the Database Directive. What argues even more against such reading is the fact that such 'interpretation' would only apply where it runs the risk of hindering the rights proposed for Articles 4 and 5. This shows that Article 35 clearly intends to adjust the scope of the protection of the *sui generis* right.

(256) However, there seems be an alternative interpretation of the legal nature of Article 35, namely, in the sense of giving precedence to the exercise of the data access and use right in Articles 4 and 5 over the application of the Database Directive in cases in which the *sui generis* database right is concerned.[159] This interpretation would be more in line with EU legal principles. It would continue to guarantee that national courts will maintain their right to interpret the Database Directive and to refer questions of interpretation to the CJEU. Nor is it illegitimate to balance the interest in promoting data access and use with *sui generis* database protection in the legal

[152] See, in particular, Drexl (2018) (n 6) 67-85.
[153] Explanatory Memorandum, p 4.
[154] Impact Assessment Report, 133.
[155] Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases, [1996] OJ L 77/20. See Explanatory Memorandum to the Data Act Proposal, p 4.
[156] *Bundesgerichtshof*, Case I ZR 47/08, *Autobahnmaut* (25 March 2010).
[157] Impact Assessment Report, p 136.
[158] Ibid.
[159] On such proposal see Drexl (2018) (n 6) 82-83.

instrument that provides for the new data access regime. The EU legislature is not obligated to implement rules on the *sui generis* database right only in the form of amendments to the Database Directive. Accordingly, Article 35 of the Data Act Proposal should be considered as *lex specialis* with respect to the Database Directive. As a directly applicable legal instrument, the Data Act even has the particular advantage that it will 'reform' the *sui generis* database right with the entry into force of the Act, while the reform of the Database Directive would only be completed with the implementation in the Member States.

(257) The Institute agrees that there is a need for excluding the applicability of the *sui generis* right where it conflicts with the exercise of the IoT data access and use right. This has not changed with the more recent case-law of the CJEU. It is true that in its *CV-Online Latvia* judgment the CJEU limited the availability of the *sui generis* database right, recognising that the right should only be considered as infringed where the unauthorised use would result in 'depriving [the rightholder] of revenue which should have enabled him or her to redeem the cost of [the] investment' for making the database.[160] Such limitation of the scope of protection in the light of the objective of the right to create incentives for the making of the database was indeed rejected in the German *Autobahnmaut* case.[161] And in most cases relating to machine-generated IoT data, the investment in creating the 'data' will anyhow be recouped by charging a price for the product. Hence, it may well be true that protection will not be available in the light of most recent case-law. However, this shows that Article 35 enacts sound policy considerations. The legislature is well justified to exclude the application of the *sui generis* right, where the database maker is relying on the right only strategically to generate additional income that is not necessary as an incentive for creating the database. In conclusion, Article 35 may not matter much in practice taking into account the recent judgment of *CV-Online Latvia*. But this judgment is not an argument for deleting Article 35. This provision is needed to create sufficient legal certainty. Moreover, it should also be noted that the reasoning of the CJEU in *CV-Online Latvia* is not the only reason for having the provision. In the case

[160] Case C-762/19 *CV-Online Latvia* ECLI:EU:C:2021:434, para 31. The requirement of 'adversely affecting the investment' in the creation of the database was explicitly included in the answer of the CJEU to the national court.

[161] *Autobahnmaut* (n 156), para 25. In that case, the plaintiff, a company that put up cameras at the entry points of German motorways to register heavy commercial vehicles for the purpose of collecting toll, sought protection of the database that contained the information on the billing for individual truck operators. The defendant tried to rely on the argument that protection should not be recognised because the toll collect company was not in need of protection to recoup the investment in the creation of the equipment that collected the data, since it was anyhow remunerated by the German government for the service of collecting the toll on the government's behalf. The German *Bundesgerichtshof* rejected this defence, arguing that the statutory provisions did not contain any such negative requirement for the availability of the right. Following the CJEU's judgment in *CV-Online Latvia*, the *Autobahnmaut* case would now have to be decided differently.

of the IoT data access and use right, the interests of the user to use the data to enable added value uses should generally prevail over the interests of the holder of a *sui generis* database right irrespective of whether there is another possibility to recoup the investment or not. This is clearly reflected in Recital 84, which does not justify the exclusion of protection by the possibility of the database maker to recoup the investment by other means but very generally by the risk of undermining the exercise of the data access and use right. This will matter enormously for future cases of data access and use rights because the *sui generis* database right can also create obstacles to data sharing in other cases where the legislature provides for data access and use regimes. Article 35 may here set a standard for future legislation. Indeed, Article 35 is an expression of the modern understanding that the *sui generis* database right largely fails to lead to innovation. This is even more true where the *sui generis* right has the potential of creating obstacles to data sharing and hence a risk of hindering follow-on innovation that depends on the use of data shared by others.

(258) There is still room for optimising the text concerning Article 35. This especially regards Recital 84. There, if the text were to be taken literally, Article 35 would only apply 'where such databases do not qualify for the *sui generis* right'. However, such a condition is not included in Article 35 and should not be included. The intention of the Proposal is exactly the other way round, namely, that where such right would conflict with the exercise of the IoT data access and use right, *sui generis* protection should also be excluded in cases where the requirements for a *sui generis* database right are fulfilled. Hence, the quoted wording should be deleted from Recital 84.

(259) Other ambiguities arise from the notion 'containing data obtained from or generated by the use of a product or related service' in Article 35. Here, if one follows Recital 14 with the definition denoting data that 'represent the user's action and events', only first-level raw data will be covered. As argued above (paras 23-24), this narrow reading would in many cases not serve the purpose of the data access and use right.

(260) In this context, the wording of Article 35 already seems to go beyond mere (unstructured) raw data, as it is also covers 'data obtained from the use of a product or a related service'. This departure from the definition of the data to which Article 35 refers is at first astonishing. However, with the term 'obtained data', the drafters of the Proposal seem to align Article 35 with Article 7(1) Database Directive, according to which investment in the obtaining of data can give rise to *sui generis* database protection. Thereby this may be intended to make clear that in a situation where machine-generated raw data is processed in real time and integrated into a structured database, protection of such database should not hinder the exercise of the IoT data access and use right. Beyond this it should be noted that the substantial

investment as the condition for acquiring *sui generis* database protection is not limited to investment in 'obtaining' the data but may also relate to the verification and presentation of the machine-generated data. Article 35 should be interpreted in the sense that it excludes *sui generis* protection for any kind of investment mentioned in Article 7(1) Database Directive. However, in the light of the recommended 'purpose-bound' approach, the legislature is recommended to adopt the wording proposed for Article 4(1) also in the context of Article 35 (see para 85 above). Hence, the provision should read at the end as follows: '…does not apply to databases containing data obtained from or directly or indirectly generated by the use of a product or a related service to which access is required to enable added value uses in the legitimate interest of the user'.

(261) Additional uncertainties result from the fact that Article 35 excludes protection for all databases that 'contain' IoT data. This raises the question of whether even the smallest amount of data generated by the use of an IoT product suffices to exclude protection or whether a minimal amount of machine-generated data should be required. In the light of the objective of the provision to prevent any hindrance of the exercise of the data access and use right, the first interpretation seems the preferable one. How much other data is contained in the database is irrelevant since Article 35 only applies when and to the extent that recognition of *sui generis* protection would hinder the exercise of the data access and use right. This does not exclude recognition of the *sui generis* right regarding the extraction or re-utilisation of non-machine-generated data contained in the database.

(262) Finally, it should be pointed out that Article 35 applies irrespective of who the rightholder is. In many cases, this will be the manufacturer of the product, who will be identical with the 'data holder' in the sense of the person who is obliged to make the data available under Articles 4 and 5. However, application of Article 35 is not excluded in cases where the *sui generis* database right is held by a third party. In practice, of course, such latter cases are not very likely to occur.

(263) The major limitation of Article 35 consists in the fact that it only applies to the IoT data access and use right in Chapter II, whereas data access and use rights can also arise from other statutory data access and use regimes as addressed in Chapter III and in the context of voluntary data sharing as addressed in Chapter IV. This raises the question of whether the scope of application of Article 35 should not be extended beyond Chapter II. There can be no doubt that the *sui generis* database right can be as much of an obstacle in such other cases as for those addressed in Chapter II. Quite to the contrary, it may be even more likely in the context of Chapters III and IV that the requirements for a *sui generis* protected database right will be fulfilled in the light of the *CV-Online Latvia* judgment of the CJEU since in such other cases

the database maker oftentimes will not be able to recoup the investment in the making of the database through other means.

(264) As regards Chapter III, it is to be remembered that according to Article 12(3) it only applies to obligations arising from legislation that enters into force after the date of the entry of the Data Act. Therefore, it is advisable to consider the impact of *sui generis* database protection on making data available in the concrete context. Conceptually, Chapter III only regulates the relationship between the data recipient and the data holder where there is indeed an obligation to share the data based on other provisions of EU or national law. Hence, those other laws should determine the relationship with *sui generis* database protection. There is however a problem as regards access regimes under national law, since the national legislature is not authorised to set aside or limit the application of the sui generis database protection as mandated by the EU Database Directive. In this regard, the EU legislature may consider allowing for such possibility by adding a second paragraph to Article 35 empowering Member States to apply rules that follow the example of Article 35 in the context of the national regime. This provision should be worded as follows:

> When adopting future national legislation to which Chapter III applies, Member States are authorised to implement a rule according to which the *sui generis* database right provided for in Article 7 of Directive 96/6/EC does not apply to databases where necessary in order not to hinder the fulfilment of the obligation to make data available pursuant to this national legislation.

