The Data Act & Policy Options for a Sectoral Regulation to Protect Competition in the Automotive Aftermarket

by **Daniel Gill** *

Abstract: The European Data Act seeks to end the exclusive control of device manufacturers over IoT data in order to open secondary markets for innovative data-driven services. One of the sectors where the Data Act may have disruptive potential is the automotive aftermarket. Here, vehicle manufacturers and third-party service providers have debated access to "vehicle data, functions and resources" for nearly a decade. Despite the acknowledgement of the European Commission that the vehicle manufacturers' data governance concept may be anticompetitive, this issue is still unregulated. The Data Act could potentially offer a solution to this problem, however due to a series of general shortcomings and sector-specific application issues, it fails to open the automotive aftermarket for innovative third-party services. Aware of this, the European Commission published an initiative for a sectoral regulation on access to vehicle data, functions and resources. While the Data Act and sectoral regulation in principle pursue similar objectives, they have different approaches. This raises the question how the lex-specialis should be designed in order to protect competition in the automotive aftermarket in the light of an enacted Data Act. Finally, this article provides policy recommendations for such a sectoral access regulation.

Keywords: data act, sector regulation, connected cars, data access, data sharing

Recommended citation: Daniel Gill, The Data Act & Policy Options for a Sectoral Regulation to Protect Competition in the Automotive Aftermarket, 15 (2024) JIPITEC 122 para 1.

A. Introduction

1 The Data Act (DA) introduces new data access and sharing rights for users of IoT devices and an obligation for the data holder to conclude a contract with the user about the utilization of the IoT data.[1] Through these means, the Data Act aims to solve the problem that manufacturers – by the technical design of the IoT device – gain exclusive control over the generated data, which often leads to insufficient data access for users and third parties, resulting in numerous problems for competition and innovation in data-driven secondary markets. This article analyzes the effects of the Data Act on competition and innovation in the automotive aftermarket, which is particularly relevant due to a controversial policy debate that currently exist between car manufacturers and third-party services regarding

* Daniel Gill: Research Assistant, Marburg Centre for Institutional Economics, School of Business & Economics, Philipps-University Marburg, daniel.gill@wiwi.uni-marburg.de. The author declare that he has no affiliation with or involvement in any organization or entity with any financial interest in the subject matter or materials discussed in this article.

1 Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonized rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act).

access to vehicle data and technical interoperability of the vehicle. This discussion is directly linked to the well-known problem of the protection of competition in the automotive aftermarket through mandatory access to essential repair and maintenance information and interoperability with the on-board diagnostic interface, within the sectoral type approval regulation.[2] While this regime has been found to successfully protect competition in the automotive aftermarket,[3] past reforms, despite the acknowledgement of arising competition problems by the Commission (in 2018), have failed to adapt the regime to the digitalization of the vehicle.[4] In 2022, the Commission made a first step into the direction of regulating this issue by publishing a call for evidence for an impact assessment for the initiative "access to vehicle data, functions, and resources".[5] Initially, Commission adoption was planned for the 2nd quarter of 2023, however nothing has happened so far. Currently (as of July 2024) Commission insiders expect that delay to continue.

2 The connected car example offers the opportunity to analyze both, the direct effects of the Data Act and the need for additional sectoral regulation, as well as the policy options for the sectoral regulation in the light of the Data Act. To what extent can the Data Act solve the problem of access to vehicle data, functions, and resources? Are additional sectoral rules necessary? And where might there be conflicts? First, this requires an analysis of the problems of the currently applied data governance model of connected cars and a brief overview of the policy discussion in this sector (section B). In a second step, it will be analyzed why the Data Act is no solution and why an additional sectoral regulation is still needed (section C). This is followed by a critical analysis of the sectoral initiative and policy recommendations for a sectoral regulation (section D). The conclusion summarizes the main results and points to alternative, more far-reaching regulatory approaches (section E).

B. The Policy Discussion on Access to Vehicle Data, Functions and Resources

3 The car manufacturers have repeatedly tried to foreclose independent competition (in the relatively profitable) automotive aftermarket by refusing access to essential information. Ultimately, this behavior led to the introduction (in the Motor Vehicle Type Approval Regulation) of the obligation of vehicle manufacturers to provide unrestricted, standardized and non-discriminatory access to repair and maintenance information (against reasonable and proportionate fees) as well as to ensure interoperability with the on-board diagnostic interface for all third parties operating in the aftermarket. Moreover, it provides a list of affected information and lays down the technical requirements for this access.[6] This sectoral technological regulation can be seen as one of the first FRAND (Fair, Reasonable And Non-Discriminatory)-like data access and interoperability solutions. An evaluation by the EU Commission in 2014 confirmed that overall, this system has successfully preserved competition in the aftermarket, albeit issues around vehicle connectivity are emerging.[7] Fueled by this new technology, these issues developed into a controversial policy discussion on access to vehicle data, functions and resources between vehicle manufacturers and third parties in 2016. Starting point of this debate is the so-called "Extended Vehicle", a technical architecture – standardized and applied by all vehicle manufacturers – that establishes a closed (non-interoperable) system that channels every communication with the vehicle

2 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.

3 Ricardo-AEA, Study on the operation of the system of access to vehicle repair and maintenance information – Final Report, 2014, available at: <https://op.europa.eu/en/publication-detail/-/publication/c2c172a5-3f49-4644-b5bb-c508d7532e4a> last accessed 02.07.2024, 133-134.

4 European Commission, Communication On the road to automated mobility: An EU strategy for mobility of the future, COM(2018) 283 final. European Parliament, Resolution of 13 March 2018 on a European strategy on Cooperative Intelligent Transport Systems, OJEU C162/2; European Parliament, Resolution of 15 January 2019 on Autonomous driving in European transport, OJEUC411/2.

5 European Commission, Call for evidence for an impact assessment for the initiative "Access to vehicle data, functions and resources", Ref. Ares(2022)2302201. There is no clear definition of the terms "functions" and resources" and they are oftentimes used interchangeable in the literature. Here, access to vehicle functions refers to the possibility of remotely activating vehicle functions such as unlocking doors (e.g. for shared mobility services) or diagnostic functions (e.g. for roadside services), but also more safety/security critical functions such as braking or steering. Access to vehicle resources on the other hand refers to the opportunity to communicate with the vehicle user (e.g. by displaying information on the dashboard).

6 Regulation (EC) No 715/2007 of the European Parliament and of the Council of 20 June 2007 on type approval of motor vehicles with respect to emissions from light passenger and commercial vehicles (Euro 5 and Euro 6) and on access to vehicle repair and maintenance information, OJEU L 171/1.

7 See Ricardo-AEA (n 3).

through the proprietary backend server of the respective manufacturer.[8] This implies the exclusive control of car manufacturers over the vehicle data, the technical (write) access to the car, and the means to directly communicate with the vehicle user (through the vehicle dashboard). Therefore, if a third party needs access to the vehicle or its data in order to develop, offer, or perform a service, direct access to (via the vehicle user, e.g., through apps) is not possible, but has to be organized through the Extended Vehicle based on individually negotiated contracts between manufacturer and third party.[9] This exclusive control is exacerbated by the fact that the majority of vehicle data, functions and resources in question are unique, non-substitutable, and inimitable, i.e., wherever a third party wants to perform a specific service for a particular vehicle, specific vehicle data, functions and resources are necessary. This setting provides car manufacturers with control over the aftermarket (and all other data-driven secondary markets), and therefore a gatekeeper position that allows them to make market entry of third parties conditional on contractual agreements. Thereby, the manufacturers have – in addition to strong incentives –sufficient means to leverage this position into secondary markets and to foreclose competition. This situation is susceptible to all sorts of anticompetitive strategies, which range from discrimination regarding the prices and conditions of access, to a full access refusal. Both may lead to the exclusion of third parties from the aftermarket. For the "locked-in" users of the connected cars this implies that they can only choose between service providers that have been allowed by the car manufacturer. Access via the on-board diagnostic system as mandated by the Type Approval Regulation offers no comparable access opportunities (both, regarding quantity and quality of access) for third parties. Consequently, competition, innovation and consumer choice are restricted, i.e., the automotive aftermarket fails to deliver efficient market results.[10]

4 This problem is not limited to the automotive aftermarket, but affects potentially all secondary markets that could benefit from technical access to vehicle and its data, and may lead to significant welfare losses due to inefficient levels of competition and innovation. Therefore, this limited access is a problem for the whole ecosystem of connected cars and the mobility system in general. Ultimately, this debate is about how open or closed cars should be as a key element of the bigger (mobility) system?[11]

5 In the policy debate on the Extended Vehicle, there are two important additional arguments. First, strong competition on the primary market will force car manufacturers to choose a more open and interoperable approach, and second, no alternative system could be as safe and secure. Regarding the first argument, the application of the economic theory of aftermarkets suggests that there is no competition between the vehicle systems (bundles of cars and the services available in the respective ecosystems) of the different manufacturers.[12] With respect to the second point, alternative systems have been developed that are less anticompetitive, and can also be made safe and secure.[13]

6 These alternative technical architectures cannot be discussed in detail here; however, they play an important role for the question of how to move forward with the sectoral regulation and are thus outlined in the following. The superior technical architecture according to the important study on "Access to In-Vehicle Data and Resources" is the "on-board application platform", an open interoperable telematics platform – and thus a totally different technological solution – which would enable car users to install third party applications directly in the vehicle – comparable to a smartphone – and decide directly about the access to vehicle data and

8 For a seminal study about this conflict see: Mc Carthy et al., Access to In-Vehicle Data and Resources – Final Report, 2017, available at: <https://transport.ec.europa.eu/system/files/2017-08/2017-05-access-to-in-vehicle-data-and-resources.pdf> last accessed 02.07.2024. For the basic ExVe concept see: ACEA, Position Paper – Access to in-vehicle data, 2021, available at: <https://www.acea.auto/publication/position-paper-access-to-in-vehicle-data/> last accessed 02.07.2024.

