

Designing Data Trustees – A Purpose-Based Approach

Louisa Specht-Riemenschneider
Wolfgang Kerber



Designing Data Trustees – A Purpose-Based Approach

Louisa Specht-Riemenschneider
Wolfgang Kerber

Imprint

Published by:

Konrad-Adenauer-Stiftung e. V. 2022, Berlin, Germany

Design and typesetting: yellow too Pasiek Horntrich GbR

The print edition of this publication was climate-neutrally printed by
Druckerei Kern GmbH, Bexbach, on FSC certified paper.

Printed in Germany.

Printed with financial support from
the German Federal Government.



The text of this publication is published under a Creative Commons
license: “Creative Commons Attribution-Share Alike 4.0 international”
(CC BY-SA 4.0), <https://creativecommons.org/licenses/by-sa/4.0/legalcode>

ISBN: 978-3-98574-044-4

The Authors

Prof Dr Louisa Specht-Riemenschneider is Professor of Civil Law, Information Law and Data Law at the University of Bonn and Head of the Research Unit for Legal Issues of New Technologies and Data Law. She is deputy chairwoman of the Expert Council for Consumer Affairs at the Umweltbundesamt (Federal Ministry for the Environment, Nature Conservation, Nuclear Safety and Consumer Protection). Louisa Specht-Riemenschneider works on all aspects of data law and data protection law, as well as on copyright law, media law and consumer protection law.

Prof Dr Wolfgang Kerber is Professor of Economics at University of Marburg. Since 2015 he is working on various research topics about the regulatory challenges of the digital economy. He has published about competition problems of large digital platforms (e.g. the Digital Markets Act), data policy and data rights, data access rights in competition law, data governance problems of IoT devices (especially the connected car), as well as data protection and consumer protection problems on digital markets.

Contact:

Dr Pencho Kuzev

Konrad-Adenauer-Stiftung

T +49 30 / 26 996-3247

pencho.kuzev@kas.de

At a Glance

Data trustees and data intermediaries could play a key role in the data economy in the future, facilitating the aggregation and sharing of significant amounts of relevant data while having the potential to ensure the protection of conflicting rights and legal interests. This key role requires the creation of a workable legal framework for such data trustees and intermediaries which are socially and politically desirable. In our study, we present various problems in three different sectors that can be solved with the involvement of data trustees.

Data trustees in the healthcare sector

In the healthcare sector, we face the problem of insufficient aggregation and analysis of data for research purposes. One solution could be to allow the combination of data sets and their processing for medical research purposes in so-called data clean rooms that meet the highest IT security standards. They also ensure that any evaluation is solely for research purposes in the public interest and that the data is not accessible to third parties, including the data providers themselves.

Data trustees in the online sector

In contrast to the healthcare sector, there is no underuse of data in the online sector but rather an overuse of personal data, sometimes in violation of data protection law. A solution is needed that gives users greater control over their data. Personal Information Management Systems (PIMS) are that solution.

Data trustees in the form of PIMS can function as “consent assistants”. PIMS already exist in the market, but they are underutilised because the benefits to data subjects are lacking. To change that, we need policy decisions that lead to system-level regulation. What does that mean? Firstly, we need an obligation to consider the specifications that PIMS impose on data processors. What is needed, secondly, are interoperability standards. Currently, European and national legislators are focused on regulating details, especially measures to minimise the risks of PIMS. These risk minimisation measures are just as necessary as general clarifications in the legal framework for data protection (possibility of declaration of

consent by PIMS, broader possibility of consent vis-à-vis PIMS, possibility of exercising data subject rights by PIMS). However, if PIMS is to be able to function as a problem-solving option, it at first and foremost requires the aforementioned regulation at the system level. Without this, any detailed regulation runs the risk of becoming pointless and futile because it will not lead to PIMS being used. In addition, a decision also needs to be made about how to fund and organise PIMS.

Data trustees in the mobility sector

In the mobility sector, data trustees can be a suitable instrument for solving access problems relating to certain mobility data. There, large amounts of data are generated by drivers through the operation of connected and automated vehicles by a variety of sensors (technical data, driving behavior of car users, environmental, traffic, weather data, etc.). This data could in turn be used by many companies as well as by public institutions for traffic regulation and safety, accident research, etc., as well as for scientific research and thus for public benefit purposes.

For several years a large conflict exists about the “extended vehicle” concept of the vehicle manufacturers, which enables them to get exclusive control over all these data and over the technical access to the vehicle. This leads to their control of the access to the ecosystem of connected driving (gatekeeper position).

A data trustee founded on a legal basis, which has this data generated in the vehicles under its control and makes it available as a “neutral entity” according to legal requirements and principles to the stakeholders of this ecosystem, the data economy as well as public institutions and science for public welfare purposes, would be a possible solution option. It would preemptively prevent the emergence of such a gatekeeper position for car manufacturers, thereby safeguarding competition, innovation, and freedom of choice for car users. Furthermore, such a data trustee could possibly also achieve a much better use of this large amount of mobility data (data as infrastructure) than would be the case with monopolistic control of the data by the car manufacturers. Specifically, two other data access solutions to this mobility data are currently under discussion:

- › Regulatory FRAND (“fair, reasonable, and non-discriminatory”) access solution: this involves strict regulation of access to this connected car data according to so-called FRAND conditions.
- › “On-board application platform”: this is about the introduction of an alternative technical solution that, through a standardised open and interoperable telematics solution, opens up the possibility for car users themselves to exercise control over the data they generate in the vehicle and allow other service providers to access the connected car.

Beyond solving this competition problem, we believe that a data trusteeship solution opens up other exciting prospects for efficient use of these very large volumes of mobility data in the future, oriented toward public welfare goals.

Content

1 Introduction	7
2 Course of the Investigation	11
3 Categorisation of Data Trustee Models	12
4 Requirements of the Data Governance Act for Data Trustees	15
4.1 Data Trustee in State Sponsorship	15
4.2 Data Trustee in Private Sponsorship	16
4.3 Data Altruistic Organisations	19
5 Problem-solving Design of Data Trustees	22
5.1 Data Trustees in the Online Sector	22
5.2 Data Trustees in the Health Sector	40
5.3 Data Trustees in the Mobility Sector	53
6 Summary of the Results in Legal Policy Recommendations for Action	87

1 Introduction

Data trustees are discussed as a key element for solving a multitude of problems. Yet, even the concept and its differentiation from data intermediaries is conceivably unclear. The European Data Strategy describes them as a tool and means for affording internet users the possibility to make their own decision about what happens to their data. There are “novel mediators in the personal data industry”¹. The European Data Strategy therefore addresses ideas of the Data Ethics Commission and also explicitly refers to them. The Data Ethics Commission adopts a narrow interpretation of the concept of data trustee to mean Privacy Management Tools and Personal Management Information Systems. It associates it with both the opportunity for “digital self-determination” and the fear of “reckless heteronomy”.² The German data strategy equates the data trustee with the concept of a Personal Information Management System, while this understanding also prevails in British legislation.³

Consideration is also given to data trustees in other contexts, such as the health sector, in the form of so-called “data clean rooms” for merging and evaluating large databases. Data from automated driving vehicles is already being stored in the Federal Motor Transport Authority’s research data centre, whose function as a data trustee could also be subject to discussion. A data trustee could also be imagined for mobility data from public transport or for agricultural vehicles that collect data during operation such as data on soil condition which are not to be solely available to the sensor manufacturer or the manufacturer of the agricultural vehicle, but also to other persons such as the farmer, via the data trustee.⁴

There is no point in defining or analysing the data trustee based on the various trustee concepts of member states’ legal systems. However, such an approach is also not necessary when it comes to adequate regulation. Instead, it is necessary to phenomenologically understand for what reason instruments referred to as a data trustee are to be developed, and which properties they need to possess for this. The demarcation between data trustee and data intermediary for this purpose may lie solely in the binding of the data processor to the interests of

the data provider in the internal relationship. A data trustee must align their actions with the interests of the other contracting party. Their own interests need to take a back seat where necessary.⁵ However, the data intermediary is not bound in this way in the internal relationship. “Data intermediary” is therefore the umbrella term, while “data trustee” is a sub form that can in turn be structured differently. Based on this understanding, Personal Information Management Systems are only one possible form of a data trustee. A data escrow which is comparable to a software escrow, for example, is also subject to a fiduciary bond.⁶ Here cryptographic keys can be recorded that grant authorised third-party access to encrypted information.⁷

Data trustees therefore have the potential to exhibit a wide range of functions, making it difficult to develop an appropriate legal framework for data trustees. This report suggests the design of a problem-orientated legal framework depending on the specific problem for which data trustee models are used.

A careful analysis of problems to be resolved with respect to the governance of data is needed for designing data trustees in a way that is orientated toward problem-solving. The question arises as to whether a data trustee solution is suitable for resolving these problems, and how it needs to be designed based on the specific technological and economic conditions. Here, a distinction should be made between data trustees that are formed through free agreements, for instance between companies, to specifically resolve complex data governance problems in a group of companies, and those data trustees that are part of a state’s regulatory solutions in order to solve market failure problems, for example due to market power or information asymmetry problems, or to achieve other public welfare goals such as scientific research in medicine. Recognising that data trustees are problem-solving tools, the obvious question is invariably whether a data trusteeship solution is better suited than other potential solutions. This question can be answered differently depending on the problem and specific context. What is more, it often proves to be the case that a pure data trusteeship solution does not suffice, for instance for solving competition problems and thus other measures such as complementary regulations for solving

data access and interoperability problems or for ensuring a high level of security are needed so that an effective solution can actually be found. In this respect, a data trustee can also represent a component within a complex regulation solution for a certain problem, which then needs to be adjusted to the overall solution accordingly.⁸

Owing to the diversity of data trustee solutions, the legal framework for such data trustees must not be a one-size-fits-all solution either.

The Data Governance Act (DGA) was originally only intended to apply when it enables data sharing on a voluntary basis, not when it is used as an instrument for satisfying claims for data access under statutory provisions.⁹ However, this is explicitly revoked in the Council’s draft Data Governance Act of 7 September 2021 (DGA-E). A mandatory data access mediation as the task of a data trustee is now also covered pursuant to Art. 2 No. 7 DGA-E.

Sector-specific regulation for data trustees could be designed in line with the data rooms announced by the Commission.¹⁰ Current discussions about data trustee models are mainly taking place in the health¹¹ and mobility sector¹² as well as with regard to Personal Information Management System (PIMS).¹³ The European Health Data Space Act and the design of a mobility data room provide an opportunity for a functional legal framework of sector-specific data trustee models. The European Data Strategy also talks about its intention to design “personal data spaces”, which should enable the individual to make in-depth decisions about what happens to their own data and thus improve monitoring of their own data.¹⁴ The European Commission presents the prospect of guaranteeing these instruments, which is likely to mean PIMS, in the Data Act, which was announced for the fourth quarter of 2021 but has now been postponed to Q1/2022.¹⁵

Using the example of these three pending data trustee models (data trusteeship model in the health sector, in the mobility sector and Personal Information Management Systems (PIMS)) to be designed in the corresponding data spaces announced by the Commission, the below investigation will show the following:

- a. Which problems can be solved with the corresponding data trustee models,
- b. How a data trustee would have to be functionally designed to resolve the problems identified
- c. Which legal framework is needed in each case, and
- d. Whether and to what extent the Data Governance Act and, if applicable, national legislation contribute toward resolving the problem.

2 Course of the Investigation

The following will highlight the fundamental models of the actual design options for data trustees (3), each of which is associated with various risks and opportunities. This fundamental modelling is independent of specific functions that data trustees can assume beyond communicating access to data and data analysis (e.g. anonymisation, pseudonymisation, data evaluation). Subsequently, the goals and benchmarks of the Data Governance Act are outlined (4) in order to develop – inversely to some extent – a solution-based legal framework (5) for PIMS (5.1), data trustees in the health sector (5.2) and data trustees in the mobility sector (5.3). The investigation closes with a summary of results in legal policy recommendations for action.

1 Europäische Datenstrategie, p. 12.
 2 Gutachten Datenethikkommission, October 2019, p. 133, available at: https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/gutachten-datenethik-kommission.pdf;jsessionid=92AD72B05F123D4DBFCC72D56297DE96.2_cid295?__blob=publicationFile&v=6 (last accessed on: 18/11/2021).
 3 *Delacroix/Lawrence*, International Data Privacy Law, 2019, p. 236 et seq.
 4 Cf. for example *Zech*, CR 2015, 137, 137.
 5 *Martinek/Omlor*, in: Staudinger, BGB, 2017, preliminary remarks on § 662 Ref No. 26; cf. also *Specht-Riemenschneider/Blankertz et al*, MMR-Beil. 2021, 25 (34).
 6 In-detail on Escrow software *Auer-Reinsdorff/Kast/Dessler*, in: Auer-Reinsdorff/Conrad, Handbuch IT- und Datenschutzrecht, 3rd edition 2019, § 38 IT in der Insolvenz, Escrow Ref No. 58–105.
 7 Cf. for example: <https://www.deposit-software-escrow.de/zugangsschlüssel-key-escrow> (last accessed on: 18/11/2021).

8 Cf. from an economic perspective on data trustee solutions as an element in data governance systems *Kerber*, in: Drexl, Data Access, Consumer Interests and Public Welfare, 2021, pp. 468–471.
 9 See Richter, ZEuP 2021, pp. 634, 666.
 10 COM (2020) 66 final.
 11 Cf. for example *Martini/Hohmann*, NJW 2020, 3573 (3575).
 12 *Steinrötter*, ZD 2021, 513 (516).
 13 *Wendehorst/Schwamberger/Grinzinger*, in: Pertot (ed.), Rechte an Daten, 2020, p. 105; Data Ethics Commission Expert Opinion, October 2019, p. 133, available at: https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/gutachten-datenethikkommission.pdf;jsessionid=92AD72B05F123D4DBFCC72D56297DE96.2_cid295?__blob=publicationFile&v=6 (last accessed on: 18/11/2021); *Golland*, NJW 2021, 2238; *Sesing* MMR 2021, 544.
 14 Europäische Datenstrategie, p. 23.
 15 Europäische Datenstrategie, p. 23.

3 Categorisation of Data Trustee Models

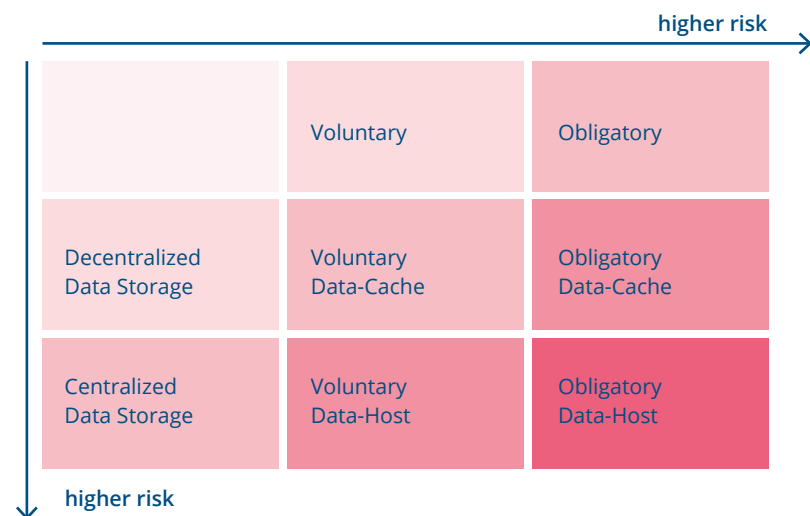
If we understand the data trustee, as is done here, as a natural or legal person or partnership that mediates access to data or data analysis results provided or held by data owners in accordance with contractually agreed or legally prescribed data governance regulations in third-party interests, then we can think of possibilities for designing data trustee models in four basic forms, which essentially differ according to the type of data storage (centralised or decentralised) and the type of use (obligatory or optional).¹⁶ What is more, data trustees also need to be distinguished according to whether they are offered by the private sector or the state. Regardless of this basic modelling, data trustees can also perform a number of other functions. For instance, they could perform the function of anonymisation or pseudonymisation of data or processing of data in another way. The same applies to any powers to create and/or use metadata.¹⁷

Decentralised storage affords the data owner with the advantage that he or she retains technical control over the data. Central storage with the data trustee promises simpler, standardised management of the data by the data trustee. As a rule, data protection and security considerations speak against central storage at the data trustee. If a large amount of data accumulates with a data trustee, it increases the risk of misuse. What is more, the potential damage is higher in the event of attacks against the intermediary. However, sometimes it may be necessary to store data centrally with a data trustee, for example to exclude the data processor from access, as was the case with the Microsoft Cloud.¹⁸ A combined solution is also possible, in which data is temporarily merged and encrypted, processed in the secure sphere of the data trustee and then deleted again, as is the case in the Data Clean Rooms of various young companies.¹⁹

The use of facultative data trustee models is based on the free decision of parties involved, especially the data subject or the technical-factual data owner. In the course of this, parties conclude a data trustee agreement which forms the basis of this legal relationship. On the other hand, obligatory data trustee models are characterised by technical-factual data owners being legally obliged to use the data trustee models in certain processing situations or to outsource their data to the data trustee altogether. The latter may be an important solution especially for such cases where the technical-factual data owner is not the (only) legitimate data owner.²⁰

Voluntary models are conceivable, for example, for the state agricultural data platform envisaged in the Federal Government's data strategy, for bio databases, for sharing hospital data for research purposes or for creating a "circular data space" for digital product passports.²¹ Obligatory data trustee solutions may be made mandatory in their use for one or more sites. For example, an idea would be an obligation to cooperate with PIMS for companies so that data subjects could encourage data processors to request access via a PIMS to data that goes beyond the provision of a service. Provided it is obliged by fiduciary ties to the data provider, for example to keep its business secrets, an obligatory data holder is also the research data centre of the Federal Motor Transport Authority ("Kraftfahrtbundesamt"), by storing data from the automated car and making it accessible from there, for example for research.

Figure 1



according to Specht/Blankertz et al.²²

16 Specht-Riemenschneider/Blankertz et al., MMR-Beil. 2021, 25.

17 Cf. zum Begriff der Metadaten Martini, in: Paal/Pauly, 3. Edition. 2021, GDPR Art. 30 Ref No. 11.

18 Wendehorst/Schwamberger/Grinzinger, in: Pertot (ed.), Rechte an Daten, 2020, p. 110.

19 For example, Apheris, www.apheris.com und Decentriq, www.decentriq.com. Cf. also Specht-Riemenschneider/Radbruch, Deutsches Ärzteblatt, number 27/28 in 2021, available at <https://www.aerzteblatt.de/archiv/220270/Datennutzung-und-schutz-in-der-Medizin-Forschung-braucht-Daten>

(last accessed on: 18/11/2021); cf. also Specht-Riemenschneider/Blankertz et al., MMR-Beil. 2021, 25 (29 et seq.).

20 Cf. also alledem Specht-Riemenschneider/Blankertz et al., MMR-Beil. 2021, 25 (29 et seq.).

21 Specht-Riemenschneider/Blankertz et al., MMR-Beil. 2021, 25 (30). Similar Bundesdruckerei, Der Datentreuhänder, November 2019, p. 2, available at: https://www.bundesdruckerei.de/system/files/dokumente/pdf/BDR.de_Datentreuhaender.pdf.

22 Specht/Blankertz et al, MMR-Beil. 2021, 25 (32).

4 Requirements of the Data Governance Act for Data Trustees

On 25 November 2020, the European Commission presented its proposal for a Regulation on European Data Governance (draft of the Data Governance Act, DGA-E),²³ which aims to create a harmonised framework for data exchange within the EU and thus improve conditions for data sharing in the Single Market (Rec. 3 et seq. DGA-E). Data sharing is an important factor for the European Commission in increasing the welfare of society as a whole, which is based on the assumption that improved access to data also leads to enhanced innovation.²⁴ This is a horizontal regulation (Rec. 3 DGA-E), which, however, only specifies minimum requirements and can thus be supplemented by sector-specific regulations such as in the European Health Data Space, in regulations for a mobility data space or for a personal data space (Art. 1 (2) DGA-E).²⁵ Its total of 35 articles is divided into eight chapters, some of which are more substantive, while others are more procedural. For data trustees, there are the following regulations:

4.1 Data Trustee in State Sponsorship

The second chapter of the Data Governance Act regulates the re-use of certain categories of public sector data, in which third party rights exist. The categories of data covered can be found in Art. 3 DGA-E: It makes positive mention of public bodies' access to data, which are protected for reasons of commercial or statistical secrecy or are subject to the protection of intellectual property or data protection (Art. 3 (1) DGA-E). This may also include data stored with a trustee or mediated by the latter, for example data from cancer registers of the countries or the Robert Koch-Institute. It is clarified that the provisions of the DGA-E do not obligate public bodies to allow the re-use of data, and that these provisions also do not affect existing confidentiality obligations of public bodies (Art. 3 (3) p. 1 DGA-E). However, if public bodies allow the re-use of data, they must comply with the requirements of Chapter II DGA-E. Corresponding agreements must not in principle lead to the granting of exclusive rights (Art. 4 (1) DGA-E). Such an exclusive agreement may only be

concluded in exceptional cases, which must fulfil the requirements set out in Art. 4 (2–6) DGA-E. This serves to comply with the requirements of (public) commercial law (Rec. 9 DGA-E). Art. 5 then regulates both the substantive requirements for the conditions, which public bodies may impose for access to the re-use of data (particularly Art. 5 (2–5) DGA-E) as well as their mandatory public access (Art. 5 (1) DGA-E). It also contains more detailed provisions with regard to the protection of intellectual property rights and sensitive commercial data, particularly for re-use of data in a third country (Art. 5 (7–13) DGA-E). The fees which public bodies may charge for the re-use of data are regulated by Art. 6 DGA-E. In order to create incentives for the re-use of data in research and innovation, they are free to charge no or only low fees (Rec. 20 DGA-E). An incentive for re-use should also be the mandatory, cross-sectoral establishment of competent bodies in Member States, which support public bodies with granting access, according to Art. 7 (1) DGA-E (cf. also Art. 7 (2) DGA-E, Rec. 21. DGA-E). To this end, they should provide them with modern technology in particular (Rec. 21 DGA-E). If necessary, they should also be allowed to take action themselves in order to grant re-use (Art. 7 (3) DGA-E). The procedure in which this access can be requested is prescribed by Art. 8 DGA-E: A central information body needs to be established to provide information about the conditions of access including fees and to accept as well as forward corresponding applications to the competent public bodies (Art. 8 (1, 2) DGA-E). These applications must be processed within an appropriate period of a maximum of two months (Art. 8 (3) DGA-E). Data subjects are entitled to an effective judicial remedy against the decision on this (Art. 8 (4) DGA-E).