(265) There can be no doubt that *sui generis* database rights can also create obstacles to voluntary data sharing, which is covered by Article 13. In such cases, the person invoking the database right will typically be a third person who claims protection against the data holder to enjoin the latter from sharing the data with another party.[162] It is in particular in such instances that the exercise of the *sui generis* database right can be extremely harmful to data sharing. However, the Data Act Proposal addresses voluntary data sharing only in the context of unfairness control of contracts. This is not the appropriate context for restricting the availability of the *sui generis* database right as in such instances both the data holder and the data recipient will be negatively affected by the exercise of the *sui generis* database right. In addition, Article 35 may not necessarily be the appropriate template for solving the conflict in the case of voluntary data sharing. In such instances, it may be appropriate to

[162] This was indeed the scenario in the German *Autobahnmaut* case (n 156). The defendant, a shareholder of a company with which the toll collecting company cooperated for the collection of the toll from the truck operators, had factual access to the billing information and decided to make this information available online to the individual truck operators to inform them on a daily basis, while the toll-collecting company only sent out its bills once a month.

work with a compulsory licensing system that would provide the third-party holder of the *sui generis* right at least with a royalty payment for the use of the database. Still, the Institute deems it extremely important to draw the EU legislature's attention to these cases, because they show that Article 35 can only be considered one element of a broader approach to adjust *sui generis* database protection for the purpose of promoting data sharing.[163] Such a compulsory licensing system should ideally be implemented as part of a reform of the Database Directive. However, this does not preclude as a matter of principle providing such a system as part of the legislation on a specific data access regime.

(266) Finally, it should be noted that the restrictive effect of *sui generis* database rights on data sharing is also mentioned in Recital 63 as regards cases where private data holders may claim such rights as a defence against public sector bodies (PSBs) that seek data access in the context of Chapter V. There, the Commission indeed opts for a compulsory licensing model, which, however, as argued above (para 161), would require an explicit provision in the operational part of the Act.

XI. Coordination with intellectual property, trade secrets and data protection law

(267) The following comments will explore more concretely how the rules of the Data Act can be better coordinated with intellectual property law, trade secrets protection and data protection.

- **Intellectual property beyond *sui generis* database rights**

(268) Intellectual property (IP) has already been addressed in this Position Statement. In such contexts, it should have become sufficiently clear that a more profound analysis and maybe even reforms of existing IP regimes may be needed to make the data economy work. Still, the Proposal does not achieve a coherent approach to the interface with IP. In Article 35, the Proposal quite rightly addresses the potential blocking effect of the *sui generis* database right on the exercise of the rights in Chapter II, while in Chapter VII on the transfer and making available of non-personal data to countries outside the EU, the Proposal adopts a rather protectionist approach to IP which may even promote extraterritorial application of European IP standards.

[163] See, in particular, Matthias Leistner, 'The existing European IP rights system and the data economy – An overview with particular focus on data access and portability' in German Ministry of Justice and Consumer Protection and Max Planck Institute for Innovation and Competition (eds), Data Access, Consumer Interests and Public Welfare (Nomos: Baden-Baden 2021) 209, 221-231.

(269) Beyond this there are additional blind spots concerning intellectual property. The reference to intellectual property rights in Recital 17 appears rather obscure and ill-informed on IP law (para 29 above). In other contexts, IP issues are not addressed, although IP protection may decrease the effectiveness of the proposed rules. More attention should in particular be paid to the interface with copyright law. Data – in the form of digitised pictures, music, films etc – may enjoy copyright protection. In such cases, copyright law – not just the *sui generis* database right – could create obstacles to the exercise of data access and use rights. Another fundamental issue is potential copyright protection for software elements that may hinder interoperability. As regards the latter, this Position Statement has already elaborated on the challenges of potential copyright protection for application programming interfaces (APIs) in the context of Chapter VIII on interoperability (paras 223-225). As regards Article 11 concerning technical protection measures (TPMs), the Position Statement has recommended paying attention to the fact that circumvention of TPMs may be prohibited pursuant to EU copyright law, which in turn could limit the possibility of establishing interoperability with data held by others (para 118 above).

(270) In the following, a remaining issue of copyright law will be addressed, namely, the question whether copyright protection more generally, hence beyond *sui generis* database rights, could hinder the exercise of the data access and use right.

(271) A first sub-issue regards the potential availability of copyright protection for creative databases. At least in theory, a conflict between the new IoT data access and use right under Chapter II and copyright protection for databases is conceivable. In practical terms, however, one might tend to think that a dataset collecting IoT data will rarely meet the requirements for copyright protection. Conversely, the possibility of a conflict between the two disciplines is exacerbated by the very definition of data in Article 2(1) of the Proposal. Data are not only described as the digital representation of acts, facts or information, but also as 'any compilation thereof' (on this term see already para 57 above). This means that even an entire database may constitute the subject of the data access and use right under Article 4 of the Proposal. If such database were protected by copyright, the two regimes would enter into direct conflict, just as in the case of a *sui generis* protected database. While for the latter, Article 35 defines the relationship, for copyright-protected databases the relationship is left open at least in the operational part of the Proposal. Yet, although there is no general provision in the Proposal that safeguards intellectual property rights – as Article 20(4) GDPR does in the context of the portability right concerning personal data –, one should not assume that Chapter II will set aside copyright protection. The Commission argues that beyond Article 35 existing intellectual property law should be respected.[164]

[164] Impact Assessment Report, p 29.

Regarding the involved interests, under Article 4, even a duty of the data holder who holds a copyright in the data can hardly be argued in light of the fact that Article 4(1) requires the data holder to provide the data free of charge. Article 4 would thus amount to a denial of copyright protection.

(272) Still, the key question remains whether compilations of machine-generated (IoT) data can at all be eligible for copyright database protection. Article 1 Database Directive defines a database as 'a collection of independent works, data or other materials arranged in a systematic or methodical way and individually accessible by electronic or other means'. Accordingly, a large number of unsorted data fixed on a hard disk would qualify as a database if combined with database management software that arranges and enables retrieval of the stored data.[165] Furthermore, the threshold for a dataset to qualify as a copyright-protected database is rather low. Article 3(1) Database Directive requires that databases constitute 'by reason of the selection or arrangement of their contents … the author's own intellectual creation' to enjoy copyright protection. This originality standard was specified by the CJEU, which ruled that the selection or arrangement of data in a database should amount to an 'original expression of the creative freedom of its authors'.[166] It follows that whenever no room is left for creative choices, typically when data are arranged mechanically or according to choices linked to the mere functionality of the database (eg in alphabetical order), copyright protection will not arise. The CJEU has further clarified that the 'labour and skill' of the author are irrelevant for copyright protection.[167] However, national courts' interpretations of the concept of 'creative choice' as the benchmark for creative expressions may continue to differ. In most instances, courts will hence be most likely to ultimately deny copyright protection. Yet each and every case has to be assessed on its own merits. Copyright protection may be more likely if the dataset includes metadata (for instance, as is often the case in the health sector) or stored permanently (as compared to real-time data). In conclusion, even if the role copyright law will play in protecting IoT datasets, meta-data and other structuring elements of databases is not entirely clear yet, it is fair to say that copyright could play at least a potential role in protecting certain structures if the condition of making use of some room for personal creativity is met.

(273) Furthermore, this issue of copyright eligibility for IoT databases arises at a time when copyright protection is expanding. It is easy to imagine that once the *sui generis* database protection is 'excluded' for IoT databases pursuant to

[165] P Bernt Hugenholtz, 'Directive 96/9/EC - on the legal protection of databases' in Thomas Dreier and P Bernt Hugenholtz (eds), Concise European Copyright Law (Kluwer, 2nd ed 2016) 379, 390.

[166] Case C-604/10 *Football Dataco v Yahoo* ECLI:EU:C:2012:115, para 41. See also Matthias Leistner, 'Copyright at the interface between EU law and national law: definition of "work" and "right of communication to the public"' (2015) 10 JIPLP 626, 627.

[167] *Football Dataco* (n 166), para 42.

Article 35 of the Proposal, data holders will claim copyright protection strategically to counter requests for data access under Article 4, until courts get to decide such cases. Some national courts may also be more willing than others to expand copyright protection in this direction. Hence, the fragmentation of national law in interpreting the Database Directive with regard to copyright could also negatively impact the application of the Data Act, at least until the CJEU takes a position on the matter.