9 In this regard, "direct" access for third parties means access to vehicle data, functions and resources authorized by the user, but without the need to negotiate with the vehicle manufacturer. In practice, the user would authorize a third party service e.g., by concluding a service contract, or by giving its consent to an application.

10 For similar conclusions see: Kerber, Data Governance in Connected Cars: The Problem of Access to In-Vehicle Data, JIPITEC 9, 2018, 310-330; Kerber/Gill, Access to Data in Connected Cars and the Recent Reform of the Motor Vehicle Type Approval Regulation, JIPITEC 10, 2019, 201-213; and Martens/Mueller-Langer, Access to digital car data and competition in aftersales services, Digital Economy Working Paper 2018-06, JRC Technical Reports, 2018, 7-10.

11 Determann/Perens, Open Cars, Berkeley Technology Law Journal, Vol. 32(2), 2018, 915-988.

12 This is also because of a limited ability of customers to consider the value of these services at the point of purchase, and a limited ability of customers to switch to other vehicle brands once the car has been purchased. See: Hawker, Automotive aftermarkets: A case study in systems competition, The Antitrust Bulletin Vol. 56(1) 2011, 57-79.

13 See: McCarthy et al. (n 8) 77; Bartsch, et al., On-Board Telematics Platform Security, 2020, available at: <https://www.tuvit.de/en/news/press-releases/press-release-detail/article/tuevit-specifies-cybersecurity-architecture-for-on-board-telematics-platform-otp/> last accessed 02.07.2024.

technical interoperability. A compromise solution is the "shared server", a data trustee solution which would put all vehicle data under the governance of an independent (neutral) entity, that can give non-discriminatory access to all stakeholders (including car manufacturers), the data economy (e.g. via data markets), and public authorities.[14]

7 Against this background, third parties (since 2016) demand a reform of the Type Approval Regulation. A reform in 2018 essentially failed to update the regulatory system to the new technology of connected cars and thus ignored the problem of access to vehicle data, functions and resources.[15] The impact assessment for the sectoral regulation that has been executed in 2022 has not been published until today, and therefore this market failure remains unsolved. The Data Act, although of horizontal scope, provides the first applicable rules that directly impact this long-standing policy debate and could be seen as a potential solution.

C. The Data Act – A Solution for the Problem of Access to the Vehicle and its Data?

8 The Data Act aims to tackle competition and innovation problems in secondary markets (similar to the case at hand) by breaking open existing data silos to facilitate data sharing and data utilization in the EU.[16] From a competition policy perspective, the key problem that the Data Act wants to solve is that manufacturers of IoT devices can obtain– through the technical design of the device,– exclusive de facto control over the generated data, with the consequence that users are unable to access and share the data they (co-)generated. As a result, third parties have only limited access to essential data, which restricts their ability to develop innovative services that can compete with those services offered by the device manufacturer.[17] Or, as Podszun and Offergeld put it: "In the data economy it is easy to block access by technical or legal means; if you cannot access the data of a smart device or system, you are quickly out of the game."[18]

I. Overview of the Data Act`s Rules on Data Sharing and Related Discussions

9 The basic approach of the Data Act to facilitate data sharing relies on the user who gets allocated the inherent value of the data and is basically free in its use and monetization.[19] To empower the user to fulfill this role, the Data Act obliges manufacturers to design the IoT product in a way that the data is easily, and where relevant and technically feasible, also directly accessible to the user by default (Art. 3(1) DA).[20] If this direct (on-device) data access is not possible, the user can demand that the data be made available (Art. 4(1) DA).[21] In addition, the Data Act provides a direct way for the user to share data with third parties, either upon request by a user or by a party acting on its behalf (Art. 5(1) DA).[22] In theory, this enables different options for the user to share data with third parties: (1) by making data available to a third party directly through the device,[23] (2) by downloading data from the manufacturer and making it available to a third party,[24] as well as (3) by requesting the manufacturer to share the data

14 For detailed descriptions of these technological alternatives and the finding that the On-Board Application Platform may be superior to the Extended Vehicle when it comes to its effects on competition and innovation in the automotive aftermarket, see: Mc Carthy et al. (n. 8).

15 Regulation (EU) 2018/858 (n 2). For an analysis of the reform of the TAR in 2018 see: Kerber/Gill (n 10).

16 Bomhard/Schmidt-Kessel, EU-Datengesetz ante portas, MMR 2024, 69, (69).

17 Regulation (EU) 2023/2854 (n 1) Rec. 20; Kerber, Data Act and Competition: An Ambivalent Relationship, Concurrences 1/2023, 31.

18 Podszun/Offergeld, The EU Data Act and the Access to Secondary Markets, available at: <http://dx.doi.org/10.2139/ssrn.4256882>, 6.

19 Hennemann/Steinrötter, Der Data Act, Neue Instrumente, alte Friktionen, strukturelle Weichenstellungen, NJW, 2024, 1; Wiebe, Der Data Act – Innovation oder Illusion? GRUR 2023, 1569 (1572).

20 Easy, secure, free of charge access for the user to the data in a comprehensive, structured, commonly used and machine-readable format, and if relevant and technically feasible directly through the device.

21 In this case, the data have to be accessible to the user without undue delay, of the same quality as is available to the data holder, easily, securely, free of charge, in a comprehensive, structured, commonly used and machine-readable format and, where relevant and technically feasible, continuously and in real-time.

22 Under the same conditions as Art. 4(1), see (n 20).

23 Which is dependent on the manufacturers decisions whether this direct access is "technically feasible", whether accessible means that the user can actually receive a copy of the data or "in-situ" access, and whether this copy can be transferred to the third party.

24 While this "circumvention" possibility exists in theory, it is questionable how practical it is, since the user has to have the technical infrastructure in place to receive data from the manufacturer and to share it with third parties, probably continuous and in real-time. For consumers, this may cause prohibitively high transaction costs.

with a third party.[25] This way, the Data Act aims to stimulate innovation on secondary markets (esp. aftermarkets) while simultaneously trying to "avoid undermining the investment incentives for the type of product from which the data are obtained".[26] To achieve a balance between these seemingly conflicting objectives, the Data Act accepts the de facto control of the manufacturers over the data and thus relies upon a data governance model that is only limited through the initial contract with the user and the new user rights of Arts. 4 and 5 DA.[27]

10 The Data Act has been subject to discussions right from the first proposal, and it is still an open question whether it can fulfill its objectives, i.e., unfold innovative effects on data-driven secondary markets.[28] In the center of this discussion is the user-centric approach of the Data Act which, especially. in B2C scenarios, may not to be able to facilitate purpose-oriented data sharing.[29] In the following, the most important general arguments are summarized. First, it is surprising that a user-centric approach has been chosen for the Data Act instead of parallel usage rights, given that IoT data is largely perceived as co-generated data to which no exclusive legal position should be created in order to facilitate independent data use.[30] Second, the de facto control of the user (consumer) is much weaker than the Data Act suggests, because the contract of Art. 4(13) DA suffers from the same issues as consent under data protection law: the user faces many informational and behavioral problems regarding the handling of data;[31] no consumer protection rules are provided by the Data Act; the manufacturer can tie the sale of the device to the data use contracts, etc. As a result, users often will have to accept contracts in which they grant the manufacturer broad and long-term competences regarding the utilization of the data ("total buy-out contracts", "take-it-or-leave-it" situation).[32] Third, the data access and sharing rights suffer from a number of problems that make them inefficient. In general, there are too many restrictions and legal uncertainties for users and third parties;[33] difficult disputes may arise about the "reasonable compensation" or the protection of trade secrets, and the scope of data may be too narrow to enable innovative services. Regarding the last point, an additional problem is that the Data Act allows for "in-situ" access, i.e., instead of a data transfer, data access and processing can take place within the server of the manufacturer, which may often not meet the requirements of third parties.[34] Moreover, hardly any criteria are provided on data usability, i.e., the technical state of the data, which may also run counter to the objective of facilitating innovative services.[35]

11 Another important general discussion is about the relation of the Data Act and the General Data Protection Regulation (GDPR). This relationship is important for this article since the majority of

25 Subject to a negotiated "licensing contract" between manufacturer and third party with FRAND conditions and a reasonable compensation for the manufacturer (Regulation (EU) 2023/2854 (n 1) Arts. 8 & 9.).