4.2 Data Trustee in Private Sponsorship

The third chapter of the DGA-E creates a legal framework for services for data sharing, the so-called data intermediaries. The aim is to promote the availability and usability of data. A “European Data Exchange Model with Trusted Data Intermediaries for B2B Data Use and for Personal Data Spaces” is to be created.²⁶ It is assumed that data availability is economically necessary and that a lack of data sharing in the private sector can mainly be attributed to a lack of trust in the use of data intermediaries.²⁷ It also aims to establish improved control over access to data and its use

in accordance with Union law. Based on this goal, in Chapter 2 “services for data sharing”, the Data Governance Act essentially commits to additional requirements whose fulfilment is intended to strengthen trust in the use of the services.

4.2.1 Data Intermediaries Addressed

Initially, only service providers for data sharing are addressed, whose main objective is to establish a commercial, legal, and possibly technical relationship between data holders (including data subjects on the one hand, and possible users on the other), as well as to support parties in the transaction of data assets between them. It is also required that the service offered targets the transfer between an indeterminate number of data holders and data users, but not data sharing intended for a closed group of data holders and users. Also not covered are services that collect data from data holders, aggregate, enrich and transform it, and license the resulting data to data users without establishing a direct relationship between data holders and data users (Rec. 22). However, providers that do not operate for profit on the basis of data altruism will be exempted from the scope of Chapter III in Art. 14 DGA-E.

Chapter II therefore covers platforms for data exchange (Rec. 22), such as Airbus’ Skywise data exchange platform, Personal Information Management Systems (Rec. 23) and data cooperatives (Rec. 24). Chapter III also addresses data altruistic organisations as special data intermediaries that provide data for purposes of general interest based on data altruism.

4.2.2 Requirements of the Data Governance Act

Those who wish to provide services for data sharing within the meaning of Art. 9 (1) DGA-E must initially undergo a registration procedure (Art. 10 (1) DGA-E), which is set out in more detail in Art. 10 (6–10) DGA-E. However, an approval by the competent authority is not necessary (Rec. 30 DGA-E); if applicable, it only confirms the application (Art. 10 (7) DGA-E). For the implementation of the registration procedure, a “one-stop-shop” solution was selected whereby data intermediaries are only subject to the jurisdiction of the Member State in which they have their principal place of business or in which their legal representative is estab-

lished (Art. 10 (2,3) DGA-E). Registration entitles the data intermediary to provide their services throughout the whole EU under the conditions set out in Art. 11 DGA (Art. 10 (4,5) DGA-E). These conditions are largely identical for the three very different data intermediaries in Chapter 2 (with the exception of additional requirements for PIMS, see below):

- › Neutrality requirements: Services shall only operate as an intermediary and they shall not use the data for any other purpose.
- › The meta data may only be used for further developing the service.
- › Structural separation between the service for data sharing and all other services provided to avoid conflicts of interest (prohibition of vertical integration)
- › Transparent and non-discriminatory access to the service
- › Requirements for data formats
- › Have procedures to prevent fraudulent or abusive practices regarding access to data
- › Take appropriate technical, organisational and legal measures to prevent unlawful access and unlawful transfer of personal data
- › Ensure a high level of security when storing and transmitting non-personal data
- › Obligation to establish oneself in the EU
- › Registration procedure
- › Trusteeship duties for PIMS

Art. 12 (1) DGA-E lastly obliges Member States to designate competent authorities for this purpose. The supervisory and oversight powers of these authorities are determined in Art 13 DGA-E. In particular, they can impose measures such as deterrent fines to ensure compliance with the requirements of the DGA-E for data intermediaries (Art. 13 (4) p. 2 lit. a) DGA-E).

4.3 Data Altruistic Organisations

The fourth chapter will create a legal framework for data altruism with the aim of establishing trust among data holders to voluntarily share their data (Rec. 36 DGA-E). This should contribute toward the emergence of data sets in the EU large enough to enable data analytics and machine learning (Rec. 35 DGA-E). Based on this goal, a register of recognised data altruistic organisations should be maintained at national and EU level according to Art. 15 DGA-E. Those organisations should be able to collect data directly from data subjects as well as process data collected by third parties (Rec. 38 DGA-E). The requirements that an institution must fulfil to be entered in the register are determined in Art. 16 DGA-E. In particular, it must be non-profit (Art. 16 lit. b) DGA-E). Requirements and procedures for registration are governed by Art. 17 DGA-E. A one-stop-shop approach is also selected for this registration (Art. 17 (2,3) DGA-E). Recognised data altruistic organisations are obliged, in the interest of transparency, to record certain information on an ongoing basis, for example about persons who were able to process data in their possession (Art. 18 (1) DGA-E). They must also draw up an annual activity report (Art. 18 (2) DGA-E). If they communicate personal data, Art. 19 DGA-E imposes additional obligations on them to protect it. For example, they must ensure that data processing is only carried out for the purposes for which data has been provided to them (Art. 19 (2) DGA-E). Finally, Art. 20 DGA-E obliges the Member States to appoint the authorities responsible for this. Their monitoring and supervisory powers are governed in Art. 21 DGA-E. In particular, violations against the Regulation by a recognised data altruistic organisation may lead to its removal from the register (Art. 21 (5) lit. b) DGA-E). Subsequently, Art. 22 DGA-E provides for the development of a European consent form for data altruism, which aims

to facilitate the collection of data by creating both legal security for data users and transparency for data holders (Rec. 39 DGA-E).

The following requirements are imposed on data altruists:

- › Entry in the register of recognised data altruists, Art. 15
- › Distinct legal personality, Art. 16
- › Founded to pursue general interest objectives, Art. 16
- › Operating on a non-profit basis and independently of any organisation pursuing profit-making purposes, Art. 17
- › Data altruism activities are carried out through a legally independent structure that is separated from other activities which it conducts, Art. 17
- › Establishment in a Member State or appointment of a legal representative in a Member State, Art. 17
- › Transparency requirements, Art. 18
- › Information obligations and ensuring purpose limitation, Art. 19

Unlike with regard to the data intermediaries of the second chapter, the registration of the data altruists also brings some benefits: For the collection of data based on data altruism, the Commission may adopt implementing acts to determine a European consent form for data altruism. This could counteract the often-bemoaned lack of legal security as regards obtaining consent under data protection laws.

23 COM (2020) 767 final.

24 *Richter*, *Europäisches Datenprivatrecht*, ZEuP 2021, pp. 635, 639.

25 Also, in the individual chapters (see for example Art. (3) 3 p. 2, 4, Art. 9 (2) 2 DGA-E) as well as in the recitals (see for example ErwG. 12 et seq., 28 et

seq., 34, 44) repeatedly emphasises that such guidelines remain applicable in addition; this also applies to the explanatory memorandum, cf. COM (2020) 767 final, p. 2.

26 COM (2020) 767 final, p. 3.

27 COM (2020) 767 final p. 7.

5 Problem-solving Design of Data Trustees

In addition to the horizontal requirements of the Data Governance Act, scope remains, as shown, for sector-specific and problem-solving regulation that complies with the minimum requirements of the DGA-E. Theoretically, the GDPR provisions could be derogated from by means of *lex posterior*, but it should be demonstrated that a problem-solving legal framework in the online sector and the health and mobility sector could be realised without such deviations. However, clarifications would be needed in any case. The following section will initially outline a problem-oriented legal framework for data trustees in the online sector, then for the health sector and finally the mobility sector.

5.1 Data Trustees in the Online Sector

Especially in the online sector, there is currently a considerable overuse of personal data, and in some cases a use in violation of data protection and consumer protection law. This can largely be attributed to an information overload of users and an enforcement deficit under data protection law. These two problems lead, for example, to cookie banners simply being clicked away and data protection declarations not being read. Solving these two problems would already be of great help. Both problems could be contained via PIMS.

In addition, however, there is also a competition problem when consents under data protection law are declared *vis-à-vis* large online platforms.²⁸ The removal of functional deficits in data protection law alone will thus not result in a functioning data protection law in this area: Even if the data subject fully accepts the information under data protection law and is aware of the risks under data protection law, the data subject will still consent to large online platforms processing personal data concerning them if they have to continue using the data processing service, e.g. social media platform, because friends and acquaintances also use this service owing to its market dominance. This also explains why data sub-

jects indicate that they have considerable worries about the handling of their personal data, but in practice they fully consent to the processing of this data, especially when it is necessary for the purpose of using large online platform.²⁹ All three problem complexes will be explained in the following.

5.1.1 Analysis of the Problem

5.1.1.1 Information Overload

The right to informational self-determination reserves the right for individuals to decide on the disclosure and use of their personal data.³⁰ In principle, individuals are free to disclose data to others as long as they act freely and autonomously.³¹ However, only those who make their decision knowing the circumstances relevant to the decision, for example purpose and scope of data processing, are free to decide about the disclosure of personal data and consent to data processing. For this purpose, data protection law standardises considerable information obligations that the data processor must fulfil. However, data processors do not have to ensure the success of the information. The data subject itself is responsible for taking note of the information under data protection law. This is also why most data protection declarations do not seem to aim toward transparency, but merely represent a legal safeguard for the use of data.³² A study in which Facebook users were asked whether they had given their consent to Facebook processing their data, for example, comes to the conclusion that only 37 per cent of users felt they had given their consent to Facebook to collect and use their data. 43 per cent of respondents declared that they had no knowledge of this and another 20 per cent believed that they had never given such consent.³³ A large part of the declarations of consent under data protection law are therefore made without the data subject being aware of the information under data protection law. They consent without knowing which data processing operations they are consenting to³⁴ or that they even consent at all. That is mainly due to the problem of information overload: Investigations in consumer behaviour research show that an increasing amount of information initially contributes to an increase in subjective decision-making efficiency.³⁵ However, once a certain amount of information is exceeded, the data subject is no longer able to actually assimilate information provided to them in view of limited cognitive abil-

ities.³⁶ Not only does the intake of information decrease on the whole, it may also result in the discontinuation of the entire information intake.³⁷ In the context of data protection law, we can generally observe that the data subject merely scrolls to the end of the data protection declaration and ticks the consent box without actually reading the privacy statement.³⁸ 78 per cent of Facebook users surveyed in the above-mentioned study stated that they had not read or merely skimmed through the data protection regulations.³⁹ That is also referred to as a “clicking-without-reading” phenomenon,⁴⁰ and is already known accordingly from the area of general terms and conditions.⁴¹ A survey conducted by the European Commission obtained similar figures, according to which 29 per cent of users never read data protection declarations and 55 per cent said they only read part of them. The main reason for this was that the data protection declarations are too long (70 per cent), and they are not clearly formulated and difficult to understand (43 per cent).⁴² Reading the data protection declarations of every website we visit in the course of a year would cost us around 76 working days of eight hours each.⁴³ Combined with the low benefit of being aware of data protection regulations, the lack of awareness may therefore even be rational. It is referred to as rational apathy.

Means used so far to solve this problem such as the one-pager supported in the trial phase by the Federal Ministry for Justice and Consumer Protection or the labelling solution developed by the Carnegie Mellon University in Pittsburgh⁴⁴ did not show the hoped-for success in practice.⁴⁵ Visualisation solutions are currently still in development, since they were not directly included in the GDPR.⁴⁶ PIMS could significantly help to solve the problem of information transfer that has failed so far, by processing data protection information for the data subjects and advising them. They could also use visualisation solutions without having to wait for the lengthy process of uniform image symbol design at Union or Member State level.

Visualisation solutions make use of the image superiority effect: Empirical studies prove that the cognitive abilities of people respond much better to images than text,⁴⁷ which is mainly due to the fact that images are understood holistically, whereas texts are understood sequentially.⁴⁸

Images are recognised long before a text can be understood. To understand an image in a form that can be recognised later on, the human brain needs an average of around one to two seconds for an image of medium complexity, whereas only five to ten words of a simple text can be understood in the same viewing time.⁴⁹ Images are also particularly suitable for activating and, hence generating attention. Signal colours such as red, orange, and yellow are primarily used for this purpose.⁵⁰ Furthermore, it is much easier to remember images than text.⁵¹ PIMS will therefore provide a service for users via this information and advice function which goes far beyond the technical consent options that are currently being discussed.⁵² This functionality could also go beyond the data protection problem-solving options and provide a problem solution for consumer protection law as a whole by providing information about a company, a website or a data processor beyond information under data protection law which the customer wants according to their personal preferences, e.g. on sustainability or on details of products, for instance where a product is produced and the working conditions prevailing there. Certainly, this requires that information is available, which the legislator would have to ensure unless the market is able to regulate this itself. Thus, PIMS could become a real (and data-protection friendly) alternative to the personalised information provision being discussed in the USA above all.

5.1.1.2 Enforcement Deficit Regarding Data Protection Law

The GDPR continues to suffer from an enforcement deficit. This is already subject to intense debate for public law enforcement, but equally applies to private enforcement. This is probably due to two things: Firstly, unsuccessful information transfer is a major reason here, too. If data protection declarations indicate that data subject rights exist and how they can be exercised, but data subjects do not observe this information, this already prevents them from exercising their user rights, unless they learn about the possibility of their use by other means.

However, the action burden of enforcement is also a main reason users do not make use of their rights, even if they are aware of the possibility of enforcement. This is because the decision to enforce the law ultimately depends on the user's personal cost-benefit analysis: Only insofar

as the anticipated benefit exceeds the anticipated cost of enforcing the law will the user avail himself/herself of his/her out-of-court and judicial options.⁵³ If the user is defeated, he/she must bear the costs of the procedure according to civil procedural principles, which he/she will feed into his/her cost-benefit analysis as a risk. What is more, the user could also estimate the success probability of enforcing data subject rights as low because he/she assumes an imbalance of power at least vis-à-vis large data processors.⁵⁴ Ultimately, however, the time needed for legal enforcement is a major factor influencing user behaviour, as proven by empirical studies from the USA and the United Kingdom in the field of copyright.⁵⁵ Here, too, PIMS could provide support by enforcing the rights of data subject (out of court) for the data subject, and hence at least minimise the time invested by the data subject.

5.1.1.3 Competition Problem

The competition problem only arises when declaring consent under data protection law to the processing of personal data vis-à-vis large online platforms. They have both great market power, which is characterised by very large economies of scale as well as direct and indirect network effects with the resulting tipping problem, and great information asymmetries vis-à-vis users, which result from an information overload of the users for example. The economic power of large digital platforms is therefore based on a combination of two co-existing serious types of market failure which are mutually reinforcing.⁵⁶ Firstly, information asymmetries on digital markets can exacerbate competition problems. If users do not observe information under data protection law and therefore fail to understand how data privacy (un)friendly a service is, competition regarding the quality of data protection friendly solutions cannot function well. Secondly (conversely), virtually monopolistic services can use opaque and more far-reaching conditions for collecting and using personal data because users have no realistic alternatives. So, both market failures reinforce each other.⁵⁷

5.1.2 Problem-solving Option: PIMS

Personal Information Management Systems (PIMS) are considered as a solution for the information overload problem and for eliminating the data protection enforcement deficit. They can potentially make a fundamental contribution to solving the competition problem in any case. As a point of departure, Personal Information Management Systems are technical tools that could help data users to better control data processing. These are “technologies and ecosystems that aim to enable people to exercise control over the collection and forwarding of their personal data”⁵⁸ and are therefore privacy enhancing technologies.⁵⁹ They can, however, greatly exceed this technical solution and provide a service to users in the form of improved information transfer and advisory services (also outside the field of data protection law) as well as for enforcing rights under data protection law. They are also suitable for removing dark patterns. This refers to means and methods that (deliberately) exploit the behavioural influence of people through heuristics and biases to the advantage of the company or third-party using the dark pattern (dark nudging),⁶⁰ for example by using a green colour for the consent button, while the refusal to grant consent is coloured red in the signal and warning colour.

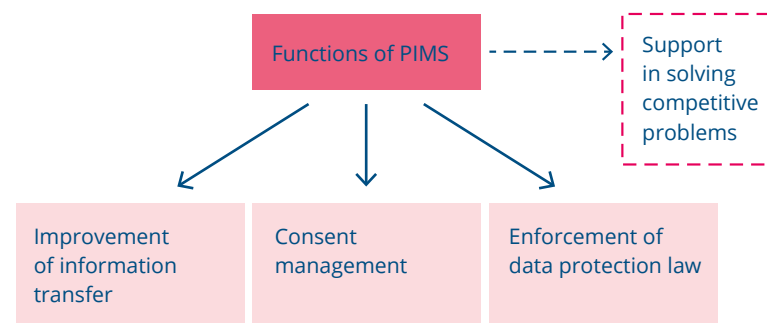
Even the PIMS user will never be able to predict with absolute certainty what consequences his/her consent will have, for example if data are passed on to third parties.⁶¹ However, our legal system does not call for such absolute certainty of the consequences related to a decision for a self-determined decision. The patient, who, for example, consents to medical care can no more monitor all the risks of a mistake by the doctor than data subjects who consent to data processing can anticipate any unauthorised use of data. Instead of this certainty about consequences, self-determination requires a free decision in the knowledge of possible risks. This certainly presupposes that data subjects are adequately informed about risks – and this is where action is needed so that information is also observed and understood. PIMS can contribute significantly to this end.

As such a protection and self-determination instrument, PIMS exhibit three main functions: Firstly, they fulfil an information and advisory function⁶² by, for instance, highlighting to the data subject what data is collected about him/her, from whom, and for which purposes, and by preparing, visualising, or explaining this information. Further information on the data processor could also be provided, and also such information that has nothing to do with data protection law, e.g. information on working conditions in the data processing company or the sustainability of the service/product offered. PIMS could therefore fulfil an essential service function and provide data subjects with information that they both need and want.

Secondly, PIMS should help data subjects to only consent to such data processing that corresponds to their preferences under data protection law. To this end, they could play the role of a “consent assistant”⁶³: They grant consent on behalf of the data subject according to conditions prescribed in the trustee contract.⁶⁴ For this purpose, they usually store their users’ personal data centrally and only pass it on to third parties if the user consents to the data recipient using the data.⁶⁵ In this function, they could help in particular to reduce cookie banners by automatically declaring the user’s consent according to the user’s specifications once they have been made, thus making individually set cookie preferences superfluous. Of course, this only applies if there is no exception to the consent requirement under Paragraph 25 (2) No. 2 of the Telecommunication Telemedia Data Act (TTDSDG). The suitability of PIMS for reducing cookie banners also depends on their concrete legislative design which will be discussed later.

Thirdly, however, PIMS can even assist with the enforcement of data protection and data consumer protection law by exercising the rights of data subjects and revoking consents, for example.⁶⁶ The automated reporting of violations against data protection and consumer protection law which a PIMS identifies when acting on behalf of the user (e.g. unauthorised tying) could also be implemented. The suitability of PIMS for solving this problem also largely depends on their specific legislative design which will be discussed later.

Figure 2: Functions of PIMS



The Data Governance Act, on the other hand, sees PIMS primarily as a means via which data can be made available to the economy. These various perspectives on PIMS as an instrument of protection and participation on the one hand, and as an instrument for better data sharing on the other, influence the principles according to which PIMS are designed. If we understand PIMS primarily as a data sharing instrument, which could become a threat to informational self-determination, regulation is first and foremost concerned with the security of data, prohibits the use of user data for other purposes and seeks to prevent incentives for data sharing. Business models that incentivise this data sharing are viewed critically. However, if we understand PIMS as a protection and participation instrument, regulation must, in addition to preventing abuse, make every effort to facilitate these technologies. Ultimately, the legislator is responsible for reconciling both perspectives on PIMS⁶⁷ by adequately taking account of both the opportunities and risks that they pose to the right to informational self-determination.