(274) Beyond databases, individual elements (images, sounds, audiovisual elements etc) could also qualify for protection. Many sensors embedded in IoT devices produce digital data of that kind. Of course, where IoT products automatically generate such data, the requirement of 'creative choices' should hardly be fulfilled. But this does not rule out that such elements, especially photographs as well as sound and audiovisual recordings, will be protected as the subject-matter of related rights. Indeed, typical examples of non-creative photographs as the subject-matter of related rights protection that are cited in the literature are photographs made automatically by cameras attached to planes or satellites.[168] Those photographs often have high commercial value and require investment. In such examples, there can be no doubt that the productions are also protected as 'data generated by the use of a product' in the sense of Article 4. In such cases, it matters enormously who will be considered the holder of the related right. The Commission assumes that the IoT data are co-generated by the manufacturer and the user of the product. However, the criteria that courts will apply with regard to related rights will not follow such data law concepts, which by their nature are just about to evolve, for identifying the producer of subject-matter that is protected in the form of related rights. Indeed, in copyright law, both practice and scholarship allocate the right to the person who has affixed the camera to the object in such a way that the camera can automatically generate the respective content.[169] In terms of Article 4 of the Proposal this would be the manufacturer (data holder) and not the user of the product.

(275) In sum, the implications for the Data Act are as follows: Copyright protection for creative databases and creative elements of datasets should not be easily set aside as in the case of the *sui generis* database protection, since copyright law protects the creativity expressed in the work and not just investment as the *sui generis* right does. Therefore, it is understandable that the Proposal limits Article 35 to the latter right. Still, a balancing between the data access regime and copyright protection should take place. For this, the exception for text and data mining, which was adopted as part of the Digital Single Market

[168] See Martin Vogel in Gerhard Schricker and Ulrich Loewenheim (eds), Urheberrecht (C.H.Beck, 6th ed, Munich 2020) § 72 para 24.

[169] See *Oberster Gerichtshof* (Austrian Supreme Court), Voralberg Online, (2001) Gewerblicher Rechtsschutz und Urheberrecht Internationaler Teil 351, 352-353 (on Austrian law); Vogel (n 168).

Directive, can provide some orientation.[170] It is now important to go ahead with the adoption of the Data Act, which should not be delayed because of problems whose likelihood to appear in practice is rather uncertain. Implementation of a special exception could still be part of future copyright legislation, although such reform will not be initiated in the foreseeable future.

(276) Instead, the EU legislature would have a better case to extend the application of the rule of Article 35 to other forms of related rights that protect non-creative photographs and sound and audiovisual recordings. Similar to the *sui generis* database right, those related rights only protect investment and, in the context of Chapter II, the holder of the right may well recoup this investment by charging a price for the product.

- **Trade secrets protection**

(277) In several provisions the Proposal seeks to safeguard the integrity of trade secrets protection. In particular, the Commission makes clear that the Data Act shall not affect trade secrets and that there is no general obligation to disclose trade secrets.[171] While the Institute agrees with this overall objective in the light of the importance of the protection of trade secrets for the functioning of the internal market in general and the data economy in particular, there is still a need to analyse the rules that are designed to coordinate data access rights with trade secrets protection.

(278) The Proposal includes two different types of rules for such coordination. On the one hand, there are Article 4(3) and Article 5(8) with more or less the same wording. On the other hand, Article 8(6) seems to go much further in safeguarding trade secrets protection. However, all of these rules create challenges, which the Commission may have simply ignored.

(279) The major challenge lies in the fact that it is often highly uncertain whether the legal requirements of trade secrets are fulfilled, or to put it differently, whether at a later stage a court will confirm trade secrets protection. As regards the question of whether certain information can be regarded a trade secret, Article 2(1) Trade Secrets Directive affirms that any information could in principle be protected as a trade secret. It is however for the holder of the information to take 'reasonable steps' to keep the information secret (Article 2(1)(c)). Whether the steps taken are 'reasonable' requires a balancing not least by taking account of the information's commercial value. The higher the commercial value, the more the holder of the information should be required to do to keep the information secret. Conversely, the requirement of commercial value of the information has to be the result of its being secret (Article 2(1)(b) Trade Secrets Directive). Most importantly, the information

[170] Arts 3 and 4 DSM Directive.
[171] Recital 28; Impact Assessment Report, p 29.

has to be 'secret', for which Article 2(1)(a) Trade Secrets Directive uses a rather vague standard in the sense that the information is 'not … known among or readily accessible to persons within the circles that normally deal with this kind of information.'

(280) The vagueness of these requirements needs to be taken account of when data holders enter into contracts on the sharing of data. Data holders may secure trade secrets protection by imposing confidentiality requirements on the data recipients which will contribute to and constitute one form of measures to keep the information secret. To secure trade secrets protection, it is no requirement that the information is actually designated as a trade secret. Given this vagueness and lack of legal certainty, the data holder will often claim 'ownership' in the data. However, the term 'ownership' is in need of interpretation. To the extent that the data will not be protected by intellectual property rights, the claiming of ownership cannot unilaterally make unauthorised use of the data by a third person illegal. In contrast, trade secrets protection can give rise to claims against third persons, but only does so based on contract-related criteria (Article 4(2)-(5) Trade Secrets Directive). If the requirements of trade secrets are not fulfilled, the data holder will at least be able to secure contractual claims against the data recipient. Hence, claiming 'ownership in data' may mean very different things. What it means requires a case-by-case assessment, and the parties will even themselves enter into the contract under considerable legal uncertainty. This uncertainty also characterises the practical benefit that trade secrets protection provides. This form of protection will prove its value in a situation of *ex post* assessment, namely, where the data holder goes to court to argue a case of an infringement of trade secrets against a third person. It will be for the court to decide *ex post* whether trade secrets protection is actually available in the particular case.

(281) The problem in the context of Articles 4(3), 5(8) and 8(6) lies in the need to assess whether there is a trade secret in an *ex ante* situation. This provides the data holder with considerable leeway to strategically claim trade secrets protection in negotiations with the data recipient (user) to limit its obligation to share data. Yet the provisions differ as regards their concrete effect.

(282) On the on hand, Articles 4(3) and 5(8) appear to strike an adequate balance. Both provisions empower the data holder to oblige the user and the third party, respectively, to accept confidentiality requirements. This corresponds to the logic of trade secrets protection that such confidentiality requirements shall be used to secure trade secrets protection in the first place. If the goal is to protect trade secrets in the framework of Articles 4 and 5, the data holder should be allowed to require confidentiality from the user and the third party in relation to yet other persons.

(283) However, the assessment of Article 8(6) has to be different. This provision provides the data holder with the possibility to refuse the sharing of data if

these data are protected as trade secrets. Here, to apply the law, a decision has to be made in an *ex ante* situation, namely, whether the data are protected as trade secrets or not. This provision opens the door for the data holder to strategically claim the existence of trade secrets to refuse the sharing of the data. Moreover, two different sets of cases have to be distinguished in this context. In the first case, the data holder claims to be the trade secret holder in the sense of Article 2(2) Trade Secrets Directive. In other cases, however, the data holder may only have received control over the data from another person who has imposed a confidentiality requirement. In this latter case, the situation of the data holder in the sense of Article 8 will be particularly uncomfortable. On the one hand, this person would not be allowed to grant access to the data if the data really constituted trade secrets. Such disclosure of the data would amount to an infringement of trade secrets protection pursuant to Article 4(3)(b) Trade Secrets Directive, which under national law may even constitute a criminal offence. If the data however did not qualify as trade secrets, the refusal to make the data available would be a contravention of the regime for data access with the risk of being sanctioned under the applicable rules.

(284) While it is true that Article 8(6) allows the EU and national legislation to deviate from the trade secrets defence, this should not justify inclusion of this unjustifiably broad defence in the Data Act. Therefore, the Institute recommends deleting Article 8(6). As regards the application of this provision in the context of Article 5 as proposed by the Commission, this rule would even be irreconcilable with Article 5(8). As regards obligations to make data available under other rules of EU law or national law, it should be for those laws to coordinate the requirements for the coordination of trade secrets protection with the data access regime. Yet for future EU legislation, the legislature is recommended to follow the approach of Articles 4(3) and 5(8). In the case of national laws, of course, it would be for the national legislature to provide for the necessary coordination. This should not be a concern from the perspective of EU law. The national legislature is still under a duty to respect the rules of the Trade Secrets Directive.

(285) Also, it should not be ignored that Article 3(2) Trade Secrets Directive explicitly states that the ‘acquisition, use or disclosure of a trade secret shall be considered lawful to the extent that such acquisition, use or disclosure is required or allowed by Union or national law.’ This means that, even as a matter of EU trade secrets law, a Member State is not at all required to safeguard trade secrets protection in the framework of national data access and use regimes. However, as Recital 18 Trade Secrets Directive explains, Article 3(2) Trade Secrets Directive should not exempt the data recipient from the obligation to keep the data confidential. This shows that national legislation can coordinate data access regimes with trade secrets protection

following the model of Articles 4(3) and 5(8) of the Data Act Proposal without violating the Trade Secrets Directive.