26 Regulation (EU) 2023/2854 (n 1) Rec. 32.

27 Kerber, Governance of IoT Data: Why the EU Data Act Will not Fulfill Its Objectives, GRUR International 2023 Vol. 72(2), 120-135, (132); Kerber, EU Data Act: Will new user access and sharing rights on IoT data help competition and innovation?, Journal of Antitrust Enforcement 2024, 1-7, (3); Specht-Riemenschneider, Der Entwurf des Data Act – Eine Analyse der vorgesehenen Datenzugangsansprüche im Verhältnis B2B, B2C und B2G, MMR 9 2022, 809-826, (817).

28 See among others: Drexl, et al., Position statement of the Max Planck Institute for Innovation and Competition on the Commission's Data Act Proposal of 23 February 2022, at: <https://doi.org/10.2139/ssrn.4136484>; Specht-Riemenschneider (n 27); Podszun/Offergeld (n 18); Krämer, Improving the Economic Effectiveness of the B2B and B2C Data Sharing Obligations in the Proposed Data Act, CERRE Report (2022); Martens, Pro- and Anticompetitive Provisions in the Proposed European Union Data Act, Bruegel Working paper 01/2023; Metzger/Schweitzer, Shaping Markets: A Critical Evaluation of the Draft Data Act, ZEuP 2023, 42; Wiebe (n 19); Kerber (n 27 2023 & 2024); Hennemann/Steinrötter (n 19); Antoine, Datenzugangsrechte im finalen Data Act – Fortschritt, Rückschritt, neue Fragen? Schlüssel zur Förderung datengetriebener Geschäftsmodelle? CR 2024, 1-8; Eckardt/Kerber, 'Property Rights Theory, Bundles of Rights on IoT Data, and the EU Data Act', European Journal of Law & Economics 2024, Vol. 57, 113–143, <https://doi.org/10.1007/s10657-023-09791-8>.

29 The purpose in this case is to ensure competition and innovation in the automotive aftermarket. For the general discussion of a more purpose-based approach within the Data Act see Drexl et al. (n 28).

30 Drexl et al. (n 28) 19; Leistner/Antoine, IPR and the use of open data and data sharing initiatives by public and private actors, Study requested by the JURI committee, 2022, available at: <https://www.europarl.europa.eu/RegData/etudes/STUD/2022/732266/IPOL_STU(2022)732266_EN.pdf>, 81.

31 For an overview about such informational and behavioral problems see e.g.: Sibony/Micklitz/Esposito, Research Methodes in Consumer Law, 2018; Zamir/Teichmann, Behavioural Law and Economics, 2018.

32 Kerber (n 27, 2024) 4; Hennemann/Steinrötter (n 19) 7; Antoine (n 28) 6; Specht-Riemenschneider (n 27) suggests a ban in tie-ins, better cancelation possibilities and a limited contract duration.

33 Kerber (n 27, 2023) 125-128; Krämer (n 33); Podszun and Offergeld (n 18) 28.

34 Specht-Riemenschneider (n 27) 816; Podszun/Offergeld (n 18) 31-31.

35 Kim/Kwok, Data Usability as a Parameter of Rights and Obligations under the EU Data Act, Max Planck Institute for Innovation and Competition Research Paper No. 24-04.

vehicle data is considered personal data.[36] Basically, data sharing and data protection are in conflict. The question is in how far the GDPR limits data access and sharing under the Data Act. On the one hand, the data access and sharing rights also cover personal data (Art. 1(2), Rec. 35 DA); on the other hand, the Data Act is without prejudice to the GDPR (Rec. 7 DA). Therefore, both regulations apply in parallel when personal data is affected. For example, the information obligations of Arts. 13 & 14 GDPR complement the transparency obligations from Art. 3(2) DA. Also, the data portability right of Art. 20 GDPR applies parallel to the access and sharing rights of Arts. 4 and 5 DA. However, problems arise from this parallel application when it comes to the legal basis of the data processing. As Wiebe et al. (2023) explain, none of the existing legal bases (Art. 6(1) GDPR) appropriately serves as a general justification for lawful data processing in the case of the connected car and possible data access and sharing requests under the Data Act. Therefore, they conclude that the vehicle data should be anonymized as early as possible.[37] But if the data is anonymized, i.e., non-personal, the manufacturer can only use the data based on a contract with the user, and the user has the exclusive right to determine who can access, use and share the data for what purpose (Arts. 4(13) & 4(14) DA). As a result, the manufacturer faces interesting tradeoffs regarding the question whether or not to anonymize the data.[38] The following case specific analysis assumes that all vehicle data initially is personal data, esp. in typical repair and maintenance situations, where a specific user is receiving a specific service for a specific car based on individual-level data, however, in other situations, such as improvement of components, or traffic management it is assumed that the aggregated-level data that is relevant here, is anonymous data.

36 Commission Nationale Informatique & Libertés, 'Compliance Package – Connected Vehicles and Personal Data', 2017, available at: <https://www.cnil.fr/sites/default/files/atoms/files/cnil_pack_vehicules_connectes_gb.pdf> last accessed 02.07.2024, 5; Störing, What EU legislation says about car data – Legal Memorandum on connected vehicles and data, 2017, available at: <https://www.fiaregion1.com/wp-content/uploads/2017/06/20170516-Legal-Memorandum-on-Personal-Datain- Connected-Vehicles-www.pdf> last accessed 02.07.2024, 2; Metzger, Digitale Mobilität – Verträge über Nutzerdaten, GRUR 2019, 129-136, (131).

37 Wiebe et al., Studie zur Notwendigkeit und Ausrichtung von spezifischen Datenzugangsregelungen im Bereich des vernetzten Fahrzeugs in der Automobilwirtschaft, 2023, 77-78, available at: <https://www.bundesnetzagentur.de/DE/Fachthemen/Digitalisierung/Daten/Datenoekonomie/schlussbericht.html> last accessed 02.07.2024.

38 Bomhard/Schmidt-Kessel (n 16) describe this as "escape into data protection law".

II. Limitations of the Data Act as Solution for Access to the Vehicle and its Data

12 The mobility sector and the need for new rules "to ensure that existing vehicle type-approval legislation is fit for the digital age" were explicitly addressed in the explanatory memorandum of the Data Act proposal.[39] Consequently, the different roles defined by the Data Act fit quite well to the different stakeholder groups in this discussion: the car manufacturer suits the "data holder" definition of Art. 2(13) DA. The "user" according to Art. 2(12) DA can be the vehicle owner or driver, which can be a natural or legal person, [40] which seems to exclude passengers and bystanders although they are often captured by the data generation process.[41] However, the term "user" is also subject to several open questions, e.g., what happens when the device is sold, or when usage authorization (e.g. car sharing) ends.[42] "Data recipient" pursuant to Art. 2(14) DA would be third parties who either get data made available by the manufacturers directly under a legal obligation, or by request of the user.[43] The main question is whether the new instruments introduced by the Data Act are able to solve the data access problem in the automotive aftermarket. To answer this question, the following sections analyze: (1) limitations regarding the scope of data, (2) limitations regarding the data sharing mechanism, and (3) limitations regarding the utilization of data through data holders, users and third parties.

1. Limitations Regarding the Scope of Data

13 The Data Act "grants users the right to access and make available to a third party any product or related service data, 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."[44] Articles 4(1) and

39 European Commission, Proposal on harmonized rules on fair access to and use of data (Data Act) COM/2022/68 final, 6.

40 In this paper the term "users" is used for natural persons, i.e. consumers. In case the user explicitly is a legal person, the term "business user" is used.

41 For a narrower definition see: Drexl et al. (n 28) para. 59f.

42 Also general about the relations of the different stakeholders see: Schmidt-Kessel, Heraus- und Weitergabe von IoT-Gerätedaten, MMR 2024, 77.

43 Similiar for the example of connected cars: Etzkorn, (Vertragliche) Datenzugangsansprüche nach dem Data Act, RDi 2024, 116 (118).

44 Rec. 35 DA. Art. 1(2) provides that the DA covers personal and non-personal data, and specifies that Chapter 2 applies

5(1) DA concretize this seemingly broad scope of data as the "readily available data, as well as the metadata that is necessary to interpret and use that data", without disproportionate effort, going beyond a simple operation.[45] Recital 15 DA clarifies that this includes data "which are not substantially modified, meaning data in raw form [...] as well as data having been pre-processed for the purpose of making it understandable and usable prior to further processing and analysis".[46] In contrast, information derived from this data as the outcome of additional investments is excluded. This formulation implies significant limitations to the scope of data, making it unsuitable for the purpose of maintaining competition in the automotive aftermarket.