5.1.2.1 Essential Elements of a Problem-solving Oriented Legal Framework for PIMS

A functioning legal framework for PIMS requires decisions at a system-level, not isolated solutions. If the intention is for PIMS to work, two prerequisites need to be ensured at this system level: Firstly, an

obligation for data processors to cooperate with PIMS, and secondly, a standardisation of technical requirements for cooperation. If these two system requirements are met, further fine-tuning of the legal framework is needed to guarantee the functioning of PIMS, but without decisions at the system level this fine-tuning is useless. It is also necessary to minimise the risks associated with PIMS through adequate regulation and to answer the organisational and financing question.

5.1.2.2 Regulation at System Level

Obligation to Take PIMS Requirements into Account

The Data Ethics Commission already called for a binding consideration of PIMS requirements in its report.⁶⁸ Also vzbz, Stiftung neue Verantwortung (SNV) as well as other voices in the literature advocate for such a binding consideration of PIMS requirements.⁶⁹ An obligation to consider PIMS requirements for data processors means that specifications made by the data subject vis-à-vis the PIMS must be considered by the data processor and he/she is prohibited from interacting with the data subject past the PIMS, insofar as specifications have been made to the PIMS. In fact, such a consideration of PIMS specifications is absolutely imperative, because only then is there sufficient benefit of their use: If a duty to consider is not established by PIMS, online actors could simply disregard the specifications of PIMS and continue to request consent from the user. In particular, it would not be worth the user making use of a PIMS if only a limited portion of consents can be processed in this way. Then he/she would only have a limited overview of his/her granted consents. This would not remedy the information overload problem. Only if consideration of PIMS specifications is mandatory could PIMS achieve market penetration which may establish a counterweight to the market power of major online services and therefore put PIMS in a position to actively negotiate the conditions of data processing in the long-term.

Technical Standardisation

Moreover, technical standardisation for the automated processing of consents and corresponding data transfers is inevitable. Common technological standards are needed between all players in the digital economy. The problem of standardised and open interfaces (APIs etc.), but also semantic standardisations is also the case for data access issues

and data portability issues and is therefore not new. It is clear from the standard-setting literature that such standards can either be set in classic (collective) standard-setting procedures or via market-powerful companies.⁷⁰ Such a system cannot arise decentral from below by many PIMS. In this sense, it constitutes a classic standard-setting problem with the typical market failure problems. In this respect, standardisation policy and the commitment to certain standards play a pivotal role if the setting of these standards by large digital corporations is to be prevented.

5.1.2.3 Fine-tuning the Legal Framework

Fine-tuning for Solving the Data Protection Situation

If a mandatory consideration of PIMS requirements and technical standardisation is ensured, it merely requires further fine-tuning in the legal framework which is essentially limited to clarifications, however. On the one hand, this concerns the support of the information function of PIMS (a), on the other hand it concerns the creation of legal certainty for consent management (b) as well as for the opportunity to enforce data subjects' rights under data protection law (c). Ultimately, the risk of abuse must be adequately prevented, conflicts of interest of the PIMS must be countered and thus the overall risk for informational self-determination must be minimised (d).

Support of the Information Function

If PIMS are to support with transferring data protection information, this does not require any immediate legislative action because assistance in the transfer of information is not prohibited by law. The PIMS also do not act on behalf of the responsible person. The question of whether the responsible person has correctly implemented the information obligations is not influenced by their activity in this respect unless this is explicitly agreed. The transfer of information on data processing carried out by the responsible person does not therefore have to comply with the requirements of Art. 13, 14 GDPR (of course, something else goes for information on data processing carried out by the PIMS). In this respect, the question of the supporting information transfer activities by PIMS does not depend on the form in which this information transfer must take place according to law. The PIMS can therefore also make use of visualisation solutions without any problems.⁷¹ However, it would be

positive if opportunities for transferring information (also in the scope of application of Art. 13, 14 GDPR) would be improved as a whole. For example, this would be possible via a layer model of information transfer that also includes visual elements.⁷² Images are better understood and remembered due to the image superiority effect⁷³ and for that reason are to be given preference over purely text-based information transfer. However, in order to design visualisation solutions with adequate efficiency, the development of uniform image symbols would be desirable.⁷⁴

Enabling Effective Consent Management in a Legally Secure Way

However, there is a need for action in the area of consent management. Overall, this should be supported by enabling regulation within the GDPR. On the one hand, this includes the clarification that proxy consent is possible, while also enabling consent vis-à-vis PIMS on the other hand. The possibility of proxy as well as broad consent should in any case be provided for those PIMS which meet specified requirements, e.g. IT security requirements. Some of these requirements can be taken from the Data Governance Act. Their compliance could be verified within a state certification system or recognition procedure (as provided for in the TTDSG).

It is disputed whether a third party may declare consent on behalf of the data subject at all.⁷⁵ In data protection law, too, consent can be thought of not only as an institution of justification, but also as a legal declaration.⁷⁶ Whereas proxy constellations are not *expressis verbis* anchored in the GDPR, they are in principle established under Union law.⁷⁷ The decision for such a proxy solution is ultimately an exercise of the right to informational self-determination and therefore to be recognised.⁷⁸ In any case, the same requirements are to be placed on granting power of attorney as on the consent itself.⁷⁹ Although this contradicts Paragraph 167 (2) of the German Civil Code (BGB), consent under the GDPR is not to be interpreted according the standards of national law, but instead autonomously under Union law.⁸⁰ The high requirements of consent, which are intended to ensure genuine self-determination of the data subject, would be undermined if the requirements did not also apply to granting power of attorney.⁸¹

Acting as an intermediary (*Erklärungsbote*) is also possible and many PIMS are currently acting as such because they lack their own scope for decision-making. Apart from presenting the specific declaration of consent, only a proxy solution would guarantee scope for manoeuvre for PIMS. However, such a proxy solution would probably only make sense in combination with the possibility of broad consent. Ultimately, the meaning and purpose of assisted consent is precisely not to have to ask the data subject again for each consent, but instead to afford the data subject the opportunity to define in advance for which cases and under which conditions consent should be granted, and to consent on behalf of the data subject if the conditions are met. The scope of decision-making of the proxy PIMS would therefore lie particularly in the specific selection of the data processor. The fact that it is subject to narrow instructions in the internal relationship does not pose a problem. Ultimately, the seller also acts as a so-called “representative with a committed strategy” based on the right of representation.⁸² For reasons of legal certainty, the possibility of representation should be enshrined in law; as explained, Union law already allows for it today.

Data processing carried out by PIMS must currently (and also under the requirements of the new TTDSG) as a rule be justified by consent, which, even if it is declared vis-à-vis a PIMS, is subject to a strict purpose limitation.⁸³ Consent that either determines a specific purpose but not a specific person responsible or a specific person responsible but no specific purpose is invalid.⁸⁴ A data transfer carried out by a PIMS must therefore be justified by the consent of a data subject, which is given specifically for the individual case. However, granting effective consent through PIMS is already possible de lege lata via so-called dynamic consent. Here, in a first step, the data subject’s data protection preferences are requested, in other words, the user specifies for which broad purposes they would like to provide data concerning him/her (e.g. not for personal advertising, but for research purposes). In the event that a suitable data processing situation occurs, the user will be requested via the PIMS to grant his/her consent for the specific case.⁸⁵ However, it also seems worth considering de lege ferenda the negotiation of prerequisites for a broad consent according to the standardised consent form that the Medicine Informatics Initiative and the DSK have agreed on for the health sector.⁸⁶ In any

case, a meta consent seems conceivable for the health sector, in which PIMS could provide data for research purposes.⁸⁷ It would allow the person granting consent to decide, regardless of the specific occasion, for which type of research project the data subject would like to give what kind of consent (specific or broad) in which research context.⁸⁸ The Data Ethics Commission recommends examining the possibility of such meta-consent.⁸⁹

Enabling Enforcement of Data Protection Law through PIMS

PIMS should also be able to exercise data protection powers and (automatically) report data protection breaches. If, for example, the consent has to be given in order to use a service, this may violate the prohibition of coupling, Art. 7 (4) GDPR. Such a violation of data protection law can be automatically notified to the competent data protection authorities. This does not require an adjustment of the legal framework, however.

Yet clarifications in the legal framework appear desirable for enforcing data protection rights by PIMS. Thus is because the GDPR does not regulate whether Art. 15 et seq. GDPR can be invoked by third parties. The conclusion could be drawn from Art. 80 GDPR, which also allows third parties to exercise specific rights, that precisely this is not permitted for Art. 15 et seq. GDPR. On the other hand, it could also be reasoned that the legislator did not intend to make any statement precisely in this regard, and an exercise of the data subject's rights by third parties is thus not excluded in any case.⁹⁰ The legislator should clarify this.

Fine-tuning to Solve the Competition Problem

If it is not only data protection problems that are to be addressed, but also the resolution of competition problems, PIMS should be enabled, in addition to the above-mentioned specifications, to change the provider in favour of a more data protection-friendly platform; in other words, to terminate the corresponding platform usage contract and conclude new platform usage contracts. However, this should already be possible with the current provisions under civil law.

Yet the competition functional deficit cannot be resolved by a functioning legal framework for PIMS alone. Rather, two further substantive legal

requirements are needed: Firstly, an interconnectivity obligation for large online platforms, and secondly, a payment option for using services of large online platforms as an alternative to the declaration of the consent under data protection law, unless this is already prescribed by the prohibition of coupling. Large online platforms should therefore be obliged to enable users from other platforms to directly interact with their customers, to allow them to send and receive messages in the case of social network messenger services,⁹¹ as well as to give users the choice of paying to use the service as opposed to declaring their consent under data protection law.⁹²

If a functioning legal framework for PIMS can be successfully established, they could form a counterweight to large online platforms if they are used by a large number of people. If there is market power at both the provider and demand side (or at least negotiating power), platforms would no longer be able to dictate the conditions of data processing. The possibility of gaining negotiating power can and must be the long-term goal to be achieved with the help of PIMS. What is more, a key task of competition policy is to solve the problem of digital platforms' market power, for instance via the "Digital Markets Act" (DMA), which is currently being discussed at EU level or the new Paragraph 19a German Act Against Restraints of Competition (GWB) in German competition law.

5.1.2.4 Minimise Risks

PIMS play an important role in solving the problems identified by facilitating informed decisions about the processing of data or the entry into a contract altogether and the exercise of data subjects' rights. In doing so, they resolve the problems of informational self-determination but only insofar as these can be solved at all by informed consent. Whether consent should be able to legitimise any form of data processing is a completely different issue which is to be clarified by the legislator. Particularly hazardous processing activities could, for example, be tied to additional requirements or prohibited completely. For instance, this could include the merging of data by very large online platforms within the meaning of Art. 5(a) DMA.

The Data Ethics Commission also recommends the introduction of a certification and monitoring system for PIMS. Blank mandates to PIMS should be excluded, provisions should be made in the case of insolvency or dissolution of PIMS. Moreover, the requirements under the Data Governance Act must be complied with.⁹³

5.1.2.5 Funding and Organisation

There are two options for funding PIMS: Either PIMS will be provided by the state alone or private sector models will (also) be enabled. Preference per se must not be given to state data processing because the state appears to be particularly trustworthy in dealing with personal data. On the contrary, the informational right to self-determination was designed as a right of defence against the state, and in a large number of legal systems, data processing by the state is associated with much greater risks than data processing by private companies. Nevertheless, a constitutional state is naturally suited to operate as a provider of PIMS. However, this requires an explicit legislative decision. Until now, the legislator has not been sufficiently involved in the development of PIMS, which reveals how it does not want to exclude the private development of PIMS in any case.⁹⁴ The private sector activity of PIMS can only succeed if the activity is ultimately profitable, however. This raises two main questions: Firstly, who is to pay for the PIMS (the data processor or the user)? And secondly, what is the PIMS to be paid for (the volumes of data transmission or the service it offers)?

Both questions cannot be answered in isolation from one another: The obligor of the counter performance for an activity of the PIMS may be the data processor or the individual user. If the data processor is obliged to carry out the activity, the PIMS is incentivised to communicate as much data to the company as possible in order to achieve the highest possible price (assuming that the volume of data determines the price). Such an incentive for transferring as much personal data as possible is to be viewed critically as regards the effective guarantee of the right to informational self-determination.⁹⁵ It would incentivise the PIMS to encourage the user to consent to the communication of as much data to the data processor as possible, which would result in the PIMS ultimately becoming less of a monitoring and participation instru-

ment than an instrument for increased data sharing which would be less in the user's interest than in the data processor's interest.

On the other hand, if the users have to pay for the activity of the PIMS, the protection of informational self-determination would be dependent on the user's income⁹⁶ whereby weaker incomes would be disadvantaged. However, PIMS offer a service for the user, for which he/she should also have to provide a counter performance, at least in the starting point, to prevent the above-mentioned false incentive. A reduction of the remuneration to be paid through a monetisation of the data subject's personal data, e.g., through a rebate, is also subject to intense debate,⁹⁷ but is highly problematic regarding its incentive effect. To ensure that less financially sound persons can also be provided with a PIMS, state subsidisation of recognised or certified PIMS should be considered.

5.1.3 Suitability of DGA-E and Paragraph 26 TTDSG for Problem-solving Regulation of PIMS

5.1.3.1 Data Governance Act

The Data Governance Act also and especially pursues the goal of ensuring better control over data and its use in harmony with Union law. The means chosen to achieve this goal is the creation of trust. The European legislator assumes that currently lacking or in any case not readily available data intermediaries on the market for improving the control of data use – usually PIMS – will emerge or exist to a greater extent as soon as trust in these services is strengthened. As has been shown, a lack of trust is not the main problem for PIMS that prevents it from becoming more established on the market. The lack of market penetration is rather due to the fact that the use of PIMS currently only brings limited benefits to data subjects. Firstly, this is because there is no obligation to take account of PIMS specifications and there is no technical standardisation, and secondly, PIMS alone cannot solve the problem if users often feel compelled, due to market power, to consent to data processing especially by large platforms. Corresponding business models have therefore not yet been able to establish themselves on the market. Only when the necessary functional conditions for PIMS are established in the described form through regulation will they offer a benefit to users which will promote their use. Although the additional requirements of the DGA-E serve to

prevent abuse, they make the activities of PIMS even more difficult. The DGA-E is completely unsuitable for achieving improved control over the access and use of data so long as it exclusively provides for these additional requirements, without stipulating supplementary obligations to take account of the PIMS guidelines and technical standardisation. What is more, a corresponding fine-tuning of the legal framework needs to be provided for which ensures legal certainty and is designed in an incentive-based way (fulfilment of requirements for abuse prevention must lead to legal certainty under data protection law.) Calls for legal certainty under data protection law had already been made by the Data Ethics Commission.⁹⁸

5.1.3.2 Paragraph 26 of the Telecommunications Telemedia Data Protection Act (TTDSG)

Paragraph 26 TTDSG aims to create a “reliable and credible”⁹⁹ framework for services to manage consents granted according to Paragraph 25 (1) TTDSG, which results in “end users entrusting their data to such services”¹⁰⁰, so as to reduce cookie banners as a result. Paragraph 26 TTDSG is limited to the consent to storing cookies or to the retrieval of information from cookies already stored in accordance with Paragraph 25 TTDSG. The reduction of cookie banners aims to decrease users’ informational overload and thus to resolve the problem of informational overload under data protection law in a specific case. The national legislator assumes – as is already the case with the European legislator – that the lack of dissemination of PIMS on the market is mainly due to a lack of trust and therefore wants to strengthen this trust through Paragraph 25 TTDSG. However, it is not so much that users’ trust in PIMS is lacking than the absence of a decisive advantage of using PIMS (see above). In this respect, the goal of reducing cookie banners through PIMS will only be achieved when the legal framework makes PIMS functional by enabling them to support both data protection as well as competitive problem solving.

TTDSG contributes little to this solution. Its approach is to only (and only marginally) fine-tune the legal framework, but not to change it at a system level: The PIMS is enabled to transfer declarations of consent under data protection law for data subjects even without a possible recogni-

tion according to Paragraph 26 TTDSG. The other grey areas under data protection law are not infringed upon. Moreover, much like the DGA-E, Paragraph 26 TTDSG does not regulate the grey areas at a system level either. It solely serves to reduce the risk of abuse by enabling the recognition of PIMS through an independent body subject to Paragraph 26 (2) TTDSG if the services

1. have user-friendly and competitive procedures and technical applications for obtaining and managing consents,
2. have no economic self-interest in granting consent and in the data managed and are independent of companies that could have such an interest,
3. process personal data and information on consent choices only for the purposes of managing consent, and
4. present a security concept that enables an assessment of the quality and reliability of the service and technical applications, and which indicates that the service both technically and organisationally meets the legal requirements on data protection and data security that arise from the Regulation (EU) 2016/679 in particular.

The specific requirements to be fulfilled by the services for consent management for the purpose of recognition should be specified by a statutory instrument.

Browser manufacturers should take account of the settings in PIMS regarding cookies. The TTDSG does not impose an obligation to comply with PIMS settings, however.¹⁰¹ Telemedia providers can therefore continue to request the individual consent of individual users, which is why the regulation will not contribute toward reducing cookie banners and thus to reducing users’ informational overload.¹⁰² The duty to take account of PIMS requirements cannot be incorporated in the statutory instrument itself which is currently being drafted because Paragraph 26 TTDSG does not leave any scope for this. An obligation to comply with the PIMS requirements would have to be standardised in Paragraph 26

TTDSG itself as a consequence of the recognition, and the necessary clarifications under data protection law (see above) would either have to be standardised in the TTDSG as a consequence of recognition, or, for a wider scope of application, in the Federal Data Protection Act (BDSG) or the GDPR.

5.2 Data Trustees in the Health Sector

Unlike in the online business sector, the health sector is not affected by an overuse, but rather an underuse of data at least for research purposes. Although various Member States have registers at the national level which can be used for research purposes such as the Cancer Register or the Research Data Centre in Germany, the access to data is not coordinated or only to a limited extent, making it difficult for the individual scientist to identify the correct access addressee. Therefore, on the one hand, a central European or Member State coordination body is needed to which applications can be made for research data access by means of a standardised electronic form, and which decides on whether application requirements are met as well as on the type and scope of data access. Such coordination bodies also exist in Finland and Australia, for example.¹⁰³

However, it will never be possible to store all data in such registers because the registers usually hold disease-specific data (e.g., cancer data) or purpose-specific data (e.g., billing data). In this respect, in addition to a coordination body which is designed as a data trustee, there needs to be flexible data trustee solutions provided by the state or the private sector with whose help even heterogeneous data can be shared and evaluated in accordance with data protection law.

Ultimately, a data donation function in an electronic patient record would also contribute toward solving the problem of underuse of data for research. Electronic patient records, as they are being developed in Sweden and Denmark, but also in Germany (ePa) or Austria (ELGA), also function as a data trustee because they communicate patient data to health care providers in the interest of the patient. This means they pri-

marily resolve an existing efficiency problem in health care, which also and primarily results from the fact that data has previously been stored with the health care provider and is thus often not accessible to other health care providers visited by the patient. Incentives for the use and provisions against unauthorised access to data as well as data misuse are needed to resolve this efficiency problem. However, a data release option/data donation option based on informed consent and its technical guarantee must be enshrined in law to solve the problem of data underuse.

In the following section, the approach of a central coordinating body in Finland and Australia is explained at first as probably the most advanced approach for such a coordinating body. Such a body is also proposed by a current report on behalf of the Federal Ministry of Education and Research (BMBF).¹⁰⁴ Subsequently, the additionally required flexible data trustee solutions are presented which can either be offered by the private sector or drawn up by the state. In a third step, the specific design parameters of these various data trustee solutions will be discussed.

5.2.1 Coordination Unit for Data Access

5.2.1.1 Findata

In Finland, claims for data access from the Secondary Use Act are coordinated via a Data Permit Authority, Findata, operated at the Finnish Institute for Health and Welfare but which is independent of the institute's other activities. It is under the supervision of the Ministry of Social Affairs. If permission to access data is granted by Findata,¹⁰⁵ Findata collects the data from the data-holding entities, combines, pseudonymises and anonymises it where necessary and then makes it available to the applicant via a secure hosting service that is to be specifically set up, cf. Paragraph 10 No. 6 Secondary Use Act. If data was provided based on consent under data protection law, access to data may only be granted if this is covered by the scope of the consent, cf. 43. Data holders are public bodies such as national data repositories, healthcare and social welfare care, data archives, but also registered data from private providers of social and health care services.¹⁰⁶

5.2.1.2 My Health Systems

In Australia, access to research data is guaranteed via the My Health Records Act – a state-operated system for providing health information on health care recipients for recipients' health care purposes (primary use) as well as for other purposes such as scientific and research purposes (secondary use). A recipient of health care has a health record in this system as soon as he/she either registers or, in the case that the Minister orders an opt-out model, he/she does not opt out. The system operator runs the National Repositories Service which stores the most important health record data sets. Other data sets are stored by registered repository operators. Together, these data sets constitute the health care recipient's personal health record.

Health data can be made available from a health care recipient's personal health record for the purpose of research if it concerns anonymised data or else (personal) health data, if the data subject consents, Paragraph 15 and 83.