(286) Furthermore, the Institute wants to stress that the Commission is not really faithful to its premise that trade secrets protection should also be preserved in the context of data access regimes. Articles 4(3) and 5(8) can be described as systems for the compulsory licensing of trade secrets. Pursuant to the EU Trade Secrets Directive, trade secret holders are protected against unlawful disclosure, acquisition and use of trade secrets. Importantly, 'unlawful' can refer to the acts not authorised by the trade secret holder, irrespective of whether such acts are carried out 'contrary to honest commercial practices'.[172] In other words, the lawfulness of the acquisition, use and disclosure of a trade secret hinges on the authorisation of access by the trade secret holder.[173] If Articles 4 and 5 of the proposed Data Act are to be interpreted as subjecting trade secrets to compulsory data sharing, all these dimensions of trade secret protection would be, to some extent, curtailed, even if the confidentiality of trade secrets can be safeguarded. Consequently, the competitive advantage of the initial trade secret holder stemming from the discretion to authorise access to, acquisition and use of a trade secret would be diminished. This is recognised by the Impact Assessment Report, which states that, even though manufacturers will be able

> to continue exploiting data from products and rely on trade secrets protection [, …] they will have to respond to new requirements: for instance, they will no longer be able to assert their competitive advantage purely based on the exclusive control of data collected by products they manufacture [and] are likely to face more competition in aftermarket services, in which their position so far was difficult to challenge.[174]

(287) Here, one could go so far as to criticise the Commission for not having taken into account that the duty to license trade secrets could negatively affect the attainment of the pro-competitive objectives of trade secrets protection. However, such concerns have to be rejected. First, in the context of Articles 4 and 5, access to the data is required to serve the interest of the user and the interest in enhancing competition in the market for added value services. And second, such concerns would overlook the vagueness of the concept of a trade secret. To argue against a duty to share trade secrets would allow data holders to seek trade secrets for any data, at least to the extent that they are secret, to justify the decision to keep them secret. This would basically render any right of data access and use ineffective.

[172] Article 4(2)(a) and (b) Trade Secrets Directive.
[173] Article 4(2) and (3) Trade Secrets Directive.
[174] Impact Assessment Report, p 44.

(288) However, if the legislature decided – in contrast to what the Institute recommends – that Article 4 should allow the user to use the data for any purpose, Articles 4(3) and 5(8) would have to be criticised, since this would allow the user to share the data with myriads of other persons. Despite the availability of imposing confidentiality requirements on all those third-party data recipients, every act of disclosure to another person increases the risk that the trade secret will ultimately leak and the trade secrets holder will lose protection. Hence, it is important that the data access regime clearly define the purposes of the use of the data. Accordingly, the need to appropriately coordinate data access regimes with trade secrets protection also requires a purpose-bound approach as recommended here for the design of the IoT data access and use right.

(289) Finally, the Proposal also seeks to coordinate trade secrets protection in Chapter V concerning B2G data sharing. Pursuant to Article 17(2)(2), the (potential) existence of trade secrets protection does not exclude access of public sector bodies (PSBs) to the data. However, the wording of this provision is much more open-ended than Articles 4(3) and 5(8). In contrast, Recital 66 makes clear that Article 17(2)(c) should also require the PSB to ensure confidentiality. Therefore, the legislature is recommended to integrate an explicit statutory confidentiality requirement in the wording of Article 17(2).

(290) Trade secrets protection may also matter in other contexts of the Proposal where trade secrets protection is not mentioned. This holds especially true for the switching of data processing services under the rules of Chapter VI. In this context, two situations have to be distinguished. In the first situation, where the trade secrets holder decides to use data processing services to store and process data, it is for this person to secure trade secrets protection, requesting data security guarantees from the service provider. In the second situation, the customer of the service is the recipient of trade secrets and, accordingly, will have to respect confidentiality requirements contractually imposed on it by the trade secrets holder as a third party. Hence, it is in turn for the customer to request guarantees from the service providers that the storing or processing of the trade secrets in the context of providing data processing services, including the switching of providers for such services, do not violate its confidentiality obligations vis-à-vis the trade secrets holder. The fact that Chapter VI does not make any reference to trade secrets protection shows that the rules of the Trade Secrets Directive fully apply in this context. This also means that in the second situation it is a matter of the agreement with the third-party trade secrets holder whether trade secrets can legally be stored on a cloud and whether the recipient is allowed to switch to another cloud services provider under the rules of Chapter VI. This also shows that, quite rightly, Chapter VI does not seek to put the legal regime of trade secrets protection

aside solely for the purpose of promoting the development of the market for data processing services.

- **Protection of personal data**

(291) One of the biggest challenges for the legislature concerns the coordination of the rules of the Data Act with data protection law. The Institute welcomes the fact that the Proposal does not selectively provide rules for non-personal data. In many real-life situations and sectors, both personal and non-personal data are simultaneously generated and used and distinguishing between the two is often practically impossible. Hence, especially horizontal rules should in principle address both categories of data, while at the same time safeguarding the right to data protection of data subjects. The latter may also lead to the need to apply the regime of data protection law to entire datasets for which it is not possible to distinguish between different types of data. In the light of this, the Proposal needs to be analysed more specifically where it provides for rules that exclusively apply to non-personal data and thereby may deviate from data protection rules. In the worst case, this may lead to conflicting obligations that an addressee cannot fulfil at the same time.

(292) While it may seem that the Data Act and data protection law promote conflicting objectives – with the Data Act aiming at promoting data sharing and data protection law guaranteeing control of the data by the data subject – in many regards the two fields are complementary. In particular, IoT devices often collect personal data from the user, and the users as data subjects may especially be interested in accessing and porting these data. More generally, data protection is not opposed to data sharing as such, even where the recipient may be a third person. Where consent by the data subject is required for such sharing, such consent has an enabling function. It allows the data subject to make use of data, including commercial use, in her or his own interest by sharing the data. Anonymisation can convert personal data to non-personal data and can further enhance the use of data by third parties.

(293) The Proposal builds on these insights. Recital 31 acknowledges the close link of the data access and use right of Chapter II with the data portability right of Article 20 GDPR. There, the Proposal explicitly states that the new rules are meant to ‘complement’ Article 20 GDPR. This may mean many things. First, Recital 31 confirms that Article 20 GDPR continues to apply in the context of Article 4. Secondly, however, the stated complementarity does not automatically answer the question of whether Articles 4 and 5 create overlapping regimes in addition to Article 20 GDPR or whether the new provisions should only apply to non-personal data. In any instance, there is an obvious need of coordination. The operational rules of Chapter II adopt a selective approach: In principle, they also apply to personal data. However, to coordinate the two sets of rules, the Proposal restricts the application of some

of its rules (see Article 4(6)) to non-personal data and ensures that others (see Article 4(5)) will respect the principles of the GDPR.

(294) To assess whether this coordination achieves optimal results, the main elements of the two regimes need to be looked at more closely, namely, (a) the types of data covered, (b) the legal basis for processing and (c) technical feasibility, transmission and re-use of data. In Recital 31, the Proposal only seems to mention the first two, by setting out that the IoT access and use right to data should apply 'irrespective of its nature as personal data, of the distinction between actively provided or passively observed data, and irrespective of the legal basis of processing'.

(295) As regards the types of data, it is appreciated that the Commission explicitly includes observed data within the access right under the Data Act. Here, the Data Act Proposal is clearer than the GDPR, where Article 20(1) only stipulates that the portability right applies to data 'provided by' the data subject. This launched an immediate discussion whether 'observed' data, such as information about the physical conditions of the user collected by a fitness tracker, should be covered. In the light of the recent development of IoT products, commentators immediately claimed that this should be the case and were finally seconded by the European Data Protection Board in its Guidelines according to which observed data should also be covered by Art. 20 GDPR.[175] Recital 31 quite rightly confirms this reading for the Data Act. One may still bemoan the fact that observed data is not mentioned in the Proposal's operational part. However, it should be sufficiently clear that personal data generated by the use of an IoT product will typically be 'observed data'.

(296) As regards Article 20(1) GDPR, it is generally held that this provision does not cover derived or inferred data. Recital 14 of the Proposal supports the same for the right of Chapter II. However, as argued above, this Position Statement proposes that it go further under the recommended purpose-bound approach to also cover derived and inferred data where this is necessary to enable added value uses and services. Such derived and inferred data can of course also be personal data. This means that the data access and use right of Chapter II, not distinguishing between personal and non-personal data, may cover a larger body of personal data than the data portability right of the GDPR.

(297) A data controller is allowed to process personal data to the extent that Articles 6 and 9 GDPR provide a legal basis for such processing. In contrast, pursuant

[175] European Data Protection Board, 'Guidelines on data subject rights – Right of access' (01/2022), p 31. The former WP29, now EDPB, already in 2017 stated that observed data shall be understood as part of 'provided data' and hence, it should be covered by the Right to Data Portability under Art. 20 GDPR. See WP29, 'Guidelines on the right to data portability' (2017) WP242, p 9-10.

to Article 20(1)(a) GDPR, the data portability right is limited to cases where the processing is based on the data subject's consent pursuant to Article 6(1)(a) or a contract pursuant to Article 6(1)(b) GDPR. In the case of the use of an IoT product, there should typically be a contract with the user concerning the sale, rental or lease of the product, which requires the manufacturer to enable the use of the product. However, for the exercise of the data access and use right of Chapter II of the Proposal such an agreement is not an absolute requirement. This would mean that even in cases where a user has not given her or his consent and there is no direct or indirect contractual relationship, the user can also claim access to personal data under Chapter II while Article 20 GDPR would not apply. Hence, also in this regard, the Data Act would go beyond what the data portability right of Article 20 GDPR requires.