14 First, the limitation to 'readily available data' that the manufacturer can obtain 'without disproportionate effort', or 'which the OEM designed to be retrievable' means that car manufacturers are not obliged to make vehicle data accessible that is not stored (volatile data)[47] or not retrievable without additional investments. As a consequence, the car manufacturers are free to decide which vehicle data to generate and cannot be expected to invest in the generation of additional data besides that which they use themselves. However, for competition in the aftermarket, especially for the creation of innovative services, it can be necessary to access certain categories of (volatile) data that are not stored in this form, because it provides specific insights (e.g., performance data of specific parts, that is only stored in case of a fault). Moreover, if the data generation is limited to data that the car manufacturers needs to generate in order to provide their own services, the potential of innovation (from market entrants) is also limited relative to the situation where all data is generated and made accessible that could be generated technically.

15 Second, the exclusion of derived and inferred data, together with the limitation to readily available data, ignores the problem that most of the data needed to provide aftermarket services has already been processed to a certain extent. This is also directly related to the question of the impact of intellectual property rights and trade secrets on the scope of data, since the majority of the generated data is directly processed through proprietary software (e.g., predictive maintenance algorithm or diagnostic tools). This aggregated and derived/inferred data is often more important for secondary markets, but only the manufacturers are able to apply value-generating data processing. Predictive maintenance, for example needs access to raw as well as aggregated data.[48] The approach of the Data Act to include pre-processed data, as well as the data necessary to make use of this data, is a right step towards a more purpose-based scope of data.[49] However, whether this is enough to ensure competition and innovation in the automotive aftermarket and other secondary markets is still unclear.

2. Limitations Regarding the Basic Data Sharing Mechanism of the Data Act

16 The Data Act acknowledges that users of IoT devices are often not able to obtain the data necessary to make use of secondary services.[50] To solve this problem, new data access and sharing rights are introduced, which complement the right to data portability of Art. 20 GDPR.[51] While Art. 20 GDPR has been found to have severe problems regarding its

to data concerning the performance, use and environment of connected products and related services.

45 Art. 2(17) DA. Further definitions: Product data: "data, generated by the use of a connected product, that the manufacturer designed to be retrievable, via an electronic communications service, a physical connection or on-device access, by a user, data holder or a third party, including, where relevant, the manufacturer" (Art. 2(15) DA). Related service data: "data representing the digitization of user actions or events related to the connected product, recorded intentionally by the user or as a by-product of the user's action, which is generated during the provision of a related service by the provider" (Art. 2(16) DA).

46 Rec. 15 further explains that "the term 'pre-processed data' should not be interpreted in such a manner as to impose an obligation on the data holder to make substantial investments in cleaning and transforming the data. Such data should include the relevant metadata, including basic context and timestamp to make the data usable, combined with other data (e.g. sorted and classified with other data points relating to it) or re-formatted into a commonly-used format."

47 Volatile data is raw data that is directly processed within the vehicle for a specific purpose and deleted immediately afterwards. This data is also often not transferred outside the vehicle due to bandwidth limitations and the costs of transferring and storing huge amounts of data.

48 Wiebe et al. (n 37) 62; Gill, The Data Act Proposal and the Problem of Access to In-Vehicle Data and Resources, available at SSRN: <http://dx.doi.org/10.2139/ssrn.4115443>, 11.

49 Data having been pre-processed for the purpose of making it understandable and useable prior to further processing and analysis, including data collected from a single sensor or a connected group of sensors, for the purpose of making the collected data comprehensible for wider use-cases. (Rec. 15 DA). In fact, the Data Act recognizes that these data are "potentially valuable to the user and support innovation and the development of digital and other services protecting the environment, health and the circular economy, including though facilitating the maintenance and repair of the products in question." (Rec. 15).

50 Regulation (EU) 2023/2854 (n 1) Rec. 20.

51 Regulation (EU) 2023/2854 (n 1) Rec. 35.

applicability,[52] the Data Act seems to have learned from this discussion by, on the one hand, abstaining from the limitations of Art. 20 GDPR,[53] and on the other hand, exceeding it by including non-personal data and metadata, and by mandating continuous and real-time data availability (where feasible). However, while it is debatable whether this mechanism can be effective in general, there are specific issues as to its ability to maintain competition in the automotive aftermarket, since (1) vehicle users may not claim their rights, and (2) the Data Act even protects the exclusive control of car manufacturers over the vehicle data.

17 Option one for the users would be to directly access the data on the device and make it available to third parties (Art. 3(1) DA). This seems unlikely for several reasons: the car manufacturer may decide to declare that this kind of access is technically not feasible (e.g., due to safety and security considerations), the data access may only take place in-situ, i.e., without the user receiving an actual copy of the data, and even if the user would receive such a copy, the interface would need to be designed in a way that allows the user to easily transfer the data to the third party (which the manufacturer is neither obliged to, nor incentivized by competition). Option two, namely to request data from the manufacturer, and to make it available to the third party (Art. 4(1) DA), would require the user to have the infrastructures available to download from the manufacturer and to upload to the third party potentially high volumes of real-time and continuous vehicle data, which seems unrealistic. The option remains to request that the manufacturer shares the data with a third-party (Art. 5(1) DA). It seems unlikely that the user will actively claim this right when there are transaction costs for making vehicle data available to third parties. This holds especially where the car users cannot directly identify whether and how much they benefit from the (additional) data sharing with the third party, and where the service in question is already offered (as default option) by the vehicle manufacturer. Take for example the situation when a car user has to decide between the manufacturer's official repair service and a third-party repair service. If it is cumbersome for the user to authorize the third party to access and use the data (e.g., because of a lack of information and experience), the price of the third-party service (including the compensation) plus the perceived transaction costs of providing access to vehicle data, has to be lower than the price of the manufacturer's service. The price for the third-party service could even increase if the data contains trade secrets, since, in this case, additional agreements are necessary to preserve the confidentiality of the data.[54]

18 These transaction costs depend strongly on the manufacturers' design of the interface with the vehicle user and how difficult it is for the user to request the data sharing, i.e., to authorize access by a third party. The Data Act seems to be aware of the implications of the design choice towards the transaction costs of the users and consequently obliges data holders (1) to design products and services in a way that the data is easily accessible and sharable for the user as well as usable (data interoperability) for users and third parties,[55] and (2) to provide the user with far-reaching information on the data that can be generated, whether it can be generated continuously and in real-time, where it is stored, how it can be retrieved, whether the data contains trade secrets etc.[56] However, despite these provisions, the car user may still be overburdened, especially. when facing multiple or repetitive situations of decisions regarding data sharing with a third party (e.g., privacy or consent fatigue).[57] One option against this problem could be to empower users to authorize a specialized third party (e.g., a data trustee)[58] to access, manage, and share the

52 See: Krämer/Senellart/de Streel, Making Data Portability More Effective for the Digital Economy, 2020, available at: <https://cerre.eu/publications/report-making-data-portability-more-effective-digital-economy/> last accessed 02.07.2024. For a detailed analysis of the practicability of Art. 20 GDPR for providing access to vehicle data for third parties in the automotive industry see: Gill/Metzger, Data Access through Data Portability - Economic and Legal Analysis of the Applicability of Art. 20 GDPR to the Data Access Problem in the Ecosystem of Connected Cars, European Data Protection Law Review, 8(2) 2022, 221 – 237.

53 E.g. regarding the nature of the data as personal or non-personal data, whether actively or passively observed, with respect to the legal basis of its processing, and whether or not it is technically feasible to port the data.

54 Gill (n 48) 13.

55 Art. 3(1) obliges the manufacturers to make the data "by default, easily, securely, free of charge, in a comprehensive, structured, commonly used and machine-readable format, and where relevant and technically feasible, directly accessible to the user." In addition, Art. 4(4) obliges the manufacturers to not make access to the data through the user "unduly difficult". Moreover, Rec. 27 demands that users should be given the necessary technical interface to manage permissions.

56 Regulation (EU) 2023/2854 (n 1) Art. 3(2).

57 See: Choi et al., The role of privacy fatigue in online privacy behavior, Computers in Human Behavior, Vol. 81, 2018, 42-51.