However, this requires that the "Data Governance Board", which is staffed with various experts and advised by various committees, gives a positive decision on an application to use data for research purposes, Paragraph 33 and 109 A. The applicant must consent to the terms of use beforehand¹⁰⁷ and attach a risk management plan, based on which the Board assesses the risk of loss or misuse of data in particular.¹⁰⁸ Moreover, the consent of the data subject is always needed for access to personal data. If it determines that an ethical review is advisable, it must seek approval from the Australian Institute of Health and Welfare (AIHW).¹⁰⁹

Findata as well as My Health Record System are data trustees that centrally store data and function as data intermediaries between decentralised third-party storage and those requesting data. However, their coordination function is likely to be particularly important.

5.2.1.3 Design of European Coordination Units

Such a coordinating body is needed at both European and Member State level, whereby the European coordinating body should be responsible for data access across Member States, and the Member States bodies

for data access limited to the respective Member State. In principle, the fulfilment of a brokerage function between the Member States' coordination bodies is sufficient for the European body, however, the Member States' coordination bodies would also have to be responsible for providing data via corresponding secure server solutions, as is happening in research data centres in Germany, for instance. What is more, the coordinating body could make the decision on data access and on the modalities of data access and the secondary use of data and research outcomes either at the European or at the national level, as far as the legislator leaves some scope for decision-making here. It also needs to be defined to whom data may be disclosed and measures against misuse must be provided for. In Australia, for example, data is not transferred to insurers, Paragraph 16 and 109 A. Specific purposes of subsequent use are prohibited, Paragraph 70 A and 70 B. The use of data for prohibited purposes is a criminal offence, Paragraph 71 A, as well as a violation against the Privacy Act 1988, Paragraphs 72 and 73. The Data Governance Board keeps a publicly accessible register which shows who applied for data access among other things.¹¹⁰

5.2.2 Flexible Data Trustee Solutions

5.2.2.1 Data Donation Trusteeship

Requirement

In addition to the single register and coordination body, flexible data trustee solutions need to be found to solve the problem of the under-use of data in research.¹¹¹ These can have a data donation function on the one hand and a data sharing function on the other. The electronic patient record, for example, has a data donation function which is made available by the statutory health insurance funds via the gematric telematics infrastructure. As public sector entities, health insurance funds are responsible under data protection law for processing data in the electronic health record at least in Germany, cf. Paragraph 341 (4) p. 1 of the German Social Security Code (SGB V).¹¹² A "data donation" could help make data accessible for research in accordance with data protection law. Such data donations are also envisaged in Australia and Finland.¹¹³ A model regulation can also be found in the national legislation in Paragraph 363 SGB V. The concept of a data donation is so important for medical research because it is met with great approval among the pop-

ulation. According to a Forsa survey commissioned by the Technologie- und Methodenplattform für die vernetzte medizinische Forschung e. V. (Technology and Methods Platform for Networked Medical Research) just under 79 per cent of Germany are prepared to make such a voluntary donation.¹¹⁴

However, consideration is also given to private bodies fulfilling a data donation function. In this case, they are PIMS and subject to the above-mentioned regulatory requirements. For instance, it is conceivable that PIMS will release data relevant to health providers such as data from fitness trackers and health apps. Theoretically speaking, this data could be released into the electronic health record and from there be released for scientific use based on informed consent. Both the electronic health records as well as PIMS organised by the private sector for the release of health data for research purposes could and should find their place in a European Health Data Space.

Regulatory Requirements

Specifications for the Transfer of Data to the Data Trustee as well as for Data Processing in the Data Trustee

As regarding the transfer of data to a data trustee as well as for data processing in a data trustee, an allocation of responsibility should be carried out under data protection law, as permitted by Art. 4 (7) GDPR.¹¹⁵ A clarification is also needed for the processing basis under data protection law for feeding data into the data trust and for processing data in the data trust. In Austria, this is based on a statutory permission norm with an opt-out opportunity for the electronic health record,¹¹⁶ while in Germany it is based on consent. While a statutory permission norm with an opt-out opportunity would result in an increased availability of data already owing to the status-quo bias,¹¹⁷ the consent solution takes account of informational self-determination to a greater extent. The legislator is responsible for deciding to which interest (freedom of research and health and well-being of the public while simultaneously safeguarding the right to informational self-determination through the possibility of objection or comprehensive guarantee of the right to informational self-determination with deferral of freedom of research and the health and well-being of the public) preference should be given here. A statu-

tory permission norm with the opportunity to object could be based on the opening clause of Art. 9 (2) lit. h GDPR (as has been done in Austria). This would make both a Union and national basis of processing possible.

If the transfer of data to and the data processing in the electronic health record or an electronic patient record is guaranteed on the basis of consent, the greatest possible granularity of consent should be ensured so as to avoid data protection concerns.¹¹⁸ Both with regard to a consent solution as well as to a statutory permission requirement it should be specified which healthcare providers receive access to which documents and data under which conditions. The patient should definitely retain control over data concerning him/her, regardless of whether a consent or opt-out solution is chosen.

Data Donation

However, to ensure data use for science, it is above all necessary to provide for a data release to existing registers and scientists authorised to submit applications. This data release can be provided for both based on informed consent and the basis of a legal permission with an opt-out solution, with the incentives and impact on freedom of research, general health/general public welfare and informational self-determination already mentioned.

In addition to the data protection requirements, it is particularly important to specify which requirements need to be fulfilled by scientists to whom data is released. Studies here have shown that the circle of scientists does not necessarily have to be limited to non-commercial researchers as long as the research purpose is tied to the public interest.¹¹⁹ In this sense, the public interest could be defined as an activity whose performance is not motivated by individual – economic, self-interested, friendly, or family – goals alone, but at least also proves to be an expression of social responsibility.¹²⁰ The conditions for a data donation should be defined as well as the permitted secondary use of data and of research results (publication obligation). Likewise, measures should be taken against the misuse of data such as the loss of a doctor's medical license, exclusion of using data provided based on the data donation option for a certain period of time, etc. An institution is needed that

decides whether the conditions for data use have or have not been met by the requesting scientist, and that decides on the modalities and scope of data access.¹²¹

If the data donation is enabled on the basis of consent, broad consent, for example based on the Medical Informatics Initiative, should be possible in any case.¹²²

What is more, the requirements on the technical infrastructure need to be defined. Security precautions should be particularly high due to the special sensitivity of the processed data.¹²³

PIMS

PIMS for data sharing in the health sector could release data based on an informed consent, e.g. into the electronic patient record. Its need for regulation derives from the above-mentioned explanations in the PIMS chapter. However, PIMS for data sharing in the health sector differ significantly from PIMS operating outside the health sector: The protectable interest in ensuring freedom of research in the public interest and the interest in improving general health justify guaranteeing an incentive for data sharing with science and research in the public interest in this area. In particular, a reimbursement of the user should therefore not be excluded here per se. It is also not apparent why data altruistic organisations alone should be able to make use of the possibility of standardised and possibly broader consent (if, as provided for in the Data Governance Act, this is declared permissible by a delegated act). Unlike non-data altruistic PIMS, data altruistic organisations must offer their services on a gratuitous basis, cf. Art. 16 DGA-E, however, the overall benefit to society of a data donation trusteeship is identical in both cases if data processing for whose purpose the data is donated provides a benefit for society as a whole.

5.2.2.2 Data Sharing Trusteeship

On the other hand, the data trustee can also be thought of as a body for sharing and evaluating large volumes of data from two or more data owners.

Requirement

Big data research is essential in medicine. With so-called “radiomics” analyses of image data, recurring texture markers can be identified that enable conclusions to be drawn about pathologies, tissue properties or the disease progression in patients.¹²⁴ Biomarkers can be generated from the overview of large amounts of data from different medical disciplines, which could help in cancer detection, diagnosis, assessment of prognosis, prediction of response to treatment and monitoring of the disease status. However, the application possibilities and success of this data evaluation largely depend on the possibility to systematically analyse the largest possible data sets. From a purely medical point of view, the creation of databases that combine large volumes of medical data from all medical disciplines (image data, laboratory data, pathology data) would be desirable in this respect. However, data protection law sets high hurdles for such combinations of data and analyses of large data sets.¹²⁵ A data trustee would offer the option of thinking about data protection and data evaluation together by creating a secure space for evaluating data in which the data would be shared, but neither the data holders themselves nor the data trustee provider could actually access and pass on this data. Technically, only the algorithmic evaluation of data is made possible and only the evaluation outcomes would then be released to the data holders. Data in the data trustee would be deleted again, however.¹²⁶

Various solutions to facilitate such an exchange of data are currently being tested on the market. Nevertheless, voluntary data sharing for scientific and research purposes is not making much headway. On the one hand, which may be due to a lack of legal certainty, while also certainly due to considerable technical effort. After all, if data should be shared between different actors, conditions need to be checked, data standards harmonised and the conditions of granting access to data discussed. This is likely to involve a lot of effort for persons and institutions requested to share data, e.g. corresponding clinics, which they will scarcely want to make on a voluntary basis without the corresponding reimbursement of costs.¹²⁷ In addition to the legal facilitation of data trustee models, thought urgently needs to be given to the harmonisation of data standards and interfaces at the same time.¹²⁸

Relationship with Federated Learning

Federated Learning means that algorithms can be trained on decentral stored data. In cases of Federated Learning, the need for central infrastructure consists solely in the provision of the technical platform and application-specific encryption,¹²⁹ as well as, for example, in the subsequent bundling of evaluation outcomes. However, Federated Learning reaches its limits in cases of vertically distributed data (such as different data from the same group of people stored in various locations – for example different hospitals). The need for a central data trustee solution therefore remains alongside Federated Learning models.¹³⁰ The analysis of vertically distributed data for purposes of Covid-19 side effects research data, for example, is much more successful in such central data trustee structures which are also referred to as data clean rooms.

Regulatory Requirements

A data sharing trusteeship can be offered as both a private sector and a government solution. There are already regulatory proposals for both concepts which are explained below. The goals in each case must be to create a secure space to evaluate large volumes of data by ensuring the highest standards of IT security law and placing this data evaluation on a secure legal basis in terms of protection law.

Private Sector Solution

Now, too, the merging and evaluation of data files in a server structure provided by a third-party is possible under data protection law based on the patient's express consent (Art. 9 (2) lit. a GDPR) and based on an overriding interest, Art. 9 (2) lit. j.) GDPR in conjunction with Paragraph 27 BDSG. However, both legal bases imply a considerable level of legal uncertainty in the case of evaluating large volumes of data. To remedy the problem of data under-use in medical research, it is appropriate to remove this legal uncertainty. If, firstly, high requirements are placed on data trustee structures in view of IT security, secondly, a transfer of the raw data is prohibited and made punishable by law, thirdly, the data to be evaluated is protected technically and under criminal law such that the risk to the data subject's rights and interests is minimised, a statutory authorisation act could permit the transfer of data to this data trustee as well as the evaluation of data in the data trustee. Corresponding

legislative proposals have already been made.¹³¹ Accordingly designed in a regulatory way, the data trustee has advantages in terms of data protection law: The data is not actually shared at any point but evaluated solely in the secure environment of the data trustee. Only the evaluation outcomes are shared, whereas the evaluated volumes of data in the trusteeship are deleted again after the evaluation process. There is no third-party entitlement to access data stored in the data trustee. The data trustee is instead merely the infrastructure solution for low-risk sharing and evaluation of large data sets.¹³² The permission to use a specific data trustee structure for a specific data trustee project could either be granted via a central "Permit Authority" or the data trustee models would have to be certified in advance via a government body, and, if certification requirements were met, could itself be entitled to decide on the use of the data trusteeship structure for the specific research project. The first companies offering such services can now be found on the market.¹³³

State Solution

Other proposals tend toward a state data trustee solution. The "Feasibility Study Virtual Network Health Data (NGD)" already developed such a state model for sharing and evaluating data sets in 2019,¹³⁴ and a current expert report commissioned by the Federal Ministry of Education and Research envisages such a solution, too.¹³⁵ It proposes the creation of an organisational structure in which healthcare institutions can provide and evaluate the health data they hold. To that end, a "neutral body" should be created that is subject to state supervision. Users could be both public and private healthcare institutions. This includes national healthcare institutions such as RKI, cancer registers, health insurance companies and research institutions; European institutions could also be connected to the NGD as users. The model provides for NGD users, if operating in public healthcare, to be obliged to transfer data to the NGD upon request of another user for analytical purposes. Companies operating in the free economy are to participate voluntarily, however.¹³⁶ However, it could be considered whether claims to data access to private healthcare providers should also be justified in such a model.¹³⁷ Only the analysis results are used by the data trustee, the evaluated data are subsequently deleted.¹³⁸

In this respect, it is designed in a similar way to the private sector model: The same questions largely arise in terms of data protection, and even if this data trustee model is selected, a decision on the processing basis under data protection law is required. Here, too, consent and permission solutions with an opt-out opportunity can be taken into account. However, a central authority for data sharing and evaluation – whether on a European, a national or federal state levels – always harbours greater risks for the informational self-determination of data subjects than decentral solutions such as those currently emerging in the private sector. On the other hand, the NGD merely stores data centrally for a short period of time; in principle, it remains stored decentrally with the users. Technically, both the European legislator and the federal and state legislators should be able to meet the highest IT security requirements. However, a correspondingly high level of security could also be prescribed by law and certified by the state for data trustees operating in the private sector. From a problem-solving perspective, there is also nothing to prevent the authorisation of both state and private sector solutions.

5.2.3 Suitability of DGA-E and EHDS for the Solution-orientated Regulation of Data Trustees in the Health Sector

The Data Governance Act also contributes little to the solution-orientated regulation of data trustees in the health sector. All the same, the provisions of Chapter 2 stipulate that “data held by public authorities”, which is likely to include data held in government registers in particular, may not be subject to any exclusive agreements and thus anticipates potential conflicts of data use from public authorities. The DGA-E shall not apply to the private data sharing trusteeship because it merely mediates data access and access to data analysis results between closed provider and demand groups.¹³⁹ The DGA-E does not allow for the state data sharing trustee without further ado, because data in state hands that fulfils the requirements of Art. 3 DGA-E – and is thus at least potentially in the hands of state solutions – must not in principle only be made accessible to a limited group of persons. Something else will only apply if this is necessary for the provision of a service in the general interest, Art. 4 (2) DGA-E. Although this is justifiable regarding the medical data sharing trustees, it needs to be clarified at a European level in any case. This

interpretation is likely to be reinforced by the fact that Chapter 2 of the DGA-E focuses on data generated with the help of public funds and not on data that has merely been evaluated with the help of public funds. However, the latter argument does not apply to the evaluation results. Having said that, the requirements of the Data Governance Act do not apply to data that has already been collected for the purposes of further use, but only for such data whose intended purpose changes.

An interesting question is whether the ePA is subject to the requirements of data altruism or those for data intermediaries, in other words provides a data sharing service within the meaning of Art. 9 lit. b) DGA-E. However, as a service offered by the statutory health insurance funds, it should not constitute a “commercial service” as defined in Art. 2 (2a) DGA-E because the statutory health insurance funds are public corporations. In any case, according to the Council version dated 24 September 2021, they are not subject to the requirements for data intermediaries, cf. Art. 2 (2a) lit. d) DGA-E.¹⁴⁰ In this respect, the question only arises for ePA offers from private insurance companies that do not yet exist on the market (but are laid out in Paragraph 341 IV, V SGB V). The ePA would at least potentially fall under either the requirements for data intermediaries from Chapter 3 of the DGA-E or the requirements for altruistic data intermediaries from Chapter 4 DGA-E. Yet since it is a prerequisite for data altruistic organisations that they themselves operate on a non-profit basis and this is unlikely to apply to health insurance funds organised under private law,¹⁴¹ such a privately offered ePA may only be subject to the requirements of Chapter 3 DGA-E as far as its scope of application is open. The ePA establishes a legal and technical relationship between data hosts (the insured persons) on the one hand, and potential users on the other. Its status as an “intermediation service” pursuant to Art. 2 (2a) DGA-E¹⁴² could at most be opposed by the ePA merely being open to insured persons and those entitled to use it. If the intention were to consider this as a closed group of persons, the necessary focus of a data intermediary toward mediation between an undetermined number of data hosts and data users would not be fulfilled. It could also be justified that only one insured person can use his/her respective ePA and for this reason, too, there is no mediation between an undetermined number of data hosts and data users. Yet this is countered by the fact that potentially anyone who fulfils the require-

ments may belong to the group of insured persons and authorised users, and potentially any insured person of a statutory health insurance fund may use an ePA. The DGA-E does not intend to exclude such services from the scope of application, it merely calls for services to be open to a number of both data users and data hosts that is not determined in advance. The DGA-E should therefore also be applicable if it places certain requirements on data hosts and data users.¹⁴³ Whether an ePA operated by private health insurance funds would be a data intermediary as defined by Art. 2 (2a) DGA-E cannot yet be answered clearly due to these various interpretations. In particular, the prohibition of vertical integration that data intermediaries must comply with pursuant to Art. 9 DGA-E would present considerable challenges for private health insurance funds offering the ePA. The EHDS-Act could not deviate from these requirements either since the Data Governance Act sets minimum requirements that can only be exceeded but not fallen short of.

Statutory health insurance funds operate according to the ECJ ruling dated 11 June 2009, C-300/07, Ref No. 49 on a not-for-profit basis which is why they are generally considered to be a data altruistic organisation. Chapter IV DGA-E intends to facilitate the voluntary provision of data by individual persons or companies for the common good (data altruism; Rec. 35 explicitly mentions health care in this context). To this end, organisations operating, or better still, promoting data altruism, should be able to register as “data altruistic organisations recognised in the Union” to strengthen trust in their activities. A common consent form could be developed for data altruism to reduce the cost of obtaining consent and facilitating the transferability of data.¹⁴⁴ In particular, legal uncertainties in connection with data provided on an altruistic basis for scientific research and for statistical purposes are to be removed (Rec. 39).

Data altruism has a certain similarity with data release according to Paragraph 363 (1, 8) SGB V.¹⁴⁵ However, the prerequisite is that data altruism activities are exercised via a legally independent structure which is separate from other activities conducted by the data altruistic organisation, Art. 16 lit. c DGA-E. If this condition is met, a consent form provided via a terminal device within the meaning of Art. 22 DGA-E could be used to obtain informed consent pursuant to Paragraph 363 (2) SGB V in the future.

5.3 Data Trustees in the Mobility Sector

5.3.1 Data of the Connected Car: The Discussion so far

An exceptionally large share of mobility data is emerging in connected vehicles, which constantly generate and process data via a large number of sensors, such as for operating driver assistance systems. At the same time, cars are connected to other actors via mobile communication (connectivity), with which they constantly exchange data (also in real time). In this respect, connected vehicles can be compared to many other smart devices (Internet of Things). The data collected in this process can relate to a wide range of aspects: Technical data pertaining to the operation of the vehicle (and its components), data on the location, speed, driving behaviour of the drivers, data on external conditions such as weather, traffic (including congestion), road conditions, but also data on the use of entertainment providers and other services offered online via the car through the car occupants. Considering the growing use of connected cars, the operation of these vehicles gives rise to an ever-greater amount of mobility data that could be used by a variety of actors (also in real time). In addition to the car manufacturers, its suppliers as well as car repair and maintenance companies (remote diagnosis and maintenance), and insurance companies (with new insurance models), such mobility data may also be interesting for many other innovative service providers that can offer their services to car users within the ecosystem of connected driving (navigation, entertainment, online shopping etc.). Having said that, such data may also be particularly important for fulfilling tasks of public interest such as road safety, accident research, traffic control, investigation of accidents, environmental protection, and scientific research.¹⁴⁶

For years, there has been intense competition policy debate in the EU on the question of access of firms, car users and public institutions to this data generated in the vehicle (“access to in-vehicle data and resources”).¹⁴⁷ The starting point of this conflict lies in the car manufacturers’ decision for a certain governance concept for the connected car (so-called “extended vehicle” concept), which ensures their exclusive control over the data generated in the cars. Many other service providers who would like to offer car users their services in the connected car, fear that car

manufacturers will use this exclusive control over the data from the connected car to foreclose them from the lucrative business of new manifold services or demand a high price for access to these markets.¹⁴⁸ The conflict of interests between car manufacturers on the one side, and all other stakeholders in the emerging connected driving ecosystem on the other, already became clear on the C-ITS platform initiated by the EU Commission, where the stakeholders were unable to agree on solutions for access to this mobility data.¹⁴⁹ A study commissioned by the Commission came to the conclusion in 2017 that the “extended vehicle” concept used by car manufacturers is not a suitable solution to the problem, for example due to the ensuing competition problems, and therefore preference should be given to other solutions.¹⁵⁰ One of these solutions was the so-called “shared server” concept, which corresponds to a data trustee solution. Although the Commission has acknowledged the need to solve this problem of “access to in-vehicle data and resources”¹⁵¹, it has not yet presented a proposal for a solution.

In the following, we will at first analyse the various existing problems as regards data from connected vehicles, and then discuss the proposed solutions. In this context, the proposal of a data trustee solution, which has not been adequately addressed in the current discussion, will be presented for this study in particular.