(298) Under Articles 6 and 9 GDPR a data controller can be allowed to use personal data without any consent given by the data subject or a contract with the data subject. Such cases cannot be excluded with regard to IoT data. For instance, Article 6(1)(d) GDPR allows for data processing in the vital interest of the data subject or of another natural person. This could authorise the data holder to use the data of a smart fitness tracker to protect the health of the data subject/user. In this regard, the more restrictive Article 4(6), 1st sentence, requiring a contractual agreement given by the user, is truly astonishing. This could prevent the manufacturer of a motor vehicle from using the technical data of the car to protect third parties who may be harmed through the operation of the vehicle. This is yet another reason for deleting this requirement of a contractual agreement for non-personal data. Where personal and non-personal data included in the same dataset cannot be separated, the rules of the GDPR sufficiently set the standard for use restrictions. No additional restrictions are justified for non-personal data, except where data are protected under IP or trade secrets law.

(299) One big limitation to the working of the right to have the data directly transferred to another data controller under Article 20(2) GDPR is that it will only apply if the transfer is 'technically feasible'. This is underlined by Recital 68 GDPR, which states that Article 20 GDPR creates no 'obligation for the controllers to adopt or maintain processing systems which are technically compatible'. Direct portability has therefore failed to function correctly on account of two reasons: Firstly, data controllers ('data holders' under the Data Act Proposal) have denied portability for reasons of technical feasibility. Secondly, the other data controller ('data recipient' under Chapter III of the Data Act Proposal) is not obliged to accept the data subject's ('user' under the Data Act Proposal) data from the first data controller ('data holder' under the Data Act Proposal).

(300) Recital 31 states that unlike Article 20 GDPR, the Act 'mandates and ensures the technical feasibility of third-party access for all types of data coming within its scope, whether personal or non-personal'. Thereby, the Recitals seem to go beyond Article 20(2) GDPR as regards the technical provision of the data. However, this is not mirrored in the operational part of the Proposal. Neither Article 4 nor Article 5 contain a binding rule guaranteeing technical feasibility as contained in Recital 31. In addition, Article 5(1) of the proposal does not explain the concrete technical means needed to make the data available in a continuous manner and in real time. Under settled CJEU case-law, recitals have no binding legal force.[176] Thus, they do not have an autonomous legal effect when there is no counterpart within the legal act's operative provisions. This may leave us with the same problem that Article 20 GDPR presented for effective portability.

(301) For this reason, the legislature is recommended to take a more ambitious approach. What is missing are obligations for the data holder to guarantee interoperability. Such rules are provided for in Chapter VIII for operators of data spaces, providers of data processing services and vendors of smart contracts. Hence, interoperability requirements as obligations of data holders that control IoT data are missing in both Chapters II and VIII. The Institute admits that since manufacturers of IoT products belong to very different sectors and IoT products generate data in very different formats, setting up generally applicable requirements for interoperability may pose a particular challenge. Yet this does not have to mean that such requirements cannot yet be formulated at all for IoT products. It seems that the requirements as formulated in particular for the technical means in Article 28(1)(c) would also be suitable for IoT products (see para 219 above). If the legislature does not want to take this road, it should at least import the wording from Article 20(1) GDPR to Articles 4(1) and 5(1) and provide that data have to be made available in a 'structured, commonly available and machine-readable format'. As regards the technological requirements for data access, the IoT data access and use right should at least be as advanced as the data portability right of the GDPR.

(302) Another central feature of the legal regime for IoT data is the data minimisation principle regarding personal data as set out by Article 5(1)(c) GDPR. In the context of IoT products, this principle limits the possibilities of the data holder (manufacturer) to collect personal data from the user of the product. Recital 8 of the Data Act Proposal seems to confirm the relevance of the data minimisation principle for the Data Act, albeit in the context of how important it is to make use of technical and organisational means to guarantee adherence to it. The principle itself, however, has not entered the text of Article 4. There, Article 4(6) defines the extent to which the data holder can make use of the data, however only with regard to non-personal data. This

[176] Case C-315/20 *Regione Veneto* ECLI:EU:C:2021:912, para 28.

shows that Article 4 does not provide a full picture of the rights and obligations between the data holder and the user. This may be considered unfortunate. While it is true that the application of the GDPR is fully guaranteed by Article 1(3), Article 6(1) regarding the obligation of the third party vis-à-vis the user explicitly mentions the obligations arising from the GDPR. As a matter of clarity, the Institute therefore recommends adding another sentence to Article 4(6), where the data minimisation principle should also be mentioned. While it is true that Article 6(1) does not specifically refer to data minimisation, its respect is more important as regards the obligations of the data holder vis-à-vis the user. The sentence could have the following wording:

> The data holder shall only use personal data of the user subject to the rights of the data subject and the respect of the principle of data minimisation in particular, and shall delete the data when they are no longer necessary for the purpose.

(303) The data minimisation principle is also mentioned in Recital 34, although without clearly referring to personal data. This recital sets out an additional obligation not mentioned in Article 5 according to which the third party should only 'access additional information that is necessary for the provision of a service requested by the user'. The meaning of this formula is rather opaque. It obviously is supposed to refer to Article 6(1) regarding the relationship of the third party with the user. It may well be that the third party as a service provider is in need of additional data, ie beyond the data the data holder is required to make available in order to provide its service. Hence, this would be data to be provided by the user directly. However, it would be for the user and the data holder to clarify the extent to which additional data shall be delivered as part of their contract. The general reference Recital 34 makes to the data minimisation principle is misplaced. It does not and should not apply as regards non-personal data, since the sharing of such data should in principle be promoted – at least where such sharing does not enter into a conflict with intellectual property and trade secrets protection. At best, reference to the data minimisation principle could be included in the text of Article 6(1) with regard to personal data as proposed (para 302 above) for the text of Article 4(6). Equally, the first sentence of Recital 34 should be deleted.

(304) Safeguarding principles of data protection law may lead to problems where datasets include both personal and non-personal data. This necessarily requires a balanced approach that does not conflict with data protection rules, but still promotes data sharing. However, unlike Articles 4(3) and 5(8) regarding trade secrets protection, the Proposal does not provide any particular approach to coordinating data protection with data access and use rights. The Institute recommends that the legislature go further based on a risk-based approach. This approach would be in compliance with the GDPR.

Article 24(1) GDPR requires controllers to take the 'nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons' into consideration when processing personal data.

(305) This risk-based approach should hence apply where the requested data is mixed. It requires a balancing of the risk for the data subject with the interests of the data recipient in access to data. To minimise the risk the following principles should be followed: As a general rule, the recipient should not obtain access to personal data that are not needed. This corresponds to the principle of data minimisation. Moreover, data subjects should not be 'tricked' into consenting to personal data processing against their will. In this regard, Article 6(2)(a) and (b) of the Proposal takes the right approach to exclude the use of so-called dark patterns. Furthermore, there has to be a legal basis for the processing of personal data. On the assumption that Articles 5 and 6 will only apply to third parties that provide the user with an added value service, Article 6(1)(a) or (b) GDPR will indeed typically offer such a legal basis for processing personal data of the user.

(306) More complicated are cases where the data protection rights of persons other than the user of the product are involved. For these cases, Articles 4(5) and 5(6) require a legal basis under the GDPR for making the personal data available. However, getting consent from such a third person, for instance a by-stander in a machine-generated photograph, may often not be possible. In such cases, there is a clear risk that the data holder will invoke the absence of consent of the data subject to deny data access. This raises the question whether it would be possible to consider an alternative risk-based approach to cater for both the data protection interest and the interest in accessing the data.

(307) In case of third-party data subjects the first question is whether the data will make the person identifiable and thus qualify as personal data. For this requirement, the CJEU has set the benchmark very low, by holding that it will suffice that the data controller holds additional data which is reasonably likely to be used in combination to identify the data subject.[177] To enable data access in such cases, the data holder would have to apply techniques that reduce the likelihood that such data can be used for identifying the person, including anonymisation in particular. In general, the risk-based approach requires taking account of both the likelihood of (re-)identification of the data subject and how severe the implications of the (re-)identification are. Such balancing will crucially depend on the semantics of the data. For health data, processing requires explicit consent pursuant to Article 9(2)(a) GDPR. Therefore, anonymisation also needs to be effective. For mobility data, in contrast, the legitimate interest clause of Article 6(1)(f) GDPR may be sufficient to justify a certain risk of (re-)identification. For agricultural data, both the risk of

[177] C-582/14 *Breyer* ECLI:EU:C:2016:779, para 45.

(re-)identification of the farmer and the severity of the implications of the identification for the farmer are low, which means that a higher likelihood of identification can be accepted. The remaining question however is who ought to assess these requirements. First, one would think of the data holder. Yet the data holder may not have any interest in making the data accessible. Nor, under Article 4(1), can the data holder claim compensation for the additional costs caused by anonymisation. Hence, the data holder would have strong incentives to rely on data protection rights of third persons to deny data sharing under Articles 4 and 5 of the Proposal. Thus, the data recipient is the more appropriate party to undertake the balancing exercise.