58 For approaches of data trustees in the area of mobility, see: Specht-Riemenschneider/Kerber, Designing Data Trustees – A Purpose-Based Approach, 2022, available at: <https://www.kas.de/de/analysen-und-argumente/detail/-/content/datentreuhaender-gesellschaftlich-nuetzlich-rechtlich-groessere-anforderungen-erforderlich> last accessed 02.07.2024); or, with a study about the concept of a "Mobilitätsdatenwächter", Reiter et al., Gutachten

data on behalf, and in the best interest of the user in order to further reduce transaction costs. This way, third parties could aggregate data from many vehicle users (and across brands) and provide all stakeholders with higher quality data sets regarding scale and scope. Article 5(1) DA explicitly includes this option.[59]

19 A more fundamental problem with respect to the basic data sharing mechanism is that the Data Act protects the de facto exclusive control of the manufacturer over the vehicle data. It does not provide third parties with a direct right to access the data and requires a negotiated agreement between data holder and third party which can lead to considerable problems and costs. The Data Act provides leeway for themanufacturers to make the data accessible either within the vehicle, or through their servers (Rec. 22), or to organize data availability for third parties in the form of "in-situ" data access (Rec. 8), which means that the third parties would not get a copy of the data, but would bring their algorithms to the manufacturers servers in order to derive insights.[60] At the same time, the Data Act is silent on the user's ability to directly transfer data for free to third parties in return for benefits without the approval of the data holder. According to Martens (2023) the Data Act does not want to open this possibility because it would undermine the data holder's ability to charge a price.[61] Although the user initiates the data sharing, the specific conditions of the data sharing agreement are subject to negotiations between data holder and third party based on the principles of contractual freedom.[62] Kerber (2022) states that this can lead to considerable problems (e.g., around the modalities of "FRAND" terms, or the reasonable compensation) and raise costs and delays that make the mechanism unattractive. Moreover, this contractual freedom may be problematic where there are imbalances in the negotiation power between data holder and third party, which may potentially lead to contractual terms that limit effective competition and innovation in the independent aftermarket. The Data Act provides a complex thicket of obligations regarding these contracts. The next section compares these limitations regarding the opportunities of data holders, users and third parties to make use of the data.

3. Unequal Opportunities Regarding the Utilization of the Vehicle Data

20 The Data Act regulates the contractual relationship between data holder, user and third party with the objective to prevent the exploitation of contractual imbalances.[63] It bases on the principle of contractual freedom to negotiate the conditions for making data available and provides asymmetric limitations to this freedom for data holders and third parties.[64] These unequal opportunities may distort competition and innovation in the automotive aftermarket. For the car manufacturers, the only restrictions, besides the general rules on unfair contractual terms of Art. 13 DA, seem to arise with respect to the pre-contractual information obligations of Art. 3(2) DA, the prohibition to derive insights about the commercial situation of the user of Art. 4(13) DA, and the prohibition of "dark patterns" in Rec. 38 DA (not reflected in the Articles). In contrast, for third parties, the Data Act provides a range of direct limitations. Art. 6(1) DA obliges the erasure of the data when no longer necessary for the agreed purpose (unless contractually agreed with the user), which may deprive third parties of the possibility to aggregate and store this data for any future (currently unknown) purposes. Art. 6(2)c DA prohibits data sharing with other third parties (unless contractually agreed with the user), which prevents better supply of vehicle data e.g., on data marketplaces and thus adds to the preservation of the gatekeeper positions. Art. 6(2)d DA prohibits third parties (and users, but not manufacturers) to share data with gatekeepers (designated pursuant to Art. 3 DMA), which is particularly critical due to the role of Google and Apple regarding automotive operating systems. Art. 6(2)e DA prohibits third parties to use the data to develop a product that competes with the manufacturer`s product, or to share the data with a third party with that intent, which "reduces the scope of legitimate data-driven innovations to not-too-close substitute products"[65] and raises legal risks for innovators.[66] Moreover,

– Einführung eines „Mobilitätsdatenwächters" für eine verbrauchergerechte Datennutzung – Notwendigkeit, Modell, gesetzliche Grundlagen, 2022, available at: <https://www.vzbv.de/sites/default/files/2022-11/22-11-15_Gutachten_Mobilit%C3%A4tsdatenw%C3%A4chter_BRC_2022-15-11_Clean_Finalversion.pdf> last accessed 02.07.2024.

59 See also Regulation (EU) 2023/2854 (n 1) Recs.: 26, 30, 33.

60 See critically Kerber (n 27) 124; Drexl et al. (n 28) 29. For a more positive understanding of "in-situ" access see: Martens et al., Towards Efficient Information Sharing in Network Markets, 2021, available at: <https://ssrn.com/abstract=3954932> last accessed 02.07.2024.

61 Martens (n 28) 11.

62 Regulation (EU) 2023/2854 (n 1) Rec. 43: "On the basis of the principle of contractual freedom, parties should remain free to negotiate the precise conditions for making data available in their contracts within the framework for the general access rules for making data available."

63 Regulation (EU) 2023/2854 (n 1) Rec. 5.

64 Regulation (EU) 2023/2854 (n 1) Rec. 43.

65 Martens (n 28) 14.

66 Graef/Husovec, Seven Things to Improve in the Data

the Data Act provides data holders (and users) with possibilities to (contractually) restrict the accessibility and sharing of the data, if security requirements (Art. 4(2) DA) or the confidentiality of trade secrets (Arts. 4(8) and 5(11) DA) would be undermined. These provisions may be abused by the car manufacturer in order to prevent data sharing based on safety and security consideration, which is particularly relevant for connected cars. There are no similar limitations for the manufacturers.[67]

4. No Technical Access to the Vehicle (Functions and Resource)

21 Most importantly, the Data Act does not regulate the interoperability of IoT devices with third party services, or in this case, access of third parties to the vehicle functions and resources. However, this access is critical for many innovative services for several reasons. First, similar to the existing (but technologically obsolete) on-board diagnostic interface, aftermarket services may need (remote) access to specific vehicle functions and resources in order to trigger certain events and, test functionality. Second, for some aftermarket services it may be necessary to install an application on-board the vehicle to directly access, aggregate and process relevant information, or activate certain functions and resources. If this is not possible, their services may be limited in functionality and quality. Third, direct access to the vehicle also implies opportunities to communicate with the driver (and/or passengers), without being dependent on mails or calls. If this ability is held exclusively by the vehicle manufacturers, they have an additional competitive advantage in offering services, i.e., they will be able to steer the consumers into their services (manipulation). The existing access to vehicle functions and resources through the on-board diagnostic interface does not provide sufficient access, since it is limited in scope and functionality and reflects only a minor part of the access opportunities of the manufacturers.[68]

III. Suitability of the Data Act to solve the Problem of Access to the Vehicle and its Data

22 Does the Data Act eliminate the exclusive de facto control of the car manufacturers over the vehicle data? No, but it may even strengthen it! Indeed, accessibility by design and the rights of users to access and share the data with third parties may have a positive effect on competition and innovation in the automotive aftermarket. However, this is based on the problematic assumptions that individual vehicle users are able to negotiate with the manufacturers about the terms and conditions and even dictate the purposes of the data processing,[69] and that the users will actively make use of their data sharing right. Both seem unrealistic given the potentially high transaction costs, uncertain benefits, and the ability of the manufacturers to offer these contracts on a "take-it-or-leave-it" basis. In fact, it can be argued that the users do not have meaningful control about their vehicle's data, which can be interpreted as another market failure due to informational and behavioral problems.[70] Moreover, the scope of data may not be fit for the purpose of maintaining effective competition. Most importantly however, interoperability of the IoT device with third party services is not regulated at all.

23 Despite its good intentions, the Data Act may in fact confirm the existing exclusive de facto control of the car manufacturers over the vehicle data

Act, 2022, 2 at: <https://ssrn.com/abstract=4051793> last accessed 26.06.24.

67 Another question is, in how far Art. 4(13) DA de facto limits the data utilization opportunities of the car manufacturers (for non-personal data). According to the literature, the manufacturer can make the sale of the vehicle conditional on the users' agreement on potentially far-reaching and long-term data usage because the user faces the same informational and behavioral problems that are well-known regarding the consent to the processing of personal data and the Data Act is nearly entirely silent on this initial contract and includes no specific rules for the protection of consumers. Therefore, it is widely expected that the manufacturers can offer "total-buy-out" contracts on a "take-it-or-leave-it" basis, which would allocate all rights to use, share and monetize the data to the manufacturers for the entire life-time of the vehicle (see: Kerber (n 27) 132; Wiebe et al. (n 37) 67; Specht-Riemenschneider (n 27) 817; Colangelo, European Proposal for a Data Act – A first Assessment, 2022, 17, available at: <https://cerre.eu/wp-content/uploads/2022/07/200722_CERRE_Assessment-Paper_DataAct.pdf> last accessed 02.07.2024).

68 See also Kerber/Gill, Revision of the Vehicle Type-Approval Regulation: Analysis and Recommendations, 2022, available at SSRN: <http://dx.doi.org/10.2139/ssrn.4174028>, 5.

69 Which may be true in specific B2B situations in which the business user is in the better negotiation position, but cannot hold for B2B situations where the business user depends on data access, or any B2C situation.