5.3.2 Analysis of the Problem

5.3.2.1 Accident Research in the Connected Vehicle

There are three main problems for data in the mobility sector, each of which requires different problem-solving concepts: In the case of connected vehicles, the first problem to emerge is that of accident investigations of vehicles with automated driving functions. Attempts have already been made to solve this problem with a data trustee as well as various data access obligations:

Specific data from vehicles with automated driving functions must be transmitted to third parties and may be made available to third parties for the purposes of accident research, Paragraph 63a paras. 3 and 5 StVG. This data is to be collected by an access-moderating data trustee.¹⁵² Section 63a of the StVG (Straßenverkehrsgesetz) is to be distinguished

from Section 1g (5) of the StVG, according to which the Federal Motor Transport Authority is entitled to make non-personal data from vehicles with autonomous driving functions accessible to research bodies for traffic-related public benefit purposes, including accident research.¹⁵³ These regulations are still very new and only time will tell whether they are actually suitable as a problem-solving approach or whether it needs legislative adjustments.

The decisive factor is that there is a reliance on vehicle data, particularly regarding switching automated driving functions on and off, for investigating the causes of an accident with partially automated driving; however, this data is on the servers of the car manufacturers, which are at the same time interested parties in these disputes. To thus secure the integrity of vehicle data to be made available, a data trustee solution seems useful for this special data, i.e. this data can be used in a tamper-proof way in the event of accidents. Yet, it is a special set of data for a very specific, narrowly defined purpose. Of course, there may also be other exclusive access solutions to certain data of a connected car, in which data is to be stored outside the access range of the car manufacturers. A special data trustee solution could be useful here.

5.3.2.2 Data Access of Public Institutions and the Scientific Community

The mobility sector overall is also confronted with the problem of an increasingly articulated need for data access by public bodies vis-à-vis private data holders, such as for fulfilling public service tasks. For instance, the state seeks access to mobility data from navigation systems to enable intelligent transport systems. Having said that, it may be important for state institutions to get access to certain types of mobility data not only for traffic control, but also for other public interest purposes. Furthermore, access to mobility data could be important for research purposes. Here, too, the question arises as to whether data trustee solutions have a role to play.

5.3.2.3 Competition Problem due to the “Extended Vehicle” Concept

However, the main problem in the mobility sector, which could also be resolved with a data trustee, is, thirdly, still the competition problem associated with data in the connected car. It will therefore be in the focus of the following remarks. For a meaningful discussion on the possible contribution of a data trustee solution and its adequate design, it is however necessary to analyse the problem in detail and compare it with other solution options.

Important for understanding this competition problems is that it is a well-known problem in the automotive industry. For decades, car manufacturers have repeatedly tried to prevent competition with independent providers on the markets for repair and maintenance services as well as spare parts. In this respect, competition policy long felt the need to protect undistorted competition between car manufacturers (and their authorised repairers) and the independent repair and maintenance companies (as well as spare parts manufacturers). Because access to essential repair and maintenance information and data (particularly vehicle diagnostic data), which only car manufacturers have at their disposal, has already played a critical role in the past, there has been a (FRAND-like) regulation in the Motor Vehicle Type Approval Regulation since 2007 obliging car manufacturers to provide essential repair and maintenance information (including diagnostic data) in order to ensure such undistorted competition on the so-called aftermarkets in the automotive sector.¹⁵⁴ This comprehensive sector-specific regulation is a mandatory access regime to this information (and diagnostic data) for independent vehicle repair and maintenance businesses. It also encompasses mandatory technical interfaces (like the OBD adapter found in every vehicle), standardised formats of information provision, regulatory measures in relation to vehicle safety as well as a charging scheme for providing this information. Despite minor problems, this regulation was so far capable to protect competition on the motor vehicle repair and maintenance markets.¹⁵⁵ The problem, however, is that this information and data access regulation has not yet been adequately adapted to the new technology of connected vehicles.¹⁵⁶

How can the problems arising for competition, innovation and consumer choice from the extended vehicle concept used by the automotive industry be briefly summarised?¹⁵⁷ According to this governance approach for the connected vehicle, the car manufacturers have exclusive control (1) over the data generated by cars, since this data is directly transferred to proprietary (back-end) servers at the car companies. This means that without the consent of car manufacturers, neither car users nor other actors such as insurance companies, repair shops, navigation services or public bodies (for example for traffic regulation) can access this huge amount of mobility data. While car manufacturers are in principle willing to provide access to certain types of mobility data against payment, this is only on their own terms, i.e. they can freely decide which data they want to make available and at what prices and conditions. What is more, car manufacturers (2) also have exclusive control over technical access to the vehicle’s IT system, in other words, without the car manufacturer’s consent it is not possible to conduct remote diagnosis, repairs and maintenance for example through independent service providers, or to get access to the vehicle’s dashboard in order to make service offers to car users.¹⁵⁸ This means that car manufacturers have designed the vehicles as closed systems, over which they exercise exclusive control.¹⁵⁹ In this respect, there is not only a data access problem, but also an interoperability problem, especially regarding complementary services to connected driving.¹⁶⁰

As a result, car manufacturers have attained a genuine gatekeeper position for all secondary markets in the connected driving ecosystem with the “extended vehicle” concept, because no access to data generated by car users and the vehicle’s IT system is possible without their consent.¹⁶¹ From a competition economics perspective, this means that they can gain complete control over all markets for complementary products and services, which requires either access to this data or access to the vehicle’s IT system.¹⁶² This enables car manufacturers to easily leverage their market power to these markets, distort competition or foreclose competitors. This may also have a serious negative impact on innovation activities in secondary markets, because it may block innovations by independent service providers, as well as significantly restrict consumers, i.e., the car users, regarding their free choice of service providers on

these complementary markets, as they can only use service providers that have previously concluded contracts with car manufacturers. This refers not only to traditional aftermarket service providers such as repair and maintenance companies, but also to the manifold new services that can be offered on such secondary markets in the connected driving ecosystem.¹⁶³ It is particularly interesting, that the “extended vehicle” concept enables car manufacturers to de facto “appropriate” data generated by car users through the operation of the vehicle,¹⁶⁴ in order to monetise it in a variety of ways.¹⁶⁵ Car manufacturers can therefore become monopolistic providers of mobility data generated in the vehicles sold by them. Yet, from an economic point of view, it is very doubtful whether this will lead to an efficient and innovation-stimulating use of this mobility data.¹⁶⁶

5.3.3 Problem-solving Options

5.3.3.1 Overview

In 2016, the EU Commission had brought together “stakeholders” concerning connected and automated driving as part of its “Cooperative Intelligent Transport System” initiative, to tackle the associated problems. In this context, various models have been developed on how to solve the “access to in-vehicle data and resources” problem. In addition to the car manufacturers’ “extended vehicle” concept, two other models in particular have emerged as alternatives, which have been supported by other “stakeholders” in this C-ITS process. These are (1) the so-called “shared server” concept and (2) the “on-board application platform”.¹⁶⁷

With the “**shared server**” concept, there is the same technical solution at first, i.e., that data generated in the vehicle will be transferred to an external server outside the vehicle via which access to data can then take place. However, this server is not under the control of the car manufacturer, but rather a neutral entity that manages this data and can make it accessible to others according to certain principles.¹⁶⁸ This can be understood as a data trusteeship solution, which we will develop in more detail below.

The “**on-board application platform**” is primarily another technological solution that does not require data to be transferred to an external server but enables the storage and processing of data in the car.

This requires open and interoperable telematics systems, but for whose development a longer period of time is needed. With this solution, interface standardisation applicable to all manufacturers is needed for the entire automotive mobility system for the exchange of data and interoperability with complementary services, as are uniform safety standards that reliably guarantee the necessary very high security of vehicles (including cyber security). The openness and interoperability of such a standardised technical solution for the entire mobility system makes it technically possible for car users themselves to exercise control over data generated in the vehicle, and to freely decide which service providers they give access to their vehicle. They can then choose between all service providers that meet the safety standards, which can be ensured by mandatory certification. Besides eliminating car manufacturers’ gatekeeper position, the development of such standardised “on-board application platforms” is necessary in the longer-term for the future transition to an integrated mobility system with automated (and autonomous) driving in any case.¹⁶⁹

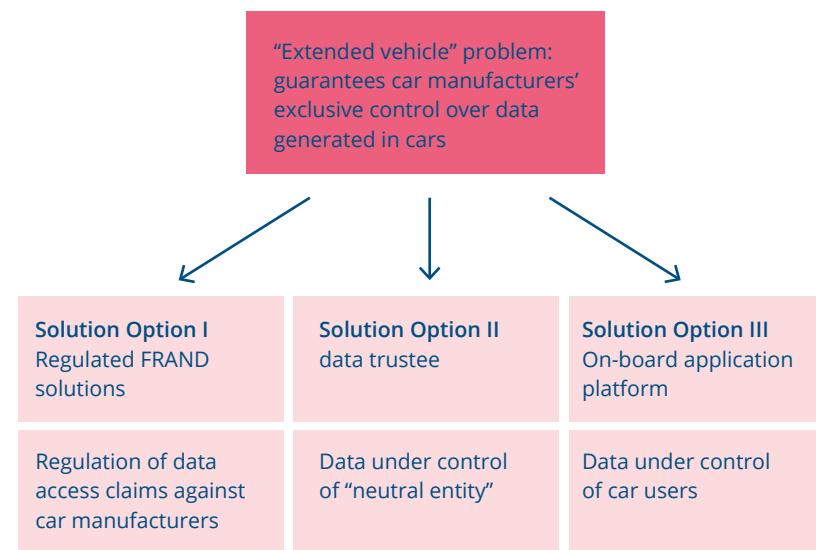
In the discussion so far, there is broad consensus (except for car manufacturers) that the “extended vehicle” concept has serious problems regarding competition on secondary markets and other associated negative effects on innovation and consumer choice. This was also the result of the TRL Study (2017) commissioned by the EU Commission, which made a comprehensive comparison between these three solutions: In the long-term, the “on-board application platform” and in the short- and medium-term the “shared server” solution should be preferred over car manufacturers’ “extended vehicle” concept.¹⁷⁰ In this context, it has been clarified that these solutions, particularly the “on-board application platform”, make it possible to meet at least equally high safety standards as with the “extended vehicle” concept.¹⁷¹ In this respect, the car manufacturers’ main argument to date, that only the “extended vehicle” concept enables a sufficiently high degree of safety and should therefore be preferred over other solutions despite competition problems, is not correct.¹⁷²

Already years ago, the EU Commission has acknowledged the need for a solution to the problems arising from the “extended vehicle” concept, and has already announced solutions. In its European Data Strategy in

February 2020, the Commission underlined the importance of sharing large volumes of “in-vehicle data” for innovative mobility-related services, and announced a reform of the Motor Vehicle Type Approval Regulation as a sector-specific regulation solution in which “the rights and interests of the car-owners generating the data are respected and compliance with data protection rules are ensured”¹⁷³. Considering the planned “Data Act”, solutions could in principle also be discussed within such a legislative framework.¹⁷⁴

Regarding the type of solution, discussions seem to have primarily focused on a regulatory FRAND (“fair, reasonable, and non-discriminatory”) solution regarding access to “in-vehicle data and resources”, or the introduction of the “on-board application platform”. In this study, we would also like to present and discuss the further option of an additional data trustee solution (based on the “shared server” idea). Since the requirements for a suitable solution can be most easily explained with the regulatory solution with FRAND access, we will at first present this before proceeding to the data trustee solution and “on-board application” solution.¹⁷⁵

Figure 3: Solution options for access to data in the connected car



5.3.3.2 Solution Option I: Regulated Access Regime with FRAND Solutions

Since a (FRAND-like) sector-specific regulatory access regime for information and data already exists in the EU (Type Approval Regulation for Motor Vehicles) for protecting competition in the area of repair and maintenance services, the obvious approach is to develop such a regulatory regime also in relation to the problem of access to “in-vehicle data and resources” for the new much broader connected and automated driving ecosystem. This could be implemented as a very far-reaching reform within the Motor Vehicle Type Approval Regulation, whereby a comprehensive adaptation to the new technical and economic condition of the connected car would be necessary.¹⁷⁶ In the simplest case, car manufacturers would continue to apply the “extended vehicle” concept with the transfer of data to external servers under their control, but the regulatory access regime would impose extensive obligations on them to grant other stakeholders access to these data under FRAND conditions. This would not only apply to the classic repair and maintenance service providers,

but also to many other providers of connected driving ecosystem services, to facilitate and ensure undistorted competition and free innovation activities in these secondary markets.

Firstly, it is important that car manufacturers should not be able to favour themselves (or their authorised repairers) over other companies.¹⁷⁷ A correspondingly designed FRAND solution could in principle help to ensure this. However, it is crucial, particularly regarding innovation, that non-discriminatory data access claims must not only refer to pre-existing services or those offered by car manufacturers themselves, but that service providers can also gain access to other data for enabling them to innovatively develop and offer new services. Therefore, it should not be the car manufacturers who decide (according to their own profit interests) on the set of data to be made accessible by FRAND solutions. This, instead, is a regulatory decision that must be taken based upon objective criteria (competition and innovation) by a regulatory authority.¹⁷⁸ Otherwise, no free innovation activities from independent service providers would be possible in this ecosystem, at least insofar as access to such data is necessary for them.

Furthermore, according to our above analysis of the gatekeeper problem, it is clear that regulation must not only solve the data access problem, but also the interoperability problem, i.e., independent service providers need to have the opportunity to gain non-discriminatory technical access to the vehicle under FRAND conditions, so as to also offer “remote services” to car users. The same applies to access to the vehicle’s dashboard to ensure a level playing field for communication with customers. In this respect, standardised interoperable technical interfaces (for data exchange and interoperability) as well as a standardised security concept (with certification solutions for service providers) are also necessary for this solution. It is also regarding interoperability that the regulator must decide objectively on which access should be granted under which conditions.¹⁷⁹ These decisions, too, should not be determined by the profit interests of car manufacturers, but rather by the goal of safeguarding competition, innovation and consumer interests. This also includes a clear scheme for fees regarding access to data and technical access to the vehicle.

Given that the existing Type Approval Regulation for Motor Vehicles already entails regulations regarding fair and non-discriminatory access to information and data, standardised technical interfaces, security standards (including security-related certifications) as well as a charging scheme, the most important regulatory building blocks are already in place. Having said that, it is still a big step to adapt this regulatory regime to the new technological and economic conditions of the connected driving ecosystem, since access is necessary not only for narrowly defined repair and maintenance services, but also for diverse and often still unknown services and uses of this data. Therefore, the already discussed openness for innovation plays an entirely different and much more significant role here than in the traditional aftermarket.¹⁸⁰ The main problem of the FRAND regulation solution is the risk of too narrow definitions regarding to which data should be granted FRAND access, or that even car manufacturers themselves can decide to which data they grant access under FRAND conditions. The same applies to interoperability. Under the conditions of the “extended vehicle” concept, car manufacturers always have a strong interest in keeping restrictions to their exclusive control over data and interoperability to a minimum. In this respect, a strong regulatory solution is needed to reduce the negative impact on competition, innovation and consumer choice ensuing from this gatekeeper position as far as possible.¹⁸¹ That is the reason why also the far more fundamental alternative solutions “shared server” and “on-board application platform” were discussed in this competition policy debate from the beginning, since they offer the opportunity to prevent the emergence of such a gatekeeper position of car manufacturers in the first place. This leads us directly to the following debate on a data trustee solution.

5.3.3.3 Solution Option II: Data Trustee

The data trustee solution (building on the original “shared server” idea), initially entails the same technical solution as the “extended vehicle” concept, namely that data generated in the vehicle will be transmitted to an external server outside the vehicle, via which data access can then take place. However, this server is not under the control of the car manufacturer but a “neutral entity” that manages this data and can make it accessible according to certain principles.¹⁸²

Data Trustee as Obligatory Data Host

The fundamental idea is that in principle all data generated in the car will be under the control of such a data trustee, i.e., the back-end server will be under the governance of the data trustee and no longer under the control of the car manufacturers.¹⁸³ This data trustee solution can also only be realised as part of a regulation, which requires car manufacturers to implement such a technical solution.¹⁸⁴ It is up to the legislator (or a regulatory body commissioned with it) to decide, on the basis of objectives to be pursued, on the principles and conditions according to which this data is to be made accessible to other companies and institutions. Institutionally, this data trustee could be a state body, or an institution organised under private law that is entrusted with this data trusteeship task. This institution should be non-for-profit and financed by cost-covering fees.

Crucial for decisions to be taken by the data trustee are the objectives and principles that need to be defined by the legislator. In addition to protecting competition, important goals could be the promotion of innovation, the protection of consumers, particularly regarding data protection, safety and environmental objectives in the mobility sector as well as scientific research. The great benefit of a data trustee solution is that it can also enable the integration of public interest objectives that play a key role in the mobility sector, such as road safety and traffic regulation etc., from the outset. This would imply that specific additional legal regulations for such access to data would no longer be necessary.¹⁸⁵ At the same time, such a data trustee would also facilitate the linking of this data generated in the car with mobility data from other areas, which would also open up new perspectives for the envisaged Common European Mobility Data Space (and for example also the Gaia-X project).¹⁸⁶ This cannot be discussed here. Important, however, is that such a data trustee solution could fulfil far more tasks and solve more problems than only the competition and innovation problems relating to secondary markets in the connected driving ecosystem.

On the Design of Data Access Regulations

The legislator can use these objectives as a guide when setting up the governance of the data through the data trustee, i.e., the guidelines for decisions to whom it makes data available and under what conditions. It can be suggested that the data trustee might primarily make this data accessible according to FRAND conditions. However, owing to the diversity of available data, strong differentiations will also be necessary as to which companies should get access to which data. A distinction will have to be made between various stakeholders with their different purposes. Yet the data to be made available should not be too narrowly defined to support broad innovation activities regarding new services. Regarding technical vehicle data, car manufacturers (and also their suppliers) will undoubtedly remain in a special position, particularly with respect to data that is directly necessary for operating the vehicle. The same is true for data that can be protected by intellectual property rights or trade secrets (except, for instance, with respect to database protection). Beyond data access for private companies that want to offer new products and services on complementary secondary markets, anonymised mobility data should also be made available as input for emerging data marketplaces and for further analysis and processing of such data. Furthermore, based on public interest objectives, data on road conditions, traffic conditions, data relevant for environmental protection, data for accident research or for clarifying liability issues in case of accidents or for the sovereign task of periodic technical surveillance of vehicle safety should be made accessible to the public institutions via the data trustee. Such data access should – where possible and reasonable – also be possible in real-time. Broad access to this data for research purposes would also be especially important. These data access regulations have to be precisely defined in each case.¹⁸⁷

From these considerations, depending on the objectives, there is considerable scope for the concrete design of such a data trustee solution for mobility data generated in the connected car. In this respect, data access and data trustee must be considered together. It is not sufficient to establishing a data trustee, it requires comprehensive legislative decisions on which data should be made available to whom, for what purpose and under which conditions.

Ensuring Consumer and Data Protection

What is the relationship between such a data trustee and consumers who, as car users, generate this data when driving? Interestingly, consumers have so far only played a very minor role in the economic policy debate on access to “in-vehicle data and resources”. This is partly attributable to the prevailing competition policy perspective, whereby it is assumed that if competition would work on secondary markets, consumers benefit in the form of lower prices, more innovation and freedom of choice.¹⁸⁸ In fact, however, the transition to the connected vehicle raises new fundamental questions that did not play a role in the previous information and data access regulation of the Motor Vehicle Type Approval Regulation. Compliance with the data protection rules of the GDPR is of crucial importance here. In the case of the currently applied “extended vehicle” concept, the car manufacturers must obtain the consent of car users for the processing of personal data according to data protection law. Since the connected vehicle (or certain functions) cannot be used without such consent, the question arises to what extent car users can make granular decisions about when and which data they provide to car manufacturers for which purposes for further processing and use or whether they are only offered the option of a general consent. From a data protection perspective the question has to be asked whether consent to data collection is effective at all without such a granular consent possibility (at least for data not required for the operation of the car).¹⁸⁹ The Federal Commissioner for Data Protection and Freedom of Information (BfDI) has just rejected this elsewhere for non-granular consent.¹⁹⁰ With the data trustee solution discussed here, it would be possible that the data trustee sets a higher standard for data protection for car manufacturers than that existing under the current (and concretely often unclear) requirements of the GDPR. This means that it may exceed the minimum standard of the GDPR (including better implementation of “privacy by design” and “privacy by default” principles). As a result, such a data trustee solution could also strengthen data and consumer protection in the use of connected vehicles.

Interoperability Specifications

So far, such a data trustee solution would only resolve the competition and innovation problems arising from an exclusive control of data by car manufacturers through the “extended vehicle” concept. It does not resolve the problem of exclusive control of car manufacturers regarding technical access to the vehicle (as well as the dashboard in the vehicle). This means that even with the data trustee solution, it remains necessary to resolve the problem of interoperability for the provision of complementary in-vehicle services through a regulatory approach. In this respect, standardised interoperable technical interfaces (for data exchange and interoperability) as well as a standardised security concept (with certification solutions for service providers) are also necessary for this solution. In principle, these are the same tasks that are also needed in a regulation solution regarding FRAND data access (cf. the above solution option I). This does not need to be explained in more detail here. It does, however, imply that a much greater regulatory role must be assigned to the data trustee than “merely” making decisions on access to this data. It also needs to directly deal with interoperability and standardisation issues as well as with security concepts (including security certifications), just as a regulatory authority has to do under solution option I.¹⁹¹ This is not surprising, because, in many contexts, effective data access solutions also require regulatory decisions on interoperability, security (and often data protection).¹⁹²

Design Options

It is not possible to go into detail here on the specific design options of such a data trustee. It is undoubtedly important that the further specification of the data access regulations is only possible with the help of the experts of stakeholders in this connected and automated driving ecosystem (car manufacturers, independent service providers etc.) and public institutions that require certain data for fulfilling their task in the public interest, as well as business and consumer associations, etc. In this respect, close cooperation between the data trustee and these stakeholders is also of central importance, also with regard to car manufacturers. This raises many specific questions of institutional design that cannot be discussed here.