(308) What does this mean for the rules of the Data Act? It is true that the application of the risk-based approach as just explained can fully be applied against the backdrop of Articles 1(3), 4(5) and 5(6) of the Proposal without requiring any revisions to the proposed rules. However, if the text remains as it stands, the Data Act will not provide any guidance on how better coordination can be achieved. Therefore, the Institute recommends that the European Data Protection Board (EDPB) launch an initiative to draft new guidelines on the protection and use of third-party personal data in the context of data access rules. This work should be done in close contact with the Commission, to take account of the interest in promoting data sharing, and should start as soon as possible so that the legislature can already refer to such rules within the Recitals to the Data Act as guidance for interpreting Articles 4(5) and 5(6).

(309) Article 5(1) Data Act refers to sharing data with third parties upon request by a user. The access request can also be exercised 'by a party acting on behalf of a user'. It is unclear whether data intermediaries are considered such parties acting on behalf of the user as they are not mentioned in the recitals of the Data Act. Since data intermediaries can play a valuable role to ensure compliance with the GDPR, the legislature should explicitly confirm in the recitals that such intermediaries should qualify as such third persons.

XII. Cross-border application of the Data Act

(310) Apart from Chapter VII (Article 27), which explicitly addresses data sharing in relation to states outside the EU, the Proposal does not specifically address scenarios that regard the application of the Data Act in cross-border situations. Yet it is equally clear that the application of the Act is in need of being clarified as regards transnational cases. For the purpose of delineating the territorial application of the Act, the Commission has proposed Article 1(2).

(311) Article 1(2) raises complex issues, not only with regard to the interpretation of the concrete rules, but even more with regard to their legal nature. As regards the latter, the problem is that the fundamental approaches to defining

the geographic scope of the Data Act will differ considerably depending on whether the Data Act is enforced by the competent authorities under Article 31 or by the courts in the context of private litigation. As a principle of public international law, administrative enforcement of the Act should be governed by the principle of territoriality. It seems that Article 1(2) delineates the scope of application of the Act especially for the purpose of public enforcement. However, where courts decide on private law disputes, courts identify the applicable law according to generally applicable choice-of-law rules of their national law (the *lex fori*), which may lead to the application of a foreign law. In this regard, the question has to arise whether Article 1(2) also contains implicit choice-of-law rules that may even depart from existing and generally applicable EU and national choice-of-law rules. Neither the operational part nor the recitals of the Proposal address the private international law dimension of the Act. Against this backdrop, it would be fair to assume that Article 1(2) does not have the purpose of changing existing private international law. However, one should also take into account that there is of course a strong interest in making the same national law apply irrespective of whether the law is applied in a public (administrative) law context or by the courts deciding on private law disputes. The market participants need to know whether they are supposed to follow the rules of the Act or not, as they cannot know whether they will later be exposed to public enforcement or sued by another party before a national court.

(312) An analysis of the potential implication of the rules of Article 1(2) for private international law depends on a proper understanding of the provisions of Article 1(2). Therefore, the following comments will first analyse the provisions of Article 1(2). Indeed, the text of these provisions presents several uncertainties that deserve to be clarified. What those rules mean from the perspective of private international law will be discussed in the second sub-part.

- **Cross-border application of the Act pursuant to Article 1(2)**

(313) The way the specific rules of Article 1(2) are phrased differs considerably from choice-of-law rules. The latter designate the law applicable to a specific legal issue, such as contractual or non-contractual obligations, and may lead to the application of a specific foreign law. Article 1(2), on the other hand, only regulates the application of the Data Act unilaterally, and it does so by distinguishing between different addressees of the Act. Thereby Article 1(2) chooses a regulatory (public law) approach to delineate its application.

(314) The rules of Article 1(2) in their entirety present a number of uncertainties. First, they refer to persons and not to the specific provisions of the Proposal. This immediately highlights the fact that there is a need to explore in more detail how Article 1(2) influences the applicability of the following Chapters of the Proposal. In addition, it is not clear whether the persons mentioned in

Article 1(2) are referred to as addressees of obligations under the Act or also as rightholders. The former is the more likely interpretation since the primary purpose of the provision seems to be to define the territorial scope of the Data Act in the context of public enforcement, for which measures and sanctions with extraterritorial reach should be avoided.

(315) What seems clear is that Article 1(2)(a) governs the application of Article 3. This provision does not explicitly mention the 'manufacturer' as the addressee of the provision, but the provision does regulate the design of the product and the information that has to accompany the product. As regards the criterion for application, to apply Article 3 of the Proposal under the condition that the product has been placed on the market in the Union makes perfect sense.

(316) Uncertainties relate in particular to Articles 4 and 5. On the one hand, one would expect that the territorial scope of application of the data access and use right should be the same for all provisions of Chapter II. However, 'data holder', the term used in Article 1(2)(b), and not 'manufacturer' is used in Articles 4 and 5 to designate the person who is under an obligation to make data available. This seems to argue for the delineation of the geographic scope of both Articles 4 and 5 according to Article 1(2)(b). However, this latter provision does not fit Article 4. Article 1(2)(b) provides that the Data Act should apply when data are made available to a 'recipient' in the EU. Yet Article 4 requires a making available to the 'user', while Article 2(7) explicitly excludes the 'user' form the definition of the 'data recipient', which is the term used in Article 1(2)(b). Taking into account that the data holder as defined in Article 2(6) will typically be the manufacturer in cases where Articles 4 and 5 apply, it seems therefore more appropriate to assume that the applicability of Articles 4 and 5 is equally governed by Article 1(2)(a). Whether to apply Article 1(2)(a) and not Article 1(2)(b) matters enormously. Application of the former would lead to continued application of the Act also in cases where the owner of an IoT product moves to a country outside the EU with the product or where the product is sold to another person living in a non-EU country.

(317) In contrast, Article 1(2)(b) should be considered to govern the applicability of Article 8, including where this provision applies to a third party in the sense of Article 5. There can be no doubt in this regard since the notion of a 'data recipient' explicitly includes third persons in the sense of Article 5. This means that for a product that was placed on the market in the EU, a user can claim the right of Articles 4 and 5 even if this user is not physically present in the EU. However, a user has no right to claim a making available of the data to a provider (third party) of an added value service that is established outside of the EU territory. This seems to be excluded by Article 1(2)(b).

(318) One may wonder whether Article 1(2)(c) is not redundant in relation to lit (b). The existence of this rule may be explained by the fact that the Proposal also

includes obligations of the data recipient, such as in Article 6, which regulates obligations vis-à-vis the user and not the data holder. Hence, Article 1(2)(b) cannot be applied for defining the scope of application of Article 6.

(319) It has to be noted that the criteria mentioned in Article 1(2)(b) and (c) are not sufficiently clear. Both rules require that the data recipient be in the European Union. This could either be a requirement of habitual residence or – in case of a natural person – actual presence at the time of receiving the data. The legislature should make this point clearer at least in the Recitals. It can be assumed that the latter interpretation is the intended one. Yet the former would seem preferable since it would guarantee identical rules irrespective of whether the data recipient is a natural or a legal person. In case of a legal person as a data recipient the Data Act should apply if the central administration is located within the EU. In parallel to this, relying on the habitual residence of a natural person lends sufficient stability and legal certainty to the applicability of the Act. Therefore, it is recommended that the habitual residence should be mentioned both in Article 1(2)(b) and (c), using the wording: '… data recipients with their habitual residence in the Union'. In EU choice-of-law rules the habitual residence of a legal person is typically defined as the place of its central administration.[178]

(320) An open question is whether Article 1(2) regulates at all the application of the Data Act to contracts that are concluded in the framework of Chapters II, III and IV. This issue is most relevant as regards Chapter IV. Article 13 uses neither the terms of 'data holder' nor 'recipient', so that it is not clear whether and which sub-rule of Article 1(2) should apply. One possible interpretation is that it should be left to the choice-of-law rules of private international law to designate the applicable national contract rules. If the law of an EU Member State applies, then the Chapter IV will also apply. Such reading is strongly recommended because it helps to coordinate the scope of application of the Data Act with private international law. This would mean, if the legislature decides that public enforcement under Chapter XI should also apply to Chapter IV, the competent authority should only have power to enforce Article 13 if this provision is applicable pursuant to the rules of the Rome I Regulation.

(321) Article 1(2)(e) delineates the application of the Data Act as regards the providers of data processing services. In this rule, the criterion should equally be made clear in the sense that the Data Act applies to 'customers with their habitual residence in the Union'.

[178] See, for instance, Art 19(1)(1) Regulation (EC) No 593/2008 of the European Parliament and of the Council of 17 June 2008 on the law applicable to contractual obligations (Rome I), [2008] OJ L 177/6.

(322) However, there is no rule regarding the application of the Data Act to operators of data spaces (Article 28) and vendors of smart contracts (Article 30), while such a rule seems to be necessary. Here, the legislature could consider taking Article 1(2)(e) as a model.

- **Private international law**

(323) As mentioned further above (para 311), the Proposal is silent on the private international law aspects of its application. This raises the question of whether the rules of Article 1(2) also contain choice-of-law rules that designate the national law that is applicable to the rights and obligations among private parties. To answer this question, several considerations play a role: First, the provisions of Article 1(2) only address the application of the future Data Act. They do not generally define which national law will apply in private law matters, requiring a court to eventually apply the law of a state outside the European Union. Second, Article 1(2) does not distinguish among different legal issues and fields of law as choice-of-law rules would do. It does not designate the applicable law for contractual matters, intellectual property, trade secrets law or, in particular, the rights of data access and use. Third, the Data Act does not comprehensively regulate all aspects of private law. The rules of the Data Act with a private law dimension will rather have to be applied by taking account of the embeddedness of the Data Act within the applicable national law. This is especially true as regards contract law. Hence, Article 1 cannot set aside the applicable choice-of-law rules for identifying the applicable contract law, which may be the law of an EU Member State or the one of another state. Fourthly, it does not seem to be the intention of the Proposal to change existing choice-of-law rules. This has already been discussed with regard to intellectual property and trade secrets protection in the context of Chapter VII (para 213 above).