70 See: Kerber (n 27) 132. In the discussion about the Data Act there are a number of suggestions that would strengthen the position of the consumers, see: BEUC, Commission must take urgent action to protect consumers' data in the automotive sector, 2022, available at: <https://www.beuc.eu/sites/default/files/publications/beuc-x-2022-009_action_to_protect_consumers_data_in_the_automotive_sector.pdf> last accessed 02.07.2024.

because it acknowledges, legitimizes, and protects this position.[71] First, the largely unrestricted initial contract between manufacturers and vehicle users, in relation to the highly restricted data utilization opportunities of third parties, grants the manufacturers a competitive advantage. Second, the Data Act neither provides direct access rights for third parties, nor is it self-evident that vehicle users are de facto able to directly transfer data to third parties for free in return for benefits without the approval of the data holder. Instead, the Data Act relies to a large extent on contractual freedom for negotiations between car manufacturers and third parties, potentially leading to many problems e.g., around the interpretation of FRAND conditions or the calculation of compensations. A sectoral regulation as announced multiple times in the Data Act,[72] and as called for by third parties, would have the opportunity to be much more targeted towards the purpose of competition in the automotive aftermarket.

D. Critical Analysis of the Policy Options for a Sectoral Regulation

24 Shortly after the Data Act proposal the European Commission published a call for evidence for an impact assessment for the initiative "access to vehicle data, functions and resources".[73] This initiative, if translated into a regulation and enacted, would reform the existing Type Approval Regulation for motor vehicles (with its rules on access to repair and maintenance information),,[74] through an (additional) access regime about access to vehicle data and technical access to the vehicle (interoperability) for the automotive aftermarket and other stakeholders within the broader mobility system. This raises the question how to align the sectoral Type Approval Regulation with the horizontal principles of the Data Act and what additional rules are necessary.[75]

25 The objectives of this initiative are to promote innovation in the automotive and mobility sector, to ensure higher quality, more choice and lower prices of vehicle-related and mobility services for consumers, and to safeguard cybersecurity, safety, personal data protection, intellectual property, as well as the necessary investment incentives for data-driven vehicle-related services.[76] This is consistent with the Data Act. However, also like the Data Act, this initiative would not eliminate the gatekeeper positions of the vehicle manufacturers but would only limit the negative effects of their exclusive control position. Moreover, different to the Data Act, the initiative does not mention (a) the empowerment of users for more meaningful control over their vehicle and the data, and (b) the unlocking of vehicle data for innovation beyond the mobility sector (e.g. data markets).[77]

26 In the policy initiative, the European Commission compares a baseline scenario (Data Act enacted, no sectoral regulation) with three policy options that represent a step-by-step deeper regulation for technical access to the vehicle and its data. Option 1 would complement the data access rights of the Data Act with equal access rights to functions and resources, and would ensure transparency about the available vehicle data, functions and resources. Option 2 would complement this by a minimum list of vehicle data, functions and resources that have to be available, including communication with the driver and access to the on-board diagnostic port. Option 3 would additionally specify how this access would occur and be controlled. All options would address the option-specific interplay between access rights and cybersecurity rules. In the following, these policy options are assessed regarding (1) access to data, (2) access to functions and resources, and (3) additional governance rules.

I. Regulated Access to Vehicle Data

27 The scope of data covered by the initiative is not clearly described and thus subject to different interpretations. First, it may rely on Art. 4 & 5 DA to make vehicle data accessible to third parties. In this case, the scope of data covered would be subject to the same legal uncertainty than the one under the Data Act (see C.I.1). Second, the principle of equal, non-discriminatory access to functions and resources of option one could also refer to data. This would imply that the manufacturer has to make available to third parties all the data that is made available to the manufacturers' services, which is a reasonable approach in theory, but could have anticompetitive consequences in practice, since an increasing number of services are provided directly by the manufacturer (e.g. software updates), and a non-discriminatory scope of data vis-à-vis authorized services could be too narrow (especially. for innovation). Third, the minimum list of vehicle data, functions and resources of policy option two could go beyond the scope of data covered by the Data Act in order to enable certain innovation activities and services, depending on the regulator's decision

71 See for a similar conclusion about the Data Act in general: Eckardt/Kerber (n 28) 22.

72 Regulation (EU) 2023/2854 (n 1) Recs 14, 25, 27.

73 European Commission (n 5).

74 Regulation (EU) 2018/858 (n 2).

75 Regulation (EU) 2023/2854 (n 1) Rec. 6.

76 European Commission (n 5) 2.

77 Kerber/Gill (n 68) 6.

on which data to include. In this interpretation, the degree of openness of the automotive sector would depend on the regulator and not anymore on the strategic decisions of the manufacturers. Overall, it is not clear if the initiative chooses a functional approach similar to the Type Approval Regulation. From a competition and innovation perspective, such an approach should be chosen since it would include all data in all forms that are necessary for the provision of the aftermarket service.[78] To reduce the uncertainty as to the interpretation of the scope of data, a sectoral regulation would have the opportunity to make much more specific definitions. It could provide e.g., a more practical delimitation of personal and non-personal data as well as of raw, pre-processed and derived/inferred data, develop guidelines to clarify which data may constitute a trade secret, or is critical to the safety and security of the vehicle, mandate a minimum of data to be accessible (independent of brand and model), and facilitate the standardization of metadata (particularly important for the many multi-brand service providers, and public sector services).

28 A conflict exists regarding the basic data sharing mechanism. The Data Act is based upon a user-centric approach where data sharing is always initiated by the user, while the Type Approval Regulation provides direct access rights for third parties. Which approach should the initiative take? It would fit into the logic of the Data Act if the Type Approval Regulation would also provide vehicle users with data access and sharing rights. From the perspective of user empowerment (Data Act objective) this would make sense. However, from the perspective of innovation and competition such a solution is unlikely to lead to sufficient quantities of data being shared and would thus be unlikely to facilitate independent innovation and competition.[79]

29 Different to the Data Act, the initiative does not seem to set restrictions regarding the possibilities of manufacturers and third parties of how to use the data, i.e., the Data Act provides the default rules. However, it would be an opportunity for the sectoral regulation to clarify some aspects that the Data Act does not sufficiently consider. Amongst others, the initial contract between manufacturer and user could be specified. This may include e.g. a limitation to the duration of this contract, minimum standards as to the granularity of the users' choice, the prohibition of "total buy-out" contracts, a clarification of which data may not be shared due to security or confidentiality requirements, rules for situations in which either the user or the data holder change, and means to discontinue data sharing without losing functionality of the car.

78 Wiebe et al. (n 37) 81; Drexl et al. (n 28) para. 25.

79 See also Kerber (n 27) 125 ff.

30 A final important aspect regarding access to vehicle data that needs to be clarified sectorally, is the relationship between the automotive industry and gatekeepers (pursuant to Art. 3 DMA), in particular Google and Apple with their automotive operating systems. The prohibition of Art. 6(2)d Data Act for users and third parties to share data with these companies may lead to significant problems regarding the interoperability of vehicles with these application platforms, and may result in less choice for users, but also to less data availability for third parties.[80] This is because the gatekeepers could, depending on the depth of their integration into the vehicle system, have incentives to allow third parties to access vehicle data through their operating systems, or at least have incentives to also collect and trade the generated vehicle data.

II. Regulated Access to the Vehicle (Functions and Resources)

31 Since the Data Act already addresses the general issue of access to (vehicle) data, the main focus of the initiative is on the specific problem of access to vehicle functions and resources. Policy option 1 proposes to complement the data access right of the Data Act with equal and non-discriminatory access rights to and transparency about the accessible functions and resources.[81] This would fit to the logic of the Data Act. Again, it is questionable whether a user-centric approach can achieve competition and innovation objectives.[82] However, the manufacturers would still be free to decide which functions and resources they make available, which implies leeway for them to decide for which services they open up their systems and for which not.[83] Additional problems would occur where third parties want to develop novel services that require access to functions and/or resources that the manufacturers are not using themselves. These innovations could be blocked because they would not be covered by the principle of equal, non-discriminatory access.[84] The minimum lists of policy option 2 could solve this problem since now the regulator would decide which

80 Martens (n 28) 13 ff.

81 For most third parties this option seems to be the absolute minimum and thus rather a starting point towards more comprehensive regulations. Since it is unlikely that the data sharing mechanism of the Data Act can solve the data access problems, merely adding functions and resources to this mechanism would be no solution.

82 Wiebe et al. (n 37) 91.

83 Determann/Perens (n 11) even argue that vehicle users should be free to decide which operating system they want to use independent of the vehicle brand.

84 Kerber/Gill (n 68) 7.

functions and resources need to be accessible from every vehicle (if the regulator includes the necessary functions and resources). Such a minimum list would be in line with the existing Type Approval Regulation, which provides such a list in its annex. An open question is whether equal and non-discriminatory access to functions and resources can be understood as FRAND approach, i.e., whether this access would be granted also on fair and reasonable terms. If not, manufacturers could easily set fees and terms that discourage third parties from seeking access.[85]

III. Additional Governance Rules for Access to the Vehicle and its Data

32 In the sectoral regulation additional governance rules need to be defined that alleviate the specific legal uncertainties, economic risks and technical issues. While the Data Act provides such rules, the initiative on access to vehicle data, functions and resources remains rather vague on this topic and only indicates a need for additional rules regarding: (1) fair competition, (2) standardization, as well as (3) cybersecurity, safety, intellectual property rights and data protection.