5.3.3.4 Solution Option III: “On-board Application Platform”

So far, we have assumed the technical solution as currently practised in the “extended vehicle” concept, namely that the data is directly transferred to an external server, which gives either the car manufacturer or the data trustee exclusive control over the data, i.e. it can only be made accessible to others with their consent. However, with the technical solution of open and interoperable “on-board application platforms”, on which data could be directly stored and processed, and software could be installed for specific applications, entirely different and much more far-reaching solutions would be technically possible. This is because control over this data and access to the vehicle could now in principle be exercised by the car users (including car owners) themselves. This would remove the technical bottleneck that gives car manufacturers exclusive control over data or access to the vehicle and would in turn facilitate the complete elimination of the car manufacturer’s gatekeeper position. Yet, as already mentioned, these open interoperable telematics platforms require extensive industry-wide technical standardisation and regulations regarding security (including a certification system).

With this technical solution the connected vehicle is no longer a closed system, but an open system from the car user’s perspective. In principle, this would allow free undistorted competition and free innovation activities on secondary markets of the connected driving ecosystem, because the car users can directly provide the necessary data to service providers and allow technical access. This does not, however, ensure that all problems are solved, i.e. competition is protected and the mobility data generated in the connected cars are used in an economic efficient way and in line with society’s goals. Firstly, other new potential problems need to be prevented. For instance, car manufacturers could restore the previously technically induced exclusivity of control over data and technical access to the vehicle through imposing far-reaching contractual obligations.¹⁹³ Furthermore, large digital platforms, such as Google and Apple, could enter this new market with car owners, which might lead to many advantages for car users but can also give rise to completely new market power problems.

However, important for our question is whether, secondly, data trustees could also play an important role under such a regime of open interoperable platforms. Due to the far greater opportunities regarding how the markets might develop under this (more open) regime, this question is not easy to answer. If car users themselves decide on the use of data in the connected vehicle and have exclusive control over this, then it may become very difficult for public institutions or academia to gain access to large data sets generated in the vehicles for public interest purposes, for example traffic data, data on road conditions, environmental data, or data for traffic safety purposes and accident research or for scientific research. For these purposes, it is often necessary to have large (and sometimes also real-time) data sets. Therefore, it may be necessary that legal obligations for vehicle owners exist for making such data available to the relevant public institutions. A data trustee commissioned by the legislator, which could be similarly organised as in solution option II, could be tasked with collecting such data from connected cars and then making it accessible – in a suitable form and in compliance with data protection – to public institutions or for scientific research purposes according to legal requirements. Whether such a data trustee should collect and make available large, anonymised data sets for innovation purposes or for training algorithms, for instance as part of a European Mobility Data Space, would be another option that could be discussed. This depends on the development of private markets for mobility data, which could be created by car owners’ own control over data.

Overall, a data trustee could also play a vital role when implementing the “on-board application platform” solution but it probably would have to fulfil fewer tasks than in solution option II.

5.3.4 Discussion and Conclusions

The discussed solution options regarding problems arising from the car manufacturer’s “extended vehicle” concept can be summarised and compared as follows:

Regulated FRAND Access Solution

As a short-term solution, it might be easiest that car manufacturers technically continue to apply the “extended vehicle” concept (with transmitting

the data to their external server) and combine this with a comprehensive regulation regarding access to this mobility data as well as technical access to the vehicle (“remote access”). This would also require an implementation of technological interfaces and security standards to secure competition, innovation and consumer choice on complementary secondary markets. The basic idea is to limit the still existing gatekeeper position of the car manufacturers as far as possible through such a regulatory access regime. This could be achieved via a comprehensive reform of the current access regime of the Motor Vehicle Type Approval Regulation.

Data Trustee Solution

In this case, data from the connected vehicle would be directly under the control of a data trustee, who makes this data accessible to other companies and public institutions (including car manufacturers) according to legally determined goals and principles, both to secure competition and for public welfare purposes. Owing to the additional interoperability problem, FRAND regulation of technical access to the vehicle is also necessary. This implies that the data trustee would also be assigned a regulatory role regarding interoperability and security standards beyond simply granting access to data (like the one that is necessary for a regulated FRAND solution). However, a data trustee solution offers more opportunities for opening these large sets of mobility data for innovation, public interests, and consumers.

“On-board Application Platform”

This solution would establish a uniform standard for open interoperable telematics systems and a standardised security system in the overall system of connected and increasingly automated driving. Technically, this would make it possible for car users themselves to decide on the use of data generated in their vehicles and the technical access to the vehicle. This could directly eliminate car manufacturers’ gatekeeper position, which is the cause of competition and innovation problems on secondary markets. This does not, however, mean that new competition problems cannot arise that need to be solved. A data trustee could also play a vital role here, especially for collecting and using mobility data from the connected car, which would be necessary for public interest purposes in the mobility sector.

This study had not the objective to conduct a comprehensive analysis of the problem of governing data generated in connected cars and deriving policy recommendations from it. Here the primary issue is the possible role of data trustee solutions. Yet this cannot be answered in isolation from the problems and alternative solutions proposed. In this respect, a brief concluding analysis follows.

The competition problems caused by the “extended vehicle” concept are well-known and need not be repeated here. What is necessary, however, is to view the problem again from the more general perspective of data economics and data policy. Data are non-rival goods that can be used by many at the same time. The EU Commission’s communication “Building a European Data Economy” (2017) with its diagnosis that data is not used or re-used enough, and this has a negative impact on innovation and the data economy, was a big step forward in the data policy debate, on which the current European data strategy is still based.¹⁹⁴

The ecosystem of connected and automated driving in the mobility sector is a complex system, in which many millions of car users will generate a huge amount of mobility data in the future, which in turn can be used in the most diverse ways by many other companies and public institutions, partly for new services for car users themselves, and partly for the data economy, but partly also for improvements in road safety, traffic regulation, accident research etc. From an economic (and even more from a societal) perspective, it is highly problematic when a very small number of private companies can in fact gain exclusive control over all this data and can decide only according to their own profit interests about access and use of these data.¹⁹⁵ From an economic point of view, such a monopolistic control over data from vehicles sold by car manufacturers not only leads to the much-discussed competition problem, but equally to a systematic under-use of this data for manifold innovation activities and for improving public policies.¹⁹⁶

The problems of data access are primarily attributed to two causes: (1) Companies collect lots of data, but transaction costs on the market are too high for sharing them more with other companies on a voluntary basis. The Data Governance Act, for example, aims to solve this prob-

lem by creating trustworthy data intermediaries. (2) The second problem are attempts by companies to gain permanent advantages through their exclusive control over certain types of data or through strategies of data monopolisation to the detriment of competition, with the manifold negative effects already discussed. Attempts of car manufacturers to permanently (!) implement the “extended vehicle” concept as a central concept for governance of data generated in the vehicles by car users needs to be understood as such a data monopolisation strategy. This is also reinforced and secured by the lack of interoperability due to a design of the vehicles as closed systems.¹⁹⁷

Therefore, the problem of access to “in-vehicle data and resources” is not only a problem between car manufacturers and independent service providers in the connected and automated driving ecosystem, as the traditional discussion suggests. It is not only about distortions of competition on secondary markets and the foreclosure of independent service providers. The range of stakeholders is far wider and encompasses car users, the general data economy and public institutions active in the mobility sector in the public interest. This is also the perspective adopted by the Common European Mobility Data Space and its objectives. From this perspective, the idea of a data trusteeship solution, which could only be sketched briefly as solution option II here, seems to be an interesting and exciting option that is worthwhile for being systematically conceptually developed and analysed regarding its benefits and problems. Such an option could not be implemented over the short-term, but we are talking about the medium- and long-term governance of massive amounts of data in the future that will be generated by car users operating connected vehicles, and the preservation of free competition and free innovation activities within the future mobility system.

Conclusions

What conclusions can be derived from this?

1. To protect competition and innovation within this ecosystem, it is necessary to set clear legal framework conditions that either severely limit the power of car manufacturers' gatekeeper position or – much better – prevent the emergence of such a gatekeeper role in the first place.

2. Since the current “extended vehicle” can no longer be accepted, a provisional solution to the problem could be the implementation of a strict regulation of the application of the “extended vehicle” concept with far-reaching data access obligations under FRAND conditions as soon as possible. The easiest way could be a further reform of the Motor Vehicle Type Approval Regulation. Due to the specific technological and economic conditions, however, a sector-specific regulatory solution is required in any case.¹⁹⁸
3. Parallel to such a solution, plans should urgently be developed for the medium- and long-term solution of the suitable governance connected and automated vehicles:
 - › This concerns, firstly, the governance of data generated in connected vehicles by car users. Here, the possibility of a data trusteeship solution that has been neglected in previous discussions so far, should be seriously examined, as suggested in solution option II, particularly in connection with solutions for other mobility data and the strategy of a European Mobility Data Space.
 - › Secondly, this also includes the development of standardised open telematics platforms for connected and automated driving. They can not only help to solve the interoperability problems, which emerge in all problem-solving options. They are also an important precondition for the integration of the connected vehicles into an already emerging mobility system for automated and ultimately autonomous driving.¹⁹⁹

5.3.5 Suitability of the DGA-E for Resolving the Problem

Outside the area of connected car data, data trustee solutions should be considered a potential option on the issue of governance of specific types of mobility data, which may be appropriate under certain conditions. The specific design of such data trustee solutions will determine whether regulations under the planned Data Governance Act are relevant and, if so, could help. The DGA cannot contribute toward the data trusteeship solution for connected car data (solution option II) discussed here but would not impede such a solution either.

- 28 *Specht/Kerber*, Datenrechte – Eine rechts- und sozialwissenschaftliche Analyse im Vergleich Deutschland – USA, ABIDA – Assessing Big Data, 2017, p. 119 et seq.
- 29 *Hoffman/Lutz/Ranzini*, Privacy cynicism: A new approach to the privacy, available at: <https://cyberpsychology.eu/article/view/6280/5888> (6.3.2018); *Smith/Dinev/Xu*, 35 MIS Quart 2011, 989.
- 30 BVerfG, decision of 15/12/1983 – 1 BvR 209/83, BVerfGE 65, 1, 43.
- 31 BVerfG, decision of 23/10/2006 – 1 BvR 2027/02, MMR 2007, 93, 93.
- 32 *Richter*, PinG 2016, 185, 186; *Specht-Riemenschneider/Bienemann*, in: *Specht-Riemenschneider/Werry/Werry* (ed.), Datenrecht in der Digitalisierung, 2020, p. 329.
- 33 *Rothmann*, Ungewollte Einwilligung? Die Rechtswirklichkeit der Informierten Zustimmung im Fall von Facebook, dated 02/11/2017, p. 7, can be found in *Rothmann/Buchner*, DuD 2018, 342 (344); making reference to: *Jennessen*, Datenschutzrecht, in press.
- 34 On the data protection provisions of Facebook: LG Berlin, judgement dated 16/01/2018 – 16 O 341/15, GRUR-RS 2018, 1060 Ref No. 40.
- 35 *Arnold*, GfK 1990, 150, 152.
- 36 *Buck-Heeb/Lang*, in: BeckOGK German Civil Code (BGB), § 675 Ref No. 248 et seq. (Status: 01/09/2021); *Köndgen*, BKR 2011, 283, 283 et seq.; *Eidenmüller*, JZ 2005, 216, 218 et seq.; *Koch*, BKR 2012, 485, 485; *Koller*, in: Commemorative publication for Huber, 2006, p. 821, 824 et seq.; *Spindler*, in: Commemorative publication for Säcker, 2011, S. 469, 474 et seq.; *Sedlmeier*, Rechtsgeschäftliche Selbstbestimmung im Verbrauchervertrag, 2012, p. 134 et seq.; *Möllers/Kernchen*, ZGR 2011, 1, 1 et seq.; *Arendts*, Die Haftung für fehlerhafte Anlageberatung, 1998, p. 23; see also: *Specht*, Diktat der Technik, 2019, p. 167.
- 37 *Martinek*, in: Grundmann, Systembildung und Systemlücken in Kerngebieten des Europäischen Privatrechts, 2000, p. 511, 524; see also: *Specht*, Diktat der Technik, 2019, p. 168.
- 38 *Arnold/Hillebrand/Waldburg*, DuD 2015, 730, 730 et seq.; *Kühnl*, Persönlichkeitsschutz 2.0, Diss. Köln 2016, p. 342; *Calo*, 87 Notre Dame Law Review 1027, 1071 (2012); *Heckmann/Paschke*, in: *Ehmann/Selmayr*, Datenschutz-Grundverordnung, 2nd edition 2018, Art. 12 Ref No. 53.
- 39 See current study: *Rothmann*, Ungewollte Einwilligung? Die Rechtswirklichkeit der Informierten Zustimmung im Fall von Facebook, can be read at: DuD 2018, 342, 344.
- 40 *Arnold/Hillebrand/Waldburg*, DuD 2015, 730, 732.
- 41 Cf. on this: *Specht-Riemenschneider/Bienemann*, in: *Specht-Riemenschneider/Werry/Werry* (ed.), Datenrecht in der Digitalisierung, 2020, p. 330.
- 42 European Commission, Special Eurobarometer 431 – Data Protection, 2015, p. 85, 89; cf. also: *Spindler/Thorun/Wittmann*, Rechtsdurchsetzung im Verbraucherschutz, p. 13
- 43 *Specht-Riemenschneider/Bienemann*, in: *Specht-Riemenschneider/Werry/Werry* (ed.), Datenrecht in der Digitalisierung, 2020, p. 330.
- 44 *Kelley/Breese/Cranor/Reeder*, A “Nutrition Label” for Privacy, p. 6, available at: <http://cups.cs.cmu.edu/soups/2009/proceedings/a4-kelley.pdf> (06/02/2018).
- 45 *Kelley/Cesca/Breese/Cranor*, Standardizing Privacy Notices: An Online Study of the Nutrition Label Approach, p. 8.
- 46 Art. 13a (2) of the parliamentary bill on the GDPR dated 12/03/2014 (EP-PE_TC1-COD(2012)0011).
- 47 *Kroeber-Riel*, Bildkommunikation, 2nd edition 1996, S. 26ff., 53ff.; cf. also: *Maar*, in: *Maar/Burda*, Iconic Worlds, 2006, p. 11.
- 48 *Bauer/Fischer/Mclnturff*, ZfbF 51 (9/1999), 805, 815; *Schierl*, Text und Bild in der Werbung, 2001, p. 228.
- 49 *Kroeber-Riel*, Bildkommunikation, 2nd edition 1996, p. 53; cf. zur Geschwindigkeit visueller Kommunikationsaufnahme: *Boehme-Neßler*, BilderRecht, 2010, p. 64 et seq.
- 50 *Kroeber-Riel*, Bildkommunikation, 2nd edition 1996, p. 102.
- 51 On the reasons cf. *Kroeber-Riel*, Bildkommunikation, 2nd edition 1996, p. 73 et seq. m. w. Nachw.; on image recollection cf. also: *Madigan*, in: Yuille, Imagery, Memory and Cognition, 1983, p. 65, 65 et seq.; *Specht*, Diktat der Technik, in press; cf. on the whole situation also: *Specht-Riemenschneider/Bienemann*, in: *Specht-Riemenschneider/Werry/Werry* (ed.), Datenrecht in der Digitalisierung, 2020, p. 334 et seq.; *Geminn/Francis/Herder*, ZD-Aktuell 2021, 05335; *Gerpött*, MMR 2020, 739;
- 52 *Krämer*, Journal of Competition Law & Economics 2021, 263; *Wendehorst/Schwamberger/Grinzingler*, in: *Pertot* (ed.), Rechte an Daten, 2020, p. 104 et seq.
- 53 On the analysis of the anticipation calculus in the framework of legal remedies cf. *Brandes/Weise*, German Working Papers in Law and Economics 2009, Paper 7; cf. also *Kaesling/Knapp*, MMR 2020, 816 (820).
- 54 *Urban/Karaganis/Schofield*, UC Berkeley Public Law Research Paper No. 2755628, 2017, p. 45; cf. also *Kaesling/Knapp*, MMR 2020, 816 (820).
- 55 *Akester*, Technological accommodation of conflicts between freedom of expression and DRM: the first empirical assessment, 2009, p. 104 et seq.; *Penney*, Stanford Technology Law Review 2019, p. 412.
- 56 *Kerber*, WuW 2021, p. 400.
- 57 *Kerber*, WuW 2021, p. 400.
- 58 Europäischer Datenschutzbeauftragter (EDSB), Stellungnahme zu Systemen für das Personal Information Management (PIM), Stellungnahme 9/2016 (201), p. 6.
- 59 *Janssen/Cobbe et al.*, Internet Policy Review 2020, Volume 9, Issue 4, 1 (2), available at: <https://doi.org/10.14763/2020.4.1536> (last accessed on: 18/11/2021).
- 60 Definition based on: *Weinzierl*, NVwZ 2020, 1087.
- 61 *Engeler*, Statement on the draft of a Telecommunications Telemedia Data Protection Act (TTDSG), BT Committee Bulletin 19(9)1056, 20.04.2021, p. 4 et seq., available at: https://www.bundestag.de/resource/blob/836166/e95c01bdb37ed9f6c08ef-027cd902e471/19-9-1056_Stellungnahme_SV_Dr_Engeler_oeATTDSG_21-04-2021-data.pdf (last accessed on: 18/11/2021); *Janssen/Cobbe et al.*, Internet Policy Review 2020, Volume 9, Issue 4, 1 (13 et seq.), available at: <https://doi.org/10.14763/2020.4.1536> (last accessed on: 18/11/2021).
- 62 Legally regulating data trustees – statement by the federation of German consumer organisations, p. 6, available at: https://www.vzbv.de/sites/default/files/downloads/2020/04/06/20-02-19_vzbv-positionspapier_pims.pdf (last accessed on: 18/11/2021).
- 63 *Freiherr von Ulmenstein*, DuD 2020, 528, 529.
- 64 Cf. on the contractual design between data subjects and data trustees *Pinsent Masons et al.*, Data trusts: legal and governance considerations, 2019, p. 26 et seq., available at: <https://theodi.org/wp-content/uploads/2019/04/General-legal-report-on-data-trust.pdf> (last accessed on: 18/11/2021).
- 65 *Specht-Riemenschneider/Blankertz et al.*, MMR-Beil. 2021, 25, 40 et seq.