(324) In light of these considerations, the legislature may well be advised to clarify, at least by including an additional recital, that the provisions of the Act 'are without prejudice to the rules of private international law relating to conflicts of law and the jurisdiction of courts'.[179]

(325) However, this should not be done without assessing whether the results of such clarification would produce – in the interaction with the application of the rules of Article 1(2) – appropriate results. If it is true that Article 1(2) does not contain conflict-of-law rules, this would not mean that private international law can be ignored. Quite to the contrary, in private law matters,

[179] Excerpted from Recital 56 Directive 2014/26/EU of the European Parliament and of the Council of 26 February 2014 on collective management of copyright and related rights and multi-territorial licensing of rights in musical works for online use in the internal market, [2014] OJ L 84/72. This Directive is a very suitable example because it also provides for administrative enforcement of the rules, which frequently have an administrative and private law dimension, by national authorities, while not addressing questions of private enforcement.

the question of what law applies in cross-border cases is unavoidable and will have to be answered by the choice-of-law rules of the competent court. Hence, where a national court of an EU Member State has jurisdiction, this court will have to identify the applicable law according to the choice of law rules of the EU, such as the Rome I[180] and Rome II Regulation[181] on the law applicable to contractual matters and non-contractual obligations, respectively. If no EU rules are available, the court would turn to its national choice-of-law rules. Only if these rules designate the applicability of the law of an EU Member State would the Data Act also apply provided that the requirements of Article 1(2) are also fulfilled. This may have the consequence that the rules of the Data Act will not apply, although the rules of Article 1(2) are fulfilled, simply because the applicable law is not the that of an EU Member State. This would lead to a disconnect of the applicability of the rules of the Data Act depending on whether the specific case arises in the framework of public or private enforcement. To address such cases, one would either have to adapt the choice-of-law rules or the rules of Article 1(2) of the Proposal.

(326) As regards the choice-of-law rules, the problem in the context of Chapters II and III is that statutory data access rights are a novelty not only for private law but also, and even more so, for private international law. However, the absence of concrete choice of law rules for such rights does not mean that existing choice-of-law rules would not apply. The question rather is whether such statutory data access rights can be characterised in such a way as to fall under existing rules. This had already been argued before the submission of the Data Act Proposal for the case of a new IoT data access and use right with the argument that – especially if the right followed a fairness and purpose-bound approach – this right should be characterised as belonging to fair trading law (unfair competition law), including for the purposes of private international law.[182] According to Article 6(1) Rome II Regulation this would lead to the application of the law of the country 'where the competitive relations or the collective interests of consumers are, or are likely to be affected'. For the IoT access and use right this would be the law of the country where the product first entered the end-user market under the control of the manufacturer.[183] This is basically the same criterion as used in Article 1(2)(a). Hence, for the IoT data access and use right, both Article 1(2) and EU choice-of-law rules coincide.

(327) As mentioned above (para 74), data accessibility by default as required by Article 3 of the Proposal will also have implications for contract law. However, Article 3 does not directly regulate contractual liability. Hence, identifying the applicable contract law pursuant to the rules of the Rome I

[180] Rome I Regulation (n 178).
[181] Rome II Regulation (n 122).
[182] Drexl (2021) (n 6) 519-522.
[183] Ibid, 522.

Regulation would not enter into conflict with Article 1(2)(a) Proposal. In this context Article 6(1) Rome I Regulation guarantees the application of the mandatory rules of the Sale of Goods Directive for a consumer with habitual residence in the EU as regards data accessibility by default according to Article 3 of the Proposal as an element of the conformity with the contract for products that are sold to this consumer in a Member State of the EU. Hence, the applicability of EU mandatory consumer law should typically coincide with the applicability of the Data Act regarding Article 3 pursuant to Article 2(1)(a) of the Proposal.

(328) Article 1(2)(b) and (c) makes Chapter III and Article 6 in Chapter II applicable to data holders and data recipients under the conditions that the data are made available to the latter within the EU. Thus, this rule gives precedence to the interest of the data recipient in having its national law applied vis-à-vis the data holder, which seems to be justified at least in the context of Chapter III by the fact that these are rights of the data recipient. From a perspective of private international law, it is not so easy to characterise the provisions of Chapter III. Articles 8 and 9 stand between contract law and the statutory rights of data access and use. In particular, Article 8(1) seems to impose a statutory obligation on the data holder to license on FRAND terms. But Article 8(2) equally requires the data holder to conclude a contract that fixes the concrete terms of the access. Even such duty to enter into a contract should be characterised as a statutory duty and not an obligation arising from a contract. This argues against a characterisation as contract law. Thus, the Rome I Regulation would not apply. Whether there are other choice-of-law rules available would have to be decided for the specific statutory access right. To the extent that Article 8 also applies in the context of Article 5 concerning the IoT data access and use right, it would seem appropriate to apply the law of the state where the IoT device first entered the end-user markets. The reason is the accessory character of Articles 5 and 6 to the IoT data access and use right of Article 4. The same law should apply to all these rights. For the same reason, application of the Data Act to such situation should be delineated according to Article 1(2)(a) and not (b) and (c).

(329) As mentioned (para 320), Article 1(2) leaves open the applicability of the contract law provision of Chapter IV. This decision has to be welcomed in particular since it avoids a conflict between the applicable law identified by a court in the EU based on the Rome I Regulation and Article 1(2). As regards the application of the Rome I Regulation, it is to be noted that despite the fact that Article 13(8) establishes Chapter IV as mandatory contract law, an opting out of the rules of Chapter IV will be possible pursuant to Article 3(1) Rome I Regulation. Because of this, consumers with a habitual residence in the EU will continue to be better protected under the rules of the Unfair Contract Terms Directive, whose cross-border application will be guaranteed by Article 6(2) Rome I Regulation provided that the other party conducts its

business in or directs its activities to the country of the habitual residence of the consumer. In contrast, this choice-of-law rule will not apply to Chapter III of the Data Act Proposal. Here, the general principle of private international law applies according to which the parties can opt out of the application of mandatory law by agreeing on the application of a different law if the applicable choice-of-law rules do not provide otherwise. To protect businesses vis-à-vis their business partners against opting out of Chapter IV is an issue that the EU legislature could consider in the framework of a future revision of the Rome I Regulation.

(330) In the Data Act Proposal, contract law is not limited to the rules of Chapter IV. Following the principle that private international law should not be changed by the Data Act, this would mean that in all other such instances the parties will remain free to choose the applicable law to the extent that this is allowed under the Rome I Regulation. This however raises a question of characterisation. Especially Chapter VI on the switching of data processing services contains rules with a contractual dimension. Article 23(1) orders such service providers to remove 'commercial, technical, *contractual* and organisational obstacles to switching'. Article 24(1) requires service providers to 'clearly set out [specific rules] in a written contract'. These rules are formulated as legal 'obligations' – a term explicitly used in Article 24(1) – rather than directly applicable contract rules whose application parties may not exclude.[184] These obligations can in principle be enforced by the competent national authorities. However, this does not answer the question of what this means for private enforcement. Excluding private enforcement in this context would not be appropriate in the light of guaranteeing full effectiveness of EU law. To argue that there is only a right of the customer to claim the inclusion of the terms in the contract as required by Article 24 would unnecessarily complicate private enforcement where the parties have already concluded a contract. At least some of the rules could indeed be directly applied, such as Article 24(1)(c) requiring a minimum term of 30 calendar days for data retrieval. In contrast to this, Article 24(1)(b), requiring an exhaustive specification of all data and application categories that are exportable, could not be directly applied as a mandatory contract rule. As a baseline it is possible to consider all these rules, whether they are fit for direct application or not, as legal obligations of the service provider in the sense of a legal right of the customer to switch the provider similar to the legal data access and use right under Article 4, requiring the conclusion of a contract to exercise to switch the service provider. This allows for a differentiation. Where a contract has not yet been concluded, the Rome I Regulation should not apply. According to its Article 1(1), this Regulation only applies to contractual obligations and not to a legal obligation to enter into a contract. Nor do its Articles 10 and 11, regarding its application to the existence and

[184] Compare Art 13(8) Data Act Proposal.

validity of the contract, lead to the conclusion that a duty to license on particular terms would fall under the Regulation. Since current private international law does not provide for a specific choice-of-law rule yet, it makes perfect sense for courts in the EU to apply the law of the country where the service provider has its habitual residence. This rule does not only guarantee that private law courts will apply the Data Act in the same situations as the public authorities pursuant to Article 1(2)(e) of the Proposal. As a matter of Article 4(1)(b) Rome I Regulation, this law will also apply as the applicable contract law (the law of the service provider's domicile) if the parties do not choose a different law. If a court has to decide on the interpretation and enforcement of an already concluded contract, the Rome I Regulation necessarily provides the rules for identifying the applicable contract law. This means that the parties are not prevented from agreeing on another law. In such an instance, the national authorities can still enforce the rules of the Data Act. In addition, in the case that the recipient has its habitual residence in a non-EU Member State which provides for different obligations than Chapter VI of the Data Act Proposal, private international law should not prevent the service provider in the EU from agreeing on the application of the law of the customer's domicile.