1. Fair Competition in the Automotive Aftermarket

33 The sectoral regulation has the opportunity to maintain fair competition in the automotive aftermarket. While competition plays only a minor role in the Data Act, the existing Type Approval Regulation has a clear focus on preserving competition in the automotive aftermarket.[86] Two additional important points have to be mentioned here for the leveling of the playing field: the compensation to be paid for the access and the dual role of the vehicle manufacturers.

34 If the sectoral regulation would follow the tradition of the Type Approval Regulation, it would oblige the manufacturers to enable access on a time-based or transaction-based model, and charge reasonable and proportionate fees that do not discourage third party access.[87] The Data Act foresees reasonable and non-discriminatory compensation for access by third parties, to promote the generation and making available of data.[88] Similar to the Type Approval Regulation, this compensation may vary depending on the volume of data and the duration of the arrangement. However, the Data Act allows for a margin (except regarding SMEs),[89] which depends, among others, on the size of the manufacturers' investments into the data collection and the question whether the data is co-generated.[90] As Monti et al. (2022) show, the calculation of the reasonable compensation under the Data Act is very complex and depends on a broad range of criteria that can be individual to the specific data access request.[91] One option to avoid this complex calculation with all its legal uncertainty, would be to oblige the manufacturers to provide access free of charge. This would also solve the inconsistency problem of the Data Act around the dual data-pricing regime.[92] If e.g., a vehicle user wants to share vehicle data with a third party in order to receive a service, the user can access the data free of charge, but may de facto not be able to directly share the data with the third party, nor can the third party access the data free of charge on behalf of the user. As a result, the third party will need to pay the manufacturer for the data access, which will increase the price of the service. Therefore, the user will indirectly pay for the data access.

35 An additional fundamental problem is the conflict of interests that car manufacturers face due to their dual role as service providers and enforcers of the necessary rules for safety, security, privacy etc. This refers to all kinds of certification and accreditation processes that third parties have to undergo. Since it is questionable whether the manufacturer can do this in a fair and neutral manner, third parties demand a "separation of duties", requiring these processes to be performed by a neutral entity.[93] An exemplary issue that could be solved this way is business monitoring. By monitoring exactly who accesses which data, functions and resources, in

85 Kerber/Gill (n 68) 8.

86 See e.g. Regulation (EU) 2018/858 (n 2) Rec. 52. This is done by adopting a purpose-based approach, which includes also independent operators other than repairers (e.g. manufacturers of spare parts and diagnostic tools, data aggregators and publishers) and covers – besides Repair and maintenance information – also a broad range of other essential inputs (e.g. diagnostic equipment, tools, applicable software, training material).

87 Regulation (EU) 2018/858 (n 2) Art. 63.

88 Regulation (EU) 2023/2854 (n 1) Rec. 46.

89 Regulation (EU) 2023/2854 (n 1) Art. 9(1).

90 Regulation (EU) 2023/2854 (n 1) Rec. 47.

91 Monti et al., Study for developing criteria for assessing "reasonable compensation" in the case of statutory data access right – Study for the European Commission Directorate-General Justice and Consumers – Final report, 2022, available at: <https://data.europa.eu/doi/10.2838/19186> last accessed 02.07.2024.

92 Martens (n 28) 10.

93 AFCAR, Creating a level playing field for vehicle data access: Secure On-board Telematics Platform Approach, 2021, available at: <https://www.afcar.eu/access-to-in-vehicle-data-and-resources> last accessed 02.07.2024.) 31. See also Wiebe et al. (n 37) 71 who suggests a trustee solution for a separation of duties.

which intervals etc., the car manufacturers may derive insights into innovation projects, customer relations etc., which may provide them with an additional competitive advantage.[94]

2. Standardization of Access to Vehicle Data, Functions and Resources

36 The Type Approval Regulation obliges standardized access to vehicle repair and maintenance information presented in an easily accessible manner that can be processed with reasonable effort.[95] The data itself has to be in a standardized (or, if not feasible, appropriate) format and also third parties other than repairers shall be empowered to process the data "with commonly available information technology tools and software".[96] Furthermore, the Type Approval Regulation mandates the development of a standardized format for the exchange of data that reflects the needs of manufacturers and third parties alike.[97] In comparison, the Data Act does not require standardization beyond the obligation to make data "easily" accessible.[98] This is reasonable since many different standards for data and interfaces have already been established in different sectors and thus standardization should be done sectorally to avoid straightjacket effects. Therefore, it should be part of the sectoral regulation to find a suitable level of standardization in the automotive industry. In particular for the objective to promote innovation in the mobility sector in general, a certain (high) level of standardization and interoperability is crucial.[99]

37 Standardization is also particularly important for the automotive aftermarket since third parties usually offer multi-brand services (or produce multi-brand parts and tools). Different data formats and qualities, different metadata, different descriptions of functions and resources, different interfaces etc. increases the costs of third parties, drive up prices and may make independent services unattractive. Accordingly, the proposed transparency requirement and the (standardized) minimum lists of accessible vehicle data, functions and resources would be particularly important since they provide third parties with (legal) certainty about what they can at least expect to be accessible.[100] Further need for standardization exists e.g., regarding sector-specific technical and organizational standards for the sufficient anonymization of personal data,[101] technical standards concerning the protection of trade secrets, the development of standard contract terms, or regarding cybersecurity and product safety.[102]

3. Cybersecurity, Trade Secrets & Data Protection

38 Cybersecurity and safety risks have always been among the most important arguments by the manufacturers to justify their exclusive control. While clearly every additional access point creates additional risks, this problem seems to be solvable through appropriate technical and organizational solutions (e.g. certification and accreditation systems).[103] The Data Act mandates secure access for users (Arts. 3(1) & 4(1) DA) and third parties (Art. 5(1) DA), it enables users and data holders to contractually restrict data access or sharing if it could undermine security requirements (Art. 4(2) DA), and prohibits third parties to use data in a manner that adversely impacts the security of the IoT device (Art. 6(2)f DA). Still, according to the regulatory initiative, the Data Act does not adequately consider the possible tradeoffs between access rights and cybersecurity requirements.[104] Additional sectoral rules should ensure the safety and security if access to vehicle data, functions and resources.[105]

39 Closely connected to cybersecurity is the topic of trade secrets that may be part of the data that

94 This problem also relates to the recent discussion that platforms (e.g. Amazon) can potentially use the data on transactions between users and third parties on their platforms to develop better (potentially anticompetitive) strategies. In the connected car discussion this issue exists since 2016 (Mc Carthy et al. (n 8)) and thus years before it has gotten an issue in the Digital Markets Act, and in some provisions of the Data Act.

95 Regulation (EU) 2018/858 (n 2) Art. 61(1).

96 Regulation (EU) 2018/858 (n 2) Art. 61(2).

97 Regulation (EU) 2018/858 (n 2) Rec. 54.

98 The Data Act acknowledges the absence of standards for semantic and technical interoperability as a barrier to data sharing (Rec. 2) but does only refer to standards regarding data processing services and data space.

99 Kerber/Gill (n 68) 10. For such an initiative see: European Commission, A European strategy on Cooperative Intelligent Transport Systems, a milestone towards cooperative, connected and automated mobility, COM(2016) 0766 final; Beyrouty et al., C-ITS Support Study, 2018, available at: <https://op.europa.eu/en/publication-detail/-/publication/426495e6-81c1-11e9-9f05-01aa75ed71a1> last accessed 02.07.2024.

100 Kerber/Gill (n 68) 9.

101 Leistner/Antoine, Attention, here comes the EU Data Act! A critical in-depth analysis of the Commission's 2022 Proposal, JIPITEC 13 2022, 339 (341).

102 Similiar: Wiebe et al. (n 37) 93.

103 Bartsch, et al. (n 13).

104 European Commission (n 5) 3.

105 This could be approach similar to the SERMI certification on access to safety/security-critical repair and maintenance information. See: <https://www.vehiclesermi.eu/>.

has to be made accessible. Granting access to such data risks the secrecy of the trade secret, and thus trade secret protection. While trade secrets are not at all mentioned in the policy initiative, the Data Act clarifies that trade secret protection does not generally shield data holders from data sharing obligations, and provides rules that aims towards preserving the confidentiality of the trade secret.[106] Although this approach has been welcomed by some scholars,[107] there is still legal uncertainty about the protection of trade secrets, which can lead to difficult disputes that can impede the effectiveness of the whole data sharing mechanism.[108] Against this background, a sectoral regulation should aim to reduce this legal uncertainty. This could include the provision of clear and neutral guidelines for manufacturers on how to determine which access risks the secrecy of trade secrets, and the definition of which technical protection measures are necessary and sufficient to protect these trade secrets.