- 66 Legally regulating data trustees – Statement by the vzbz, available at: https://www.vzbv.de/sites/default/files/downloads/2020/04/06/20-02-19_vzbv-positionspapier_pims.pdf (last accessed on: 18/11/2021).
- 67 The Data Ethics Commission also sees both perspectives on PIMS, cf. Data Ethics Commission Expert Report, October 2019, p. 135, available at: https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/gutachten-datenethik-kommission.pdf;jsessionid=92AD72B05F123D4DBFCC72D56297DE96.2_cid295?__blob=publicationFile&v=6 (last accessed on: 18/11/2021).
- 68 Data Ethics Commission Expert Report, October 2019, p. 134, available at: https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/gutachten-datenethik-kommission.pdf;jsessionid=92AD72B05F123D4DBFCC72D56297DE96.2_cid295?__blob=publicationFile&v=6 (last accessed on: 18/11/2021).
- 69 *Schwartmann/Benedikt/Reif*, MMR 2021, 99, 101; *Schwartmann/Hanloser/Weiß*, PIMS im TTDSG – Vorschlag zur Regelung von Diensten zur Einwilligungsverwaltung im Telekommunikation-Telemedien-Datenschutzgesetz, brief expert report, March 2021, p. 10, available at: https://enid.foundation/wp-content/uploads/2021/03/Schwartmann_Hanloser_Weiss-Kurzgutachten_Dienste_zur_Einwilligungsverwaltung_20210302.pdf (last accessed on: 18/11/2021); a. A. *Assion*, Stellungnahme als Sachverständiger zu BT-Drs. 19/27441, Committee Dossiers. 19(9)1039 dated 19/04/2021, p. 12, available at: https://www.bundestag.de/resource/blob/835498/3f-c24ea374301c2ba608c9509c-c64ec1/19-9-1039_Stellungnahme_SV_Assion_oeA_TTDSG_21-04-2021-data.pdf (last accessed on: 18/11/2021).
- 70 An overview of the market failure problems in the standard setting are provided by *Farrell/Simcoe*, Four Paths to Compatibility, in: *Peitz/Waldfoegel*, The Oxford Handbook of the Digital Economy, 2012, pp. 34–58.
- 71 In the scope of application of Art. 13, 14 GDPR, this is only possible if text-based information is additionally provided, cf. *Specht-Riemenschneider/Bienemann*, in: *Specht-Riemenschneider/Werry/Werry* (ed.), Datenrecht in der Digitalisierung, 2020, p. 324 et seq.
- 72 *Specht-Riemenschneider/Bienemann*, in: *Specht-Riemenschneider/Werry/Werry* (ed.), Datenrecht in der Digitalisierung, 2020, p. 339; SVRV – Gutachten zur Lage der Verbraucherinnen und Verbraucher 2021, S. 392, available at: https://www.svr-verbraucherfragen.de/wp-content/uploads/SVRV_Gutachten_2020.pdf (last accessed on: 18/11/2021).
- 73 *Kroeber-Riehl*, Bildkommunikation, 1996, p. 53, p. 73 et seq.
- 74 Such solutions for example are being developed at the Weizenbaum Institute, cf. MMR-Aktuell 2019, 419389.
- 75 Disclaiming: *Ernst*, ZD 2017, 110, 111; *Klement*, in: NK-DatenschutzR, 1. Edition 2019, Art. 7 DSGBO Ref No. 37; *Taeger*, in: *Taeger/Gabel*, DSGVO/BDSG, 3. edition 2019, Art. 7 DSGVO Ref No. 10; *Schulz*, in: Gola, DS-GVO, 2nd edition 2018, Art. 7 DSGVO Ref No. 9; *Heckmann/Paschke*, in: *Ehmann/Selmayr*, DS-GVO, 2nd edition 2018, Art. 7 DSGVO Ref No. 34; *Helfrich*, in: *Hoeren/Sieber/Holzsnagel*, MultimediaR, October 2020, part 16.1.D.I. Ref No. 51; but for that: *Janicki*, DSRITB 2019, 313, 323; *Hoffmann*, NZS 2017, 807, 808; *Specht*, in: *Specht/Mantz*, Hdb. Europäisches und deutsches DatenschutzR, 1st edition 2019, § 9 Ref No. 42; *Ingold*, in: *Sydow*, EU DSGVO, 2nd edition 2018, Art. 7 DSGVO Ref No. 19; *Buchner/Kühling*, in: *Kühling/Buchner*, DSGVO/BDSG, 3rd edition 2020, Art. 7 DS-GVO, Ref No. 31.
- 76 On the overall approval cf. *grundlegen: Ohly*, „Volenti non fit iniuria“ – Die Einwilligung im Privatrecht, 2002.
- 77 *Specht-Riemenschneider*, in: *Specht/Mantz*, Hdb. Europäisches und deutsches DatenschutzR, 1st edition 2019, § 9 Ref No. 42; *Ingold*, in: *Sydow*, EU DSGVO, 2nd edition 2018, Art. 7 DSGVO, Ref No. 19; *Buchner/Kühling*, in: *Kühling/Buchner*, DS-GVO/BDSG, 3rd edition 2020, Art. 7 DS-GVO, Ref No. 31.
- 78 *Specht-Riemenschneider*, in: *Specht/Mantz*, Hdb. Europäisches und deutsches DatenschutzR, 1st edition 2019, § 9, Ref No. 42; *Ingold*, in: *Sydow*, EU DSGVO, 2nd edition 2018, Art. 7 DSGVO, Ref No. 19; *Buchner/Kühling*, n: *Kühling/Buchner*, DS-GVO/BDSG, 3rd edition 2020, Art. 7 DS-GVO, Ref No. 31; *Kühling*, ZfDR 2021, 1, 8.
- 79 Applicable to this *Kühling*, ZfDR 2021, 1, 8.
- 80 *Riesenhuber*, in: *Riesenhuber*, Europäische Methodenlehre, 3rd edition 2015, § 10 Ref No. 4–7.
- 81 Cite MMR article
- 82 MüKo BGB-Schubert, 8th edition 2018, § 164 Ref No. 72.
- 83 *Lang*, TTDSG – Neuregelung des Datenschutzes in den Bereichen Telekommunikation und Telemedizin geplant, K&R 2020, 714, 716; *Richter*, Stellungnahme zur öffentlichen Anhörung des Wirtschaftsausschusses on 24/02/2021 zum Entwurf eines Gesetzes zur Regelung des Datenschutzes und des Schutzes der Privatsphäre in der Telekommunikation und bei Telemedizin, 2021, p. 3, available at: https://www.bundestag.de/resource/blob/835918/ed8f50751361504905b-fa51b4ee6f738/19-9-1045_Stellungnahme_SV_Richter_Stiftung_Datenschutz_oeA_TTDSG_21-04-2021-data.pdf (last accessed on: 18/11/2021).
- 84 *Art.-29-Datenschutzgruppe*, WP 259, p. 13; WP 187, p. 20 et seq.; WP 131, p. 9.
- 85 *Verbraucherzentrale Bundesverband*, Personal Information Management Systems (PIMS), 2020, p. 7, available at: https://www.vzbv.de/sites/default/files/downloads/2020/04/06/20-02-19_vzbv-positionspapier_pims.pdf, last accessed on 16/07/2021.
- 86 Available at: https://www.medizininformatik-initiative.de/sites/default/files/2020-04/MII_AG-Consent_Einheitlicher-Mustertext_v1.6d.pdf (last accessed on: 18/11/2021).
- 87 Data Ethics Commission Expert Report, October 2019, p. 127, available at: https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/gutachten-datenethik-kommission.pdf;jsessionid=92AD72B05F123D4DBFCC72D56297DE96.2_cid295?__blob=publicationFile&v=6 (last accessed on: 18/11/2021).
- 88 Data Ethics Commission Expert Report, October 2019, p. 127, available at: https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/gutachten-datenethik-kommission.pdf;jsessionid=92AD72B05F123D4DBFCC72D56297DE96.2_cid295?__blob=publicationFile&v=6 (last accessed on: 18/11/2021).
- 89 Data Ethics Commission Expert Report, October 2019, p. 126 et seq., available at: https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/gutachten-datenethik-kommission.pdf;jsessionid=92AD72B05F123D4DBFCC72D56297DE96.2_cid295?__blob=publicationFile&v=6 (last accessed on: 18/11/2021).
- 90 *Specht/Blankertz* et al, MMR-Beil. 2021, 25 (42 et seq.).

- 91 Data Ethics Commission Expert Report, October 2019, recommendation 23, p. 140, available at: https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/gutachten-datenethikkommission.pdf;jsessionid=92AD72B05F123D4DBFCC72D56297DE96.2_cid295?_blob=publicationFile&v=6 (last accessed on: 18/11/2021).
- 92 Cf. On this option only *Golland*, MMR 2018, 130 (134); *Golland*, Datenschutzregulierung als Eingriff in Wertschöpfungsmodelle, in: *Ochs/Friedewald/Hess/Lamla* (ed.), *Die Zukunft der Datenökonomie*, 2019, p. 45, p. 54.
- 93 See IV above.
- 94 Cf. *Blankertz/Specht-Riemenschneider*, What regulation for data trusts should look like, p. 28 et seq., available at: https://www.stiftung-nv.de/sites/default/files/regulation_for_data_trusts_0.pdf (last accessed on: 18/11/2021).
- 95 Cf. *vzbv*, Neue Datenintermediäre, 15/09/2020, p. 7, available at: <https://www.vzbv.de/publikationen/datenintermediaere-gesetzlich-regeln> (last accessed on: 18/11/2021).
- 96 *Krämer*, *Journal of Competition Law & Economics*, 2020, 1 (38)
- 97 Cf. *Schwartmann/Hentsch*, PinG 2016, 117 et seq.; but on the other hand: *Bisges*, MMR 2017, 301; *Specht*, in: *Stiftung Datenschutz, Datendebatten, Rechte an Daten – Regulierungsbedarf aus Sicht des Verbraucherschutzes*.
- 98 Data Ethics Commission Expert Report, October 2019, p. 134, available at: https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/gutachten-datenethikkommission.pdf;jsessionid=92AD72B05F123D4DBFCC72D56297DE96.2_cid295?_blob=publicationFile&v=6 (last accessed on: 18/11/2021).
- 99 Bundestag printed paper 19/29839, p. 78.
- 100 Bundestag printed paper 19/29839, p. 78.
- 101 So too: *Golland*, NJW 2021, 2238, 2241.
- 102 Applicable: *Golland*, NJW 2021, 2238, 2241.
- 103 Findata exists in Finland for this purpose, see. <https://findata.fi/en/> (last accessed on: 18/11/2021). In Australia, health data stored via “My Health Record” are managed by a “Data Governance Board”, cf. *Australian Department of Health*, Framework to guide the secondary use of My Health Record system data, p. 15, available at [https://www1.health.gov.au/internet/main/publishing.nsf/content/F98C37D22E65A79B-65A79BCA2582820006F1CF/\\$File/MHR_2nd_Use_Framework_2018_ACC_AW3.pdf](https://www1.health.gov.au/internet/main/publishing.nsf/content/F98C37D22E65A79B-65A79BCA2582820006F1CF/$File/MHR_2nd_Use_Framework_2018_ACC_AW3.pdf) (last accessed on: 18/11/2021). See the following section on both institutions.
- 104 Gutachten zur Weiterentwicklung medizinischer Register zur Verbesserung der Dateneinspeisung und -anschlussfähigkeit, available at: https://www.bundesgesundheitsministerium.de/fileadmin/Dateien/5_Publikationen/Gesundheit/Berichte/REG-GUT-2021_Registergutachten_BQS-TMF-Gutachtenteam_2021-10-29.pdf, p. 255 et seq. (last accessed on: 18/11/2021).
- 105 Whether Findata or the data holder itself is responsible for granting permissions is determined by § 44 of the Secondary Use Act.
- 106 See on all this *Specht-Riemenschneider*, Studie zur Regulierung eines privilegierten Zugangs zu Daten für Wissenschaft und Forschung durch die regulatorische Verankerung von Forschungsklauseln in den Sektoren Gesundheit, Online-Wirtschaft, Energie und Mobilität, August 2021, p. 102 et seq., available at: https://www.jura.uni-bonn.de/fileadmin/Fachbereich_Rechtswissenschaft/Einrichtungen/Lehrstuehle/Specht/Dateien/2021-08-25-LSR.pdf (last accessed on: 18/11/2021).
- 107 *Australian Government – Department of Health*, Framework to guide the secondary use of My Health Record system data, p. 31, available at: [https://www1.health.gov.au/internet/main/publishing.nsf/content/F98C37D22E65A79B-CA2582820006F1CF/\\$File/MHR_2nd_Use_Framework_2018_ACC_AW3.pdf](https://www1.health.gov.au/internet/main/publishing.nsf/content/F98C37D22E65A79B-CA2582820006F1CF/$File/MHR_2nd_Use_Framework_2018_ACC_AW3.pdf) (last accessed on: 18/11/2021).
- 108 *Australian Government – Department of Health*, Framework to guide the secondary use of My Health Record system data, p. 47, available at: [https://www1.health.gov.au/internet/main/publishing.nsf/content/F98C37D22E65A79B-CA2582820006F1CF/\\$File/MHR_2nd_Use_Framework_2018_ACC_AW3.pdf](https://www1.health.gov.au/internet/main/publishing.nsf/content/F98C37D22E65A79B-CA2582820006F1CF/$File/MHR_2nd_Use_Framework_2018_ACC_AW3.pdf) (last accessed on: 18/11/2021).
- 109 *Australian Government – Department of Health*, Framework to guide the secondary use of My Health Record system data, p. 31, available at: [https://www1.health.gov.au/internet/main/publishing.nsf/content/F98C37D22E65A79B-CA2582820006F1CF/\\$File/MHR_2nd_Use_Framework_2018_ACC_AW3.pdf](https://www1.health.gov.au/internet/main/publishing.nsf/content/F98C37D22E65A79B-CA2582820006F1CF/$File/MHR_2nd_Use_Framework_2018_ACC_AW3.pdf) (last accessed on: 18/11/2021). See on all this *Specht-Riemenschneider*, Studie zur Regulierung eines privilegierten Zugangs zu Daten für Wissenschaft und Forschung durch die regulatorische Verankerung von Forschungsklauseln in den Sektoren Gesundheit, Online-Wirtschaft, Energie und Mobilität, August 2021, p. 106 et seq., available at: https://www.jura.uni-bonn.de/fileadmin/Fachbereich_Rechtswissenschaft/Einrichtungen/Lehrstuehle/Specht/Dateien/2021-08-25-LSR.pdf (last accessed on: 18/11/2021).
- 110 *Australian Government – Department of Health*, Framework to guide the secondary use of My Health Record system data, p. 51, available at: [https://www1.health.gov.au/internet/main/publishing.nsf/content/F98C37D22E65A79B-CA2582820006F1CF/\\$File/MHR_2nd_Use_Framework_2018_ACC_AW3.pdf](https://www1.health.gov.au/internet/main/publishing.nsf/content/F98C37D22E65A79B-CA2582820006F1CF/$File/MHR_2nd_Use_Framework_2018_ACC_AW3.pdf) (last accessed on: 18/11/2021).
- 111 For the exact reasons, cf. above VI. 3.
- 112 *Kircher*, GuP 2021, 1, 5 et seq.
- 113 Cf. Also *Strech/von Kielmannsegg/Zenker/Krawczak/Semler*, „Datenspende“ – Bedarf für die Forschung, ethische Bewertung, rechtliche, informationstechnologische und organisatorische Rahmenbedingungen, 2020, p. 125 et seq., available at: https://www.bundesgesundheitsministerium.de/fileadmin/Dateien/5_Publikationen/Ministerium/Berichte/Gutachten_Datenspende.pdf (last accessed on: 18/11/2021).
- 114 https://www.tmf-ev.de/zoombild.aspx?img=/Portals/0/TMF_07rz_01.jpg&-text= (last accessed on: 18/11/2021); <https://www.tmf-ev.de/News/article-Type/ArticleView/articleId/4456.aspx>, last accessed on 18/11/2021; *Specht-Riemenschneider*, Studie zur Regulierung eines privilegierten Zugangs zu Daten für Wissenschaft und Forschung durch die regulatorische Verankerung von Forschungsklauseln in den Sektoren Gesundheit, Online-Wirtschaft, Energie und Mobilität, p. 127, available at: https://www.jura.uni-bonn.de/fileadmin/Fachbereich_Rechtswissenschaft/Einrichtungen/Lehrstuehle/Specht/Dateien/2021-08-25-LSR.pdf (last accessed on: 18/11/2021).
- 115 Cf. also: *Kircher*, GuP 2021, 1, 4.
- 116 Cf. §§ 13, 15 *Gesundheitstelematikgesetz* 2012, version from 18/11/2021.

- 117 *Samuelson/Zweckhauer*, Journal of Risk and Uncertainty, p. 7 et seq.
- 118 Cf. data protection criticism levelled against the German regulation, which according to the data protection authorities provides for too little granularity of consent and thus does not meet the requirements for voluntary consent: DSK, resolution dated 01/09/2020, available at: https://www.datenschutzkonferenz-online.de/media/en/20200901_PDSG_Entschlie%C3%9Fung.pdf (last accessed on: 18/11/2021); on the question whether a granularity of consent is actually necessary for its voluntariness: *Kircher*, GuP 2021, 1, 8 et seq.
- 119 *Specht-Riemenschneider*, Studie zur Regulierung eines privilegierten Zugangs zu Daten für Wissenschaft und Forschung durch die regulatorische Verankerung von Forschungsklauseln in den Sektoren Gesundheit, Online-Wirtschaft, Energie und Mobilität, p. 143, available at: https://www.jura.uni-bonn.de/fileadmin/Fachbereich_Rechtswissenschaft/Einrichtungen/Lehrstuehle/Specht/Dateien/2021-08-25-LSR.pdf (last accessed on: 18/11/2021).
- 120 *Jarass*, in: *Jarass*, EU-Grundrechte-Charta, 4th edition, 2021, Art. 13 Ref No. 8 mwN. 324 Bernsdorff, in: *Meyer/Hölscheidt*, Charta der Grundrechte der Europäischen Union, 5th edition, 2019, Art. 13 Ref No. 14.
- 121 *Specht-Riemenschneider*, Studie zur Regulierung eines privilegierten Zugangs zu Daten für Wissenschaft und Forschung durch die regulatorische Verankerung von Forschungsklauseln in den Sektoren Gesundheit, Online-Wirtschaft, Energie und Mobilität, p. 148, available at: https://www.jura.uni-bonn.de/fileadmin/Fachbereich_Rechtswissenschaft/Einrichtungen/Lehrstuehle/Specht/Dateien/2021-08-25-LSR.pdf (last accessed on: 18/11/2021).
- 122 cf. Medizininformatik-Initiative, https://www.medizininformatik-initiative.de/sites/default/files/2020-04/MII_AG-Consent_Einheitlicher-Mustertext_v1.6d.pdf (last accessed on: 18/11/2021)
- 123 DSK, resolution, available at: https://www.datenschutzkonferenz-online.de/media/en/20200901_PDSG_Entschlie%C3%9Fung.pdf (last accessed on: 18/11/2021).
- 124 *Kickingeder/Burth* et al., Radiology 2016, 880 et seq.
- 125 *Specht-Riemenschneider*, GRUR Int. 2017, 1040 (1042 et seq.).
- 126 *Specht-Riemenschneider/Radbruch*, Deutsches Ärzteblatt, number 27/28 in 2021, available at: <https://www.aerzteblatt.de/archiv/220270/Datennutzung-und-schutz-in-der-Medizin-Forschung-braucht-Daten> (last accessed on: 18/11/2021).
- 127 *Specht-Riemenschneider/Radbruch*, Deutsches Ärzteblatt, number 27/28 in 2021, available at: <https://www.aerzteblatt.de/archiv/220270/Datennutzung-und-schutz-in-der-Medizin-Forschung-braucht-Daten> (last accessed on: 18/11/2021).
- 128 *Specht-Riemenschneider*, Studie zum Forschungsdatenzugang im Auftrag des BMBF, p. 142 et seq.
- 129 *Blankertz*, Vertrauliche Datentreuhand – Wie die Datentreuhand effektiv Daten schützen und sichern kann, published in DuD 2021.
- 130 *Blankertz*, Vertrauliche Datentreuhand – Wie die Datentreuhand effektiv Daten schützen und sichern kann, published in DuD 2021.
- 131 *Specht-Riemenschneider*, Studie zur Regulierung eines privilegierten Zugangs zu Daten für Wissenschaft und Forschung durch die regulatorische Verankerung von Forschungsklauseln in den Sektoren Gesundheit, Online-Wirtschaft, Energie und Mobilität, p. 148 et seq., available at: https://www.jura.uni-bonn.de/fileadmin/Fachbereich_Rechtswissenschaft/Einrichtungen/Lehrstuehle/Specht/Dateien/2021-08-25-LSR.pdf (last accessed on: 18/11/2021).
- 132 *Specht-Riemenschneider*, Studie zur Regulierung eines privilegierten Zugangs zu Daten für Wissenschaft und Forschung durch die regulatorische Verankerung von Forschungsklauseln in den Sektoren Gesundheit, Online-Wirtschaft, Energie und Mobilität, p. 148, available at: https://www.jura.uni-bonn.de/fileadmin/Fachbereich_Rechtswissenschaft/Einrichtungen/Lehrstuehle/Specht/Dateien/2021-08-25-LSR.pdf (last accessed on: 18/11/2021).
- 133 For example, Apheris oder Decentriq.
- 134 Machbarkeitsstudie virtuelles Netzwerk Gesundheitsdaten (NGD), p 2 et seq.
- 135 Cf. Gutachten zur Weiterentwicklung medizinischer Register zur Verbesserung der Dateneinspeisung und -anschlussfähigkeit, available at: https://www.bundesgesundheitsministerium.de/fileadmin/Dateien/5_Publikationen/Gesundheit/Berichte/REG-GUT-2021_Registergutachten_BQS-TMF-Gutachtenteam_2021-10-29.pdf (last accessed on: 18/11/2021).
- 136 Machbarkeitsstudie virtuelles Netzwerk Gesundheitsdaten (NGD), p 2 et seq.
- 137 *Specht-Riemenschneider*, Studie zur Regulierung eines privilegierten Zugangs zu Daten für Wissenschaft und Forschung durch die regulatorische Verankerung von Forschungsklauseln in den Sektoren Gesundheit, Online-Wirtschaft, Energie und Mobilität, p. 140, available at: https://www.jura.uni-bonn.de/fileadmin/Fachbereich_Rechtswissenschaft/Einrichtungen/Lehrstuehle/Specht/Dateien/2021-08-25-LSR.pdf (last accessed on: 18/11/2021).
- 138 On the individual processing steps cf. Machbarkeitsstudie virtuelles Netzwerk Gesundheitsdaten (NGD), p. 14 et seq.
- 139 Cf. Art. 1 DGA-E.
- 140 In the Council version dated 24/09/2021.
- 141 Health insurance funds usually operate in the legal for of AG or VVAG.
- 142 In the Council version dated 07/09/2021.
- 143 Applicable to this *Richter*, ZEuP 2021, 534, 650, citing further literature.
- 144 COM (2020) 767 final, p. 9; krit. *Veil*, Data Governance Act III: Datenaltruismus, CR-online.de Blog, 28/10/2021, available at: <https://www.cr-online.de/blog/2021/10/28/data-governance-act-iii-datenaltruismus/> (last accessed on: 18/11/2021).
- 145 *Spindler*, CR 2021, 98, 106.
- 146 Cf. basic information on connected vehicles, *OECD/ITF*, Automated and Autonomous Driving. Regulation under uncertainty. Corporate Partnership Report, 2015; *Alonso Raposo/Ciuffo/Makridis/Thiel*, The r-evolution of driving: from Connected Vehicles to Coordinated Automated Road Transport (C-ART), 2017 (doi:10.2760/225671).
- 147 Cf. as overview *Kerber*, JIPITEC, 2018, pp. 312–315; *Specht/Kerber*, Datenrechte – Eine rechts- und sozialwissenschaftliche Analyse im Vergleich Deutschland – USA, 2018, pp. 169–192; *Martens/Mueller-Langer*, Journal of Competition Law & Economics 16, 2020, pp. 116–141.
- 148 Cf. on the “extended vehicle” concept of the car manufacturers *ACEA*, Access to vehicle data for third-party services, 2016; *ACEA*, Access to in-vehicle data (November 2021); for a critique of other service providers and consumer associations cf. *GIGIEFA*, Commission Communication on “Free Flow of Data”. Input from the Independent Automotive Aftermarket, 2016; *FIA*, Policy Posi-