(331) Based on the proposed clarification that the Data Act should not influence the applicability of existing rules of private international law, it should further be noted that what has just been explained with regard to Chapter IV also applies to all additional contract law rules of the Act. This especially includes the mandatory contract rules imposed on the providers of data processing services pursuant to Article 24. Hence, here as well providers from outside the European Union could in their contracts opt out of the application of Article 24. Whether the same applies to Article 23 is less clear since this provision obliges providers to remove contractual and non-contractual restrictions. Hence, a differentiation may be needed in this regard. One may wonder whether, in the light of Article 1(2)(e) of the Proposal, the Commission indeed was aware that such contractual opting-out of Article 24 could occur under the Rome I Regulation. However, here, one may still live with the interpretation that Article 1(2)(e) seeks to impose the contractual rules of Article 24 on service providers that offer services to customers in the EU, although these in turn could only be enforced by the national authorities. The text of Article 24 would even support such reading since the contract rules are drafted as an obligation of the service providers to include certain clauses in the contract. For the sake of guaranteeing the full effectiveness of Article 24, this should not prevent private law courts from applying Article 24 directly where the applicable contract law is that of an EU Member State.

(332) To conclude, it is possible to apply Article 1(2) of the Proposal in a meaningful way based on the applicable choice-of-law rules. Hence, the legislature should indeed clarify that the Act does not provide any rules of

private international law, thereby implicitly confirming that the generally applicable choice-of-law rules apply as regards the Data Act.

XIII. Future EU policy on promoting innovation in the data economy

(333) By facilitating access to and use of the IoT data in Chapter II, the Data Act aspires to 'stimulate innovation on aftermarkets [and] the development of entirely novel services making use of the data, including based on data from a variety of products or related services'.[185] The Institute is not convinced that the proposed IoT data access and data sharing regime can be used as an efficient means to make IoT data more broadly available to enhance data-driven innovation in any given context. The better solution therefore consists in a clearer distinction between two types of innovation – innovation as regards added value (aftermarket) services, on the one hand, and broader data-based innovation and the development of products or services unrelated to those initially purchased or subscribed to by the user, on the other hand.[186] The user-centred model of data sharing might be effective for promoting competition in aftermarkets for not necessarily innovative (eg, repair) services and, to some extent, for supporting the development of improved or new services based on the data generated by an individual user's device (eg, predictive maintenance). The proposed access regime is not well-suited for facilitating innovation 'based on data from a variety of products or related services',[187] such as 'AI analytics and advanced data-driven services',[188] given that it does not enable access to aggregated data. More broadly, by focusing on data accessibility, the Proposal does not give sufficient consideration to factors bearing on the *usability* of data as an innovation input. Data usability is crucial for any type of data-driven innovation, which is, by definition, based on the processing of large corpora of heterogeneous data.

(334) Recognising the paramount importance of 'smooth access'[189] to data, the European Commission envisaged the Data Act as an instrument of promoting AI-driven innovation, in particular, by facilitating data sharing in business-to-government and business-to-business settings.[190] While the Proposal

[185] See also Recital 28 Data Act Proposal.
[186] Explanatory Memorandum, p 13.
[187] See also Recital 28 of the Proposal.
[188] Impact Assessment Report, p 23.
[189] Communication of the European Commission of 21 April 2021, Fostering a European Approach to Artificial Intelligence, COM(2021) 205 final, 2 ('the promotion of AI-driven innovation is closely linked to implementation of the European Data Strategy […] since AI can only thrive when there is smooth access to data').
[190] European Commission, Annexes to the Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions Fostering a European approach to Artificial Intelligence, COM(2021) 205 final, p 12.

generally claims the capacity to 'enable the achievement of the objectives … including the creation of an innovative and competitive level-playing field for data-driven businesses and the empowerment of citizens',[191] it mentions AI only in passing.[192] Nor does the Impact Assessment Report expand on the goal of fostering AI innovation and the role of the Data Act in this regard, which suggests that this aspect was not subjected to a thorough analysis during the preparatory stage.

(335) The IoT access and use right in the proposed Data Act will not be capable of enhancing access to data for the purpose of training machine learning (ML) models and thus facilitating AI-enabled innovation. First, the user-centred model is not a workable solution to meet the need for *aggregated data*, as third parties can only access data via one user of an IoT device or service at a time. To collect sufficiently large amounts of data, AI developers would have to contract with myriads of users, most likely leading to prohibitively high transaction costs. Second, the scope of the access and use right is confined to data 'in the form and format' it is generated by the IoT product.[193] Such data cannot be equated with a ready-to-use input for developing AI systems and AI applications. To pre-process data in preparation for ML training, one would usually need access to additional *metadata*, including various technical specifications as to how data was collected. This holds for any situation where 'raw' data are utilised for developing innovative products and services. Third, even though IoT data constitute a valuable innovation input, IoT data are only one category of data that can serve as a resource for the data-driven economy. In some cases, such data might be subject to IP protection beyond the *sui generis* database right addressed by the Data Act Proposal. The pending overarching question is how a balance of innovation objectives and economic incentives – including those protected by IP beyond *sui generis* database protection – can be achieved, which in turn could inform the design of a more targeted access regime that is more conducive to innovation.

(336) The question of how the regulatory framework for access to data should be designed to facilitate research in the field of AI and the development of AI applications requires an in-depth analysis. First, one should elaborate a plausible causal logic of a policy intervention connecting the overall policy objective of promoting AI-driven innovation, the intermediate objective of enhancing the availability of usable data and the rules of access at the operative level. Second, a more nuanced understanding of the types of investment along the data value chain and careful consideration of the economic incentives of the market participants are required to properly structure a balance of interests. The preparation of data suitable for the

[191] Explanatory Memorandum, p 8.
[192] Explanatory Memorandum, p 7 (stating that 'the proposal deals with highly strategic technologies such as cloud computing and artificial intelligence systems').
[193] Recital 17 Data Act Proposal.

development of AI systems is not a trivial task – it involves many intermediate stages and requires expertise *inter alia* to ensure the accuracy of predictions generated by a trained model. Furthermore, the metadata required for the preparation of data for training are likely to qualify for trade secret protection. The question of how broader availability of data might be achieved without giving rise to a negative trade-off between innovation incentives of the data holders and a broader circle of innovators requires further analysis.

(337) In view of the foregoing, the aspiration that the 'preferred option' underlying the Data Act Proposal and based on the impact assessment 'would allow businesses, particularly SMEs, to … facilitate the deployment of new technologies (such as big data analytics, machine learning and AI tools'[194] may well constitute an overclaiming of what the Act can achieve. While the question of how a regulatory framework should be designed to facilitate AI-driven innovation remains open, it cannot be asserted that the access and use rights under the proposed Data Act present a suitable instrument in this regard. Furthermore, even though the Data Act does not close the door to further sector regulations to meet specific access needs, it is unclear why access to data for promoting AI-driven innovation should be addressed in a sector-specific manner.

(338) In view of the practical, technical and economic considerations, promoting the role of *data intermediaries* appears to be a more promising approach than data aggregation via individual users of IoT products and services. Yet the Data Act Proposal neglects the potential of data intermediaries in further fostering data-driven innovation. Data intermediaries can play an important role in helping data markets thrive by enabling data aggregation on a larger scale and thereby promote AI-driven innovation. Specifically, data intermediaries can (1) better understand and aggregate third-party data demand for innovative purposes, (2) bundle data supplied from multiple sources in a targeted manner, (3) further aggregate and process user data tailored to the needs of various data recipients, and (4) manage data transfer from a technical and legal perspective. Because of these capabilities, data intermediaries can significantly reduce transaction costs and enable data-driven innovation on a much larger scale. However, it is doubtful that the access right under the proposed Data Act would allow users to share their data with data intermediaries for designated purposes in exchange for payment. Article 6(1) allows processing only for the purpose and under the conditions agreed with the user, while Article 6(2)(c) forbids the third party to 'make the data available it receives to another third party in raw, aggregated or derived form, unless this is necessary to provide the service requested by the user'. Therefore, the user of the device must be the ultimate beneficiary of the service under the scenario that the Data Act addresses. This narrow conceptualisation of the access right implies that a data intermediary cannot

[194] Impact Assessment Report, p. 51.

approach users and offer payment for data, which the intermediary could then process and provide to third parties who need the data for designated innovative purposes in the first place. If the legislature really deems it appropriate to promote unrelated innovation building on the data access and use right of the user, it should relax Article 6(2)(c) for this particular purpose to allow data to be shared with third parties via data intermediaries to create data markets, *inter alia* for the purposes of developing AI. To protect stakeholders' interests – including the secrecy interests of the data holders – and maintain trust in such markets, the legislature should require that such intermediation may only be performed by intermediation services covered by Articles 9-22 Data Governance Act.