40 A final problem is the issue of protection of personal data. With the Data Act, the correct delimitation of personal data becomes even more decisive.[109] Since the sectoral regulation cannot avoid dealing with personal data,[110] it has to justify the lawfulness of the processing with any of the legal bases defined in Art. 6(1) GDPR. A straightforward solution would be to define the sharing of vehicle data for third parties as processing necessary for compliance with a legal obligation (Art. 6(1)c GDPR).[111] However, consent would still be necessary for sensitive data.[112] This means that some form of consent management may be needed anyways. This may be less of a problem where a user, who is a data subject, requests access/sharing of data that only relates to him/her. However, if the user is a business and the data relates to employees or customers (company fleets, car sharing etc.), or where the user is a data subject, but also other data subjects use the vehicle (e.g., in a family situation), more sophisticated technical solutions are necessary to unequivocally identify the data subject and assign the right data to it. In practice this could be achieved through user accounts, where the vehicle user has to log in prior to every journey. This is mandated by Rec. 21 DA, which states that, where several persons or entities are users, every user should be enabled to have access to his/her specific data. The sectoral regulation may adopt similar provisions and could add to user empowerment by demanding standardized interfaces (login-screens) and to fair competition by ensuring non-discriminatory conditions regarding consent. Another problem in this regard is that there could be situations in which the data holder cannot serve data access or sharing requests without violating the GDPR (e.g., where consent cannot be obtained from every affected data subject).[113] Since Art. 1(5) DA provides priority to the GDPR, a denial of access would likely be justified. This argument could be strategically used by car manufacturers to deny data sharing with third parties. An alternative way to deal with these issues would be consequent and state-of the art anonymization of the data prior to the sharing. The sectoral regulation could pick this way and provide sector-specific guidelines on the necessary technical and organizational means, which would be important, esp. since the Data Act does not provide such information.

106 Regulation (EU) 2023/2854 (n 1) Arts. 4(6) & 5(9). This is complemented by rules which allow the data holder to withhold/suspend the data sharing in specific cases (Arts. 4(7) & 5(10) DA) or, even refuse the data sharing upfront in exceptional circumstances, e.g. where the data holder is highly likely to suffer serious economic damages from the disclosure of the trade secret (Arts. 4(8) & 5(10) DA).

107 Leistner/Antoine (n 101) 341; Metzger/Schweitzer (n 28) 26; also, in favor of this approach and with a view to connected cars, but before the Data Act proposal: van den Boom, Vehicle data controls – Balancing interests under the trade secrets directive, 2022, available at: <https://ssrn.com/abstract=3991561> last accessed 02.07.2024.

108 Leistner/Antoine (n 101) 341ff.; Wiebe et al. (n 37) 86.

109 Drexl, Legal challenges of the changing role of personal and non-personal data in the data economy. In: De Franceschi, Schulze (eds.), Digital Revolution: Data Protection, Smart Products, Blockchain Technology and Bitcoins Challenges for Law in Practice, München, Beck, 2019, 19-41.

110 In many cases (such as providing data for traffic management) the data might be anonymized before it is shared, however, esp. in situations where a specific user (data subject) requests a specific aftermarket service, such as repair and maintenance, the service provider can and needs to identify this user.

111 For such an approach with regard to the DA see: Leistner/Antoine (n 101) 341.

112 For the definition of "sensitive data" see Rec. 51 GDPR. In the case of connected cars, every data that reveals information about mobility patterns of individual persons (e.g. to which churches, political events, or other cultural activities the data subject drives) may be defined as sensitive.

113 Bomhard/Merkle, The Draft of the Data Act, Law Digital RDi, 2022, 168, (172).

Table 1: Overview about policy recommendations for a sectoral regulation

1. Scope of access to vehicle data	• Ensure a purpose-based scope of data by including all the data (and only those) that are necessary for third parties to independently and effectively and compete in the aftermarket o independent of the level of processing of the data o independent of whether it is personal data or not o independent of trade-secrets o independent of safety/security considerations • Provide a minimum list of data to be made available to achieve further objectives in the mobility ecosystem in general
2. Scope of access to vehicle functions and resources	• Basically, similar approach as for vehicle data (scope has to fit the purpose of enabling independent and effective innovation and competition)
3. Sharing mechanism for access to vehicle data, functions and resources	• Enable users to effectively share data with third parties, e.g. by making "in-situ" access the exception • Enable users to install third party applications that then can have directly access to vehicle data, functions and resources
4. Additional governance rules	• Compensation: o either establish a FRAND based compensation regime o or empower the user to authorize third parties to access vehicle data, functions and resources free of charge • Establish specific sectoral rules to: o ensure the safety and security of access o ensure the protection of privacy o ensure the protection of trade-secrets • Facilitate the standardization of: o data formats, data quality, semantics, metadata o interfaces (for users and third parties) o safety/security requirements (authorization, accreditation) o anonymization and means to provide consent • Regulate the contract between user and manufacturer, e.g.: o duration and breadth of contract (prevent total buy-out) o possibility for user to discontinue data sharing without losing functionality of the device • Regulate the relation between gatekeepers (DMA) and automotive stakeholders with a view to competition and innovation in the mobility system

E. Conclusion

41 The Data Act is the preliminary apex of EU data regulation and a milestone of innovative law, which is not based on a classical market failure logic but constitutes a market-shaping approach.[114] Its clarification that it is no longer the de facto data holder, but the user (private or business) of the IoT device who should have control over the use and sharing of the generated data represents a fundamental readjustment of the monetization opportunities in the data economy.[115] However, in general – and especially in B2C situations – the Data Act does not challenge the gatekeeper-like position of manufacturers vis-à-vis users and third parties. Through technological design and contractual arrangements, the manufacturers may be able to keep de facto control over the data and therefore significant improvements for competition and innovation in data-driven secondary markets are hardly imaginable. The same holds for the problem of access to the vehicle and its data. The Data Act may weaken the exclusive control of vehicle manufacturers over the vehicle data but does not challenge the de facto control of the vehicle manufacturers. While the data access and sharing rights may slightly improve the data availability for vehicle users and third parties, it cannot be expected that this systematically enables third parties to effectively compete. This is mainly because the Data Act does not regulate the sector-specific issues around access to vehicle functions and resources, but also due to a series of limitations, imbalances, and legal uncertainties around access to vehicle data. Moreover, the Data Act does not provide a level playing field between car manufacturers and third parties regarding the utilization opportunities of the data. As a consequence, additional sectoral rules are necessary to ensure competition and innovation in the automotive aftermarket.

42 The European Commission has acknowledged some of these limitations and published an initiative for a sectoral regulation. This paper has analyzed the different policy options of this initiative in conjunction with the rules of the Data Act and the traditional approach of the existing regulation on access to repair and maintenance information. The analysis in chapter 4 shows that, while the objectives of the sectoral regulation are consistent with the Data Act, the basic data sharing mechanism in the sectoral regulation may rely much less on the car user. Clearly, the user would still be in the position to authorize access to the vehicle and its data for certain services, but the actual process of sharing this access may be much more direct (in line with the Type Approval Regulation), i.e., would be initiated

114 Metzger/Schweitzer (n 28) 49.

115 Hennemann/Steinrötter (n 19) 8.

by third parties and rely much less on the strategic decisions of the vehicle manufacturer. However, since the initiative is very vague on this point, other scenarios are also imaginable, e.g., that any future sectoral regulation will be aligned with the Data Act principles, by including a user-centric data sharing mechanism. In this case, this paper argues that no facilitation of competition and innovation can be expected. This shows one of the core conflicts between the objectives of the sectoral regulation and the Data Act: User empowerment – an important target in itself – may not automatically lead to improved data sharing for better competition and innovation.

43 It seems the regulator has two ways to deal with this fundamental conflict. Both ways can only be outlined here: The first option would be to stay within the current line of thinking, i.e., to accept the exclusive initial control of the car manufacturers and to improve this regulated access system in a way that enables third parties to independently and effectively compete. This would require a strong sectoral regulation with FRAND access conditions and far-reaching standardization (e.g., of user interfaces) and sectoral specifications of the Data Act (e.g., safety & security, IPRs and data protection) that should aim to create a more level playing field regarding competition between car manufacturers and third parties. The second, and much more radical, option would be to not accept the exclusive initial control of the car manufacturers and thus to avoid (a priori) many of the problems that the Data Act and the initiative want to solve. There are again two options: Either (1) mandating the introduction of a shared server through which car manufacturers and third parties can access vehicle data, functions and resources on FRAND terms, which is managed and operated by a neutral organization. Or (2) mandating the implementation of an On-Board Application Platform, through which third party applications have the same direct access as the manufacturers. Both of these alternative solutions also require extensive regulation, and therefore a sectoral regulation needs to be introduced anyways.