- tion on Car Connectivity, 2016; *BEUC*, Protecting European Consumers with connected and automated cars, 2017.
- 149 C-ITS Platform, Final Report, 2016, pp. 72–90.
- 150 *TRL*, Access to In-Vehicle Data and Resources – Final Report, 2017, pp. 8–16.
- 151 *EU Commission*, On the road to automated mobility, COM (2018) 283 fin., p. 13; Cf. also the European Parliament’s call for a solution (Report on a European strategy on Cooperative Intelligent Transport Systems (2017/2067(INI)). Committee on Transport and Tourism (PE610.712v02-00).
- 152 See the proposals of the 56th German Traffic Court Conference, Working Group II, Recommendation No. 5, available at: Janker, *SVR* 2018, 78, 79; similarly: vzbv, *Rechtssicher fahren mit automatisierten Fahrzeugen*, 2016, p. 14; critically: Brockmeyer, *ZD* 2018, 258, 259 f.; Wagner/Goebel, *ZD* 2017, 263, 267; and: Hoeren, *NZV* 2018, 153.
- 153 On the distinction/demarcation of § 63a to § 1g para. 5 see Möller, *DAR* 2021, 608, 610 f.; Steeger, *SVR* 2021, 128, 134; Wagner, *SVR* 2021, 287, 289 ff.
- 154 Regulation (EU) 715/2007 of 20 June 2007 of the European Parliament and of the Council 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, Official Journal of the European Union, L 171/1, 29/06/2007.
- 155 Kerber/Gill, *JIPITEC*, 2019, p. 255 et seq.
- 156 Cf. the latest reform in 2018: 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, Official Journal of the European Union, L 151/1, 14.06.2018. This reform of the Motor Vehicle Type Approval Regulation has not solved this problem (cf. in detail Kerber/Gill, *JIPITEC*, 2019, pp. 250–254).
- 157 Cf. on the following analysis from an economic perspective Kerber, *JIPITEC*, 2018, pp. 310–331; Martens/Mueller-Langer, Access to digital car data and competition in aftersales services, Digital Economy Working Paper 2018-06, JRC Technical Reports, 2018.
- 158 Access to the dashboard (HMI = Human Machine Interface) is important for direct communication between car users and independent service operators.
- 159 On the advantages and disadvantages of open and closed models of connected vehicles cf. Determann/Perens, *Berkeley Technology Law Journal*, 2017, p. 915.
- 160 Such combinations of data access problems and interoperability problems are well-known from other areas of competition policy.
- 161 This is a different gatekeeper concept than in the EU Commission’s proposal for a “Digital Markets Act”. This is about the access to the connected driving ecosystem with its manifold secondary markets, which car manufacturers can fully control through their exclusive control over the data and technical access.
- 162 For certain data, such as location data, there may also be the alternative of access via mobile phone data.
- 163 Cf. in more detail Kerber, *JIPITEC*, 2018, p. 318 et seq. Nor can it be expected that system competition between car manufacturers will solve this problem. Cf. *ibid.*, p. 324.
- 164 The authors are aware that the property law concept of “appropriation” is not suitable for intangible objects such as data; it should not be understood in this sense here, but rather express that manufacturers de facto gain control over the data concerned. Having said that, this de facto exclusive control over data can have the economic effect of an “ownership-like” position.
- 165 This problem, that manufacturers of smart devices can get exclusive control of data (generated with them by the users) and economically exploit it, also occurs in other areas such as smart agricultural machines or smart TV sets.
- 166 Cf. on the negative welfare effects of monopolistic data prices, Martens, in: Drexler, *Data Access, Consumer Interests and Public Welfare*, 2021, pp. 74.
- 167 On the various alternative solutions, cf. *C-ITS Platform*, Final Report, 2016, pp. 78–86; *TRL*, Access to In-Vehicle Data and Resources – Final Report, 2017, pp. 32–49; Martens/Mueller-Langer, Access to digital car data and competition in aftersales services, JRC Digital Economy Working Paper 2018-06, pp. 7–13.
- 168 In the car manufacturers’ “extended vehicle” concept, there is also a “neutral server” that only refers to that data that car manufacturers themselves want to make available to other service providers. This has nothing to do with the “shared server” solution and the solution of a “neutral” data trustee that will be presented in more detail later.
- 169 Cf. Martens/Mueller-Langer, Access to digital car data and competition in aftersales services, JRC Digital Economy Working Paper 2018-06, p. 13; Kerber, *JIPITEC*, 2018, p. 322, which also refers to the possibility of a market failure regarding the choice of optimal technology with respect to interoperability. Standardised “on-board application” platforms are also crucial for future V2I (vehicle-to-infrastructure) or V2V (vehicle-to-vehicle) communication for improving the driving safety and traffic flow.
- 170 *TRL*, Access to In-Vehicle Data and Resources – Final Report, 2017, pp. 8–16. *TRL* emphasises that all three solutions have advantages and disadvantages, but then comes to the above clear overall solution. For a detailed analysis of the positions of stakeholders in this discussion cf. Specht/Kerber, *Datenrechte – Eine rechts- und sozialwissenschaftliche Analyse im Vergleich Deutschland – USA*, 2018, pp. 169–191.
- 171 *TRL*, Access to In-Vehicle Data and Resources – Final Report, 2017, pp. 75–79; Martens/Mueller-Langer, Access to digital car data and competition in aftersales services, JRC Digital Economy Working Paper 2018-06, p. 12; *FIATÜVIT*, IT Security der On-Board Telematik Plattform, 2020; *ADPA et al.*, Secure On-board Telematics Platform Approach, February 2021.
- 172 Cf. also Kerber, *JIPITEC*, 2018, p. 318 et seq. This implies that there is no trade-off problem between competition and safety, i.e., we do not have to renounce competition in favour of more safety. Furthermore, the need for exclusive control over data cannot be derived from the safety argument (*ibid.*).
- 173 Cf. *EU Commission*, A European Strategy for Data, COM (2020) 66 fin., p. 27 et seq.; most recently, a proposal for a reform of the Motor Vehicle Approval Regulation was announced for the fourth quarter of 2021 but was postponed again.
- 174 Since so far, no proposal of the Data Act has been published, we cannot discuss this here.
- 175 Theoretically, thought could also be given to solving these data access problems through claims to data access under competition law or through the data portability right of Art. 20 GDPR.

- On the difficulties of a solution under competition law, cf. *Kerber*, *Journal of Competition Law & Economics*, 2019, pp. 381–426; on the problem of a solution via this data portability right, cf. *Martens/Mueller-Langer*, *Journal of Competition Law and Economics*, 2020, pp. 116–141; *Gill/Kerber*, *Competition Policy International*, *Antitrust Chronicle*, November 2020, pp. 54–59. Cf. also *Picht*, *International Review of Intellectual Property and Competition Law* 51, 2020, pp. 940–976.
- 176 Cf. also *Kerber/Gill*, *JIPITEC*, 2019, p. 255 et seq.
- 177 This has already been regulated in the previous access regime of the Motor Vehicle Type Approval Regulation, even if the concept of self-preference, which is now familiar from the discussion on digital platforms and the “Digital Markets Act” proposal, is not used explicitly. Important is also that car manufacturers are not allowed to monitor the retrieved data or gain advantages over independent service providers due to their much broader availability of data (*Kerber/Gill*, *JIPITEC*, 2019, 253f.).
- 178 From a competition policy perspective, the aim is to provide data for enabling more competition and innovation under FRAND conditions so that previously unknown new services and new markets can also emerge.
- 179 The current situation also assumes the necessity of a “separation of duties”, i.e., that those entities responsible for access authorisation and the approval of software by service providers are independent from car manufacturers as operators of connected vehicles.
- 180 In this sense, a procedure based on a predefined list of existing “use cases” is not suitable; rather a much stronger orientation toward the idea of “open data” from an innovation perspective is needed.
- 181 Consequently, approaches that rely on voluntary “data sharing” according to certain principles are completely insufficient for solving the problems for competition and innovation.
- 182 Although the “shared server” solution was already discussed on the C-ITS platform as a potential solution option and was also recommended by the TRL study, the question on the concrete design of this governance solution has not been discussed much. The initial idea was for all stakeholders interested in accessing the data to jointly manage it, i.e., the car manufacturers and several types of service providers (cf. *C-ITS Platform*, Final Report, 2016, p. 81 et seq.).
- 183 The question on where the data is stored can be solved in diverse ways. Decisive is the exclusive control by the data trustee.
- 184 The car manufacturers may also continue to be responsible for the vehicle’s IT system and the security (including liability), but would then assume only the role of an IT service provider.
- 185 For example, this would also apply to the above-mentioned special data trusteeship regulation regarding data from vehicles with automated driving functions, which are now stored at the Federal Motor Transport Authority’s research data centre.
- 186 “A Common European mobility data space, to position Europe at the forefront of the development of an intelligent transport system, including connected cars as well as other modes of transport. Such data space will facilitate access, pooling and sharing of data from existing and future transport and mobility databases.” (*EU Commission*, A European Strategy for Data, COM (2020) 66 fin., p. 22).
- 187 Although this is not the same case as “public sector information”, it can be considered whether the principles applied there could also play a role, at least in part, in the case of such a data trustee. After all, this data trustee also has the task of making data accessible for innovation and further economic use insofar the rights of third parties are not affected (trade secrets etc., data protection).
- 188 The automobile clubs and consumer associations have clearly taken the side of the independent service providers in this dispute over the “extended vehicle” concept. Cf. *FIA*, Policy Position on Car Connectivity, 2016; *BEUC*, Protecting European Consumers with connected and automated cars, 2017.
- 189 The stakeholders had agreed to five guiding principles on the above-cited C-ITS platform. The first of these principles refers to the approval on making data available: “(a) Data provision conditions: Consent: The data subject (owner of the vehicle and/or ... the user of the vehicle ...) decides if data can be provided and to whom, including the concrete purpose for the use of the data (and hence for the identified service). There is always an opt-out option for end users and data subjects. This is without prejudice to requirements of regulatory applications.” (*C-ITS Platform*, Final Report, 2016, p. 75 et seq.). Cf. from a consumer policy perspective *FIA*, Policy Position on Car Connectivity, 2016; *BEUC*, Protecting European Consumers with connected and automated cars, 2017, from a data protection perspective *Hornung/Goeble*, *Computer und Recht*, 2015, p. 265; *Hansen*, in: *Grundrechtsschutz im Smart Car*, 2019, p. 273; and from an economic perspective on the problems of car users as consumers with regard to this “consent” in data protection law *Kerber*, *JIPITEC*, 2018, p. 323.
- 190 *BfDI*, Musterbescheid gesetzliche Krankenkassen, available at: https://www.bfdi.bund.de/SharedDocs/Downloads/DE/DokumenteBfDI/AccessForAll/2021/2021_Musterbescheid-Gesetzliche-Krankenkasse.pdf?__blob=publicationFile&v=1 (last accessed on: 22/11/2021).
- 191 Of course, it might also be worth considering that the interoperability problem could be regulated in the Motor Vehicle Type Approval Regulation, whereas the data trustee is limited to the governance of data. Yet this would require a very careful coordination, because data and interoperability issues are closely linked with one another.
- 192 Cf. *Kerber*, in: *Drexl*, *Data Access, Consumer Interests and Public Welfare*, 2021, pp. 461–474.
- 193 As a consequence, such contractual tying agreements would have to be prohibited by competition law, at least regarding such data that are not required for the direct operation of the vehicle.
- 194 Cf. *EU Commission*, Building a European data economy, COM (2017) 9 final (10/1/2017); *EU Commission*, A European Strategy for Data, COM (2020) 66 fin.
- 195 The parallel problem of control of large amount of personal data by large digital companies is well known but so far also unsolved.
- 196 Especially regarding mobility data, the idea of “data as infrastructure” for innovation could be particularly applicable. Cf. *OECD*, *Data-Driven Innovation*, 2015; cf. also the recently published study on data commons *Bertschek/Bonin/Kühling/Thüsing/Wenzel*, *Entwicklung eines Konzepts zur Datenallmende* (Expertise im Auftrag des Bundesministeriums für Arbeit und Soziales), 2021 (IZA Research Report No. 119).

197 The new position paper published recently by the European automobile association *ACEA* (*ACEA Position Paper Access to in-vehicle data*, November 2021) defends the “extended vehicle” concept of car manufacturers again. This paper only includes small concessions, which do not change the core of this concept and the problems presented here. In particular, it also does not satisfy the requirements of a regulated FRAND data access solution as described here as solution option I.

198 This does not imply that not also a sophisticated combination of horizontal rules through the planned Data Act and additional sector-specific regulation might lead to effective solutions.

199 Already the ITS Directive of 2010 focused on a platform that allows connectivity with transport infrastructure (Directive 2010/40/EU on the framework for the deployment of Intelligent Transport Systems in the field of road transport and for interfaces with other modes of transport, OJEU L 207/1). Also, the (since 2018) mandatory eCall emergency call systems are based upon such a interoperable, standardised, secure, and open platform (Regulation (EU) 2015/758 of the European Parliament and of the Council of 29 April 2015 concerning type-approval requirements for the deployment of the eCall in-vehicle system based on the 112 service, OJEU L 123/77).

6 Summary of the Results in Legal Policy Recommendations for Action

The results of this report can be summarised in the following legal policy recommendations for action:

Fundamentals

1. The data trustee may help to resolve a wide range of problems in the digital economy. The crucial factor for their fiduciary character is the internal relationship with the data provider: A data trustee must align their actions with the interests of the other contracting party. Their own interests need to take a back seat where necessary. However, the data intermediary is not bound in this way in the internal relationship. “Data intermediary” is therefore the umbrella term, while “data trustee” is a sub form that can in turn can be structured differently.

In addition to key distinctions between centralised and decentralised data storage as well as obligatory and optional use, data trustees can assume a variety of functions, such as pseudonymisation and anonymisation or even the evaluation of data. Besides PIMS, data escrows can therefore also be data trustees, for example.

2. Owing to the different possibilities for design, various data trustee models are taken into consideration to solve different problems. Regulation should be based on these existing problems and create a functioning legal framework for the respective data trustees necessary for solving the problem.

3. However, the data trustee can only ever be one element of such a solution. Other solution components must be added. What is needed is at least a triad of data trustee, data access and interoperability.

Data Trustees in the Online Sector

4. The online sector faces a significant problem of an overuse of personal data. This problem is due to the information overload, an enforcement deficit under data protection law and, for interactions with large online platforms, a competition problem.
5. Personal Information Management Systems (PIMS) can contribute significantly toward resolving the problem of a personal data overuse in the online sector. This requires a functioning legal framework that takes in to account the opportunities and risks of a PIMS use in equal measure.
6. The lack of functionality of PIMS is not ascribed to an absence of trust, but rather to an insufficient benefit of their use. To establish this trust, a regulation at system level is needed, i.e. the obligation to take account of PIMS requirements for data processors as well as interoperability requirements. In addition, fine-tuning in the legal framework as well as measures for minimising risks are necessary.
7. These fine-tuning adjustments mainly concern
 - › The possibility of being able to give consent under data protection law for data subjects
 - › The possibility to exercise data protection rights through third parties
 - › Broader consent possibilities vis-à-vis PIMS
 - › Interconnectivity obligations of large online platforms
8. There needs to be a legislative decision on the financing and organisation of PIMS. Should PIMS also be allowed to be offered by private companies, they must be able to operate economically. To avoid false incentives, they should firstly not monetise data but rather the services alone, and secondly should not be paid by the data processors but must be financed by the users. To prevent the use of

PIMS and thus effective data and consumer protection from being income-dependent, thought should be given to subsidy models.

9. The Data Governance Act and Paragraph 26 TTDSG do not take any decisions at a system level, but only serve to minimise the risks of using PIMS. They therefore contribute little to solving the problem.

Data Trustees in the Health Sector

10. In the health sector, however, there is a problem of the under-use of data for research purposes. Firstly, this is due to the difficulty of finding the required data which are distributed in numerous registers, and secondly to uncertainty under data protection law when merging and evaluating large data sets.
11. A triad of a coordinating body, a data donation trustee and flexible data sharing trustees is needed to solve these problems.
12. The coordination body, which ideally is established at both a national level for national research projects and a European level of cross-border research projects, knows which data is in which registers by means of document reference registers and is available to the research as a contact.
13. The data donation options already exist de lege lata via structures of the research data centre and the ePA. These possibilities should be expanded and supplemented with incentives for data donation (e.g. the opportunity to contact the donating patient in case of new research findings).
14. Data stored in the registers often only refers to certain data, e.g. social insurance data or data from certain clinical pictures. Supplementary data trustee structures with the highest security standards are therefore needed in which data can be merged in a legally secure manner for purposes of research in the public interest. These data trustee solutions could be offered both by the state and by the private sector.

15. EHDS could play a key role in solving the problem of a data underuse in the health sector by complementing the horizontal regulations of the DGA-E in a meaningful way.

Data Trustee in the Mobility Sector

16. Data trustee solutions may be a suitable instrument for data access problems related to mobility data. This study focuses on the sharp increase in data generated in connected vehicles by car users in the future, which can be used by many companies and for public interest purposes (road safety, environment etc.). There is a danger that these data are also under-utilised.
17. For several years a large conflict exists about the “extended vehicle” concept of the vehicle manufacturers. This concept enables them to get exclusive control over all these data and over the technical access to the vehicle. Therefore, the vehicle manufacturers can control the access of other service providers to the ecosystem of connected and automated driving, granting them a gatekeeper position. The ensuing serious competition problems on secondary markets (repair, maintenance, navigation services etc.), with negative effects on innovation and the free choice of car owners regarding independent service providers were acknowledged by the EU Commission as a problem that should be solved. However, until today, no proposal has been made.
18. One possible solution for this problem is the establishment of a data trustee which would get exclusive control over these in-vehicle data and which would act as a “neutral” entity for granting access to these data according to the goals and principles of the legislator (for vehicle manufacturers, independent service providers, the data economy, public institutions and research). Through the prevention of the gatekeeper position of the vehicle manufacturers regarding the data, this solution can protect competition, innovation and the free choice of the car owners regarding services. Such a data trustee solution could also lead to a much broader utilisation of these mobility data (data as infrastructure) than in the case of their monopolistic control by the vehicle manufacturers.

19. Alternative solutions for this problem of access to these mobility data:


A strict regulation of access according to FRAND principles to in-vehicle data which are under the control of the vehicle manufacturers. This could be implemented through a further reform of the already existing mandatory access regime to essential repair and maintenance information (RMI) in the current Type Approval Regulation for motor vehicles. It is, however, necessary (as in the data trustee solution) that also a FRAND-regulation is implemented regarding the technical (remote) access to the vehicle for enabling the performance of complementary services (solution of the interoperability problem).

Another more far-reaching solution is the implementation of an alternative technical solution (“on-board application platform”). Through such an open and interoperable telematic platform it is possible that car owners have exclusive control over the in-vehicle data which they are generating with their cars. They can therefore directly give access to these data and access to the car to independent service providers. This would eliminate the vehicle manufacturers’ gatekeeper position.

It is crucial that for all three policy solutions comprehensive security solutions (with certification systems) would have to be implemented.

20. The solution of this gatekeeper problem regarding the in-vehicle data is necessary and urgent. In the medium and long term, the solution of standardised “on-board application platforms” should be implemented. In the short term, a further reform of the Type Approval Regulation for motor vehicles with a strict (and innovation-oriented) FRAND regulation for the access to in-vehicle data and for solving the interoperability problem can be recommended.

- 21.** The so far not much discussed data trustee solution should be assessed as fast as possible regarding its advantages and problems. We think that such a data trustee solution for the data of the connected car can open manifold interesting perspectives – beyond the solution of the competition problems – for an efficient and public interest-oriented use of these vast amount of mobility data in the future.



Data trustees and data intermediaries are important tools of the European data economy that can develop their potential for the benefit of all, only if they are given the legal opportunity to do so. The study shows that the data fiduciary models to be considered in each case must be designed in a model-specific manner. It requires a completely different legal framework in each case in order to be able to contribute to solving the problem.

The study analyses various challenges in three different sectors – healthcare, online and mobility – that can be solved by involving data trustees.