MOBILITY DATA GUARDIAN – ENSURING DIGITAL PRIVACY IN CONNECTED VEHICLES FOR ALL CONSUMERS

Position paper of the Federation of German Consumer Organisations (Verbraucherzentrale Bundesverband e.V. – vzbv) on consumer-friendly and fair access to vehicle data

18. November 2022

Legal information

Verbraucherzentrale
Bundesverband e.V.

Team
Mobility and Travel

Rudi-Dutschke-Straße 17
10969 Berlin

mobilitaet@vzbv.de

CONTENT

I. SUMMARY 3

II. CURRENT SITUATION 4

1. Political framework 5
2. Problem: Factual data sovereignty of the car manufacturers 6
3. Risk: Information overload of the users and often a lack of awareness 7

III. MOBILITY DATA GUARDIAN 7

1. Operation of a Personal Information Management System (PIMS) 9
1.1 Definition and functions 9
1.2 Requirements 9
1.3 Requirements in relation to mobility data 10
1.4 Design 10
1.5 Institutional design, quality assurance and funding 11

IV. LEGAL IMPLEMENTATION 13

1. National legislation 13
2. Sector-specific regulation 13

I. SUMMARY

Fair, consumer-friendly and independent access to vehicle data must be guaranteed so that new, innovative mobility options can emerge for consumers and drive forward the necessary mobility change. At the same time, data sovereignty of consumers must be preserved and supported.

The measures proposed to date neglect these aspects for the digitalisation of mobility. If users do not know to whom their data is flowing and for what purposes, they cannot make an informed – and thus sovereign – decision about whether and under what conditions they wish to share data. Consumers therefore need transparency and control over the whereabouts and use of the data they generate.

For this reason, the Federation of German Consumer Organisations (Verbraucherzentrale Bundesverband e.V. – vzbv) is calling for the establishment of a "**mobility data guardian**" (see III. pages 7 to 12). Going beyond previous proposals, the mobility data guardian would establish rules for all manufacturers that focus on driver control of driving data, as well as transparency concerning why companies need certain information, how long it is stored, and which third parties may access it. In addition to the tasks of a data trustee, the mobility data guardian would specifically perform the function of an authorisation body. This separation of duties between data trustee (access to the vehicle; data forwarding) and mobility data guardian (authorisation) would ensure neutrality when handling mobility data.

The operation of a Personal Information Management System (**PIMS;** see III.1.1 page 9) would help users better instruct, monitor and control data processing operations. A standardised data protection mode would enable consumers to give and withdraw their consent to the processing of their personal data by the manufacturer or to its disclosure to third parties as often as the manufacturer desires. The successful implementation of a PIMS requires, in addition to organisation and financing, the standardised technical prerequisites and, above all, an obligation for data processors to cooperate with the PIMS. The purely voluntary use of a PIMS is likely to lead to failure because of a lack of acceptance, even on the part of those affected by the data sharing. The mobility data guardian would provide consumers with a customised data protection configuration.

vzbv calls on the legislator:

- to counteract de facto data sovereignty by vehicle manufacturers with fair and consumer-friendly access to vehicle data,
- to return organisational and technical data sovereignty over vehicle-generated data to the vehicle users,
- to pursue the establishment of a "mobility data guardian" as set out in this paper in addition to a data trustee model.

II. CURRENT SITUATION

Vehicles are becoming increasingly digitally networked with each other and can communicate with each other and with the traffic infrastructure (for example, traffic lights (traffic signals) or road signs). For example, these vehicles know when a traffic light turns green.[1] Other traffic signs “tell” a vehicle where it is.[2] Cars that inform other vehicles or road users in real time about road conditions, weather, traffic situations and road works, for example, are no longer dreams of the future. Connected driving is safer, more efficient and more comfortable. Intelligent vehicle networking can increase the efficiency of transport systems, prevent accidents and benefit all consumers. The technology can both improve the driving experience and better protect pedestrians and cyclists, for example.

However, there is also a downside to these developments. With the increasing networking, more and more data is being processed (for example, captured, stored and analysed). However, the only way to realise the benefits of the technology is to reduce consumers’ scepticism regarding reliability, data security and data protection. According to a survey commissioned by vzbv, 35 percent of respondents are sceptical of it and do not want to share their mobility data. 23 percent of respondents would share data on the condition of benefitting from the data-sharing themselves. One in three (36 percent) of respondents would even do so if it benefits the general public.[3] Transparency and trustworthiness are the key factors when it comes to digitalisation in vehicles.

The decisive question here is the extent to which users have control over their vehicle's data and can exercise this control. Fair access to vehicle data is a prerequisite for generating innovations and added mobility value. With its concept for a mobility data guardian, vzbv is presenting a consumer-friendly and fair model for data access in the car that makes the claim “my car, my data” a reality. An expert report by Baum Reiter & Collegen Rechtsanwaltsgesellschaft mbH commissioned by vzbv presents the model, the necessity and the legal basis for the introduction of a mobility data guardian in more detail.[4] The statements in this paper largely refer to this expert opinion.

---

[1] Mag, Hans-Joachim: Wenn die Ampel mit dem Auto spricht (When Traffic Lights Talk to Cars), 2020, https://www.dmt-puls.de/news/wenn-die-ampel-mit-dem-auto-spricht/, 17.11.2022; Grundhoff, Stefan: Car-to-X-Kommunikation. Sprecht miteinander (Car-to-X Communication, Talk to Each Other), 2020, https://www.walter-magazin.de/auto/car-to-x-kommunikation-sprecht-miteinander/, 17.11.2022.

[2] Dietze, Carina: Schon entdeckt? Das steckt hinter den schwarz-weißen Schildern auf der Autobahn (Did you know? What’s behind the black and white signs on the highway), 2022, https://efahrer.chip.de/news/schon-entdeckt-das-steckt-hinter-den-schwarz-weissen-schildern-auf-der-autobahn_107861, 17.11.2022.

[3] Verbraucherzentrale Bundesverband e.V.: Intelligente Mobilität: 35 Prozent sehen das Teilen von Daten skeptisch (Intelligent mobility: 35 percent view data-sharing sceptically), 2021, https://www.vzbv.de/publikationen/intelligente-mobilitaet-35-prozent-sehen-das-teilen-von-daten-skeptisch, 15.11.2022; Kantar Public Germany: Verbraucherbefragung zu den Themen Schuhe und Autonomes Fahren (Consumer Survey on Footwear and Autonomous Driving), 2021, page 61,https://www.vzbv.de/sites/default/files/2021-10/vzbv%20%20Schuhe%20und%20Autonomes%20Fahren%20-%20Tabellen%20inkl.%20Methode%20%28003%29.pdf, 17.11.2022.

[4] Reiter, Julius; Methner, Olaf; Schenkel, Bénédict in cooperation with Bönninger, Jürgen: Einführung eines "Mobilitätsdatenwächters" für eine verbrauchergerechte Datennutzung (Introduction of a “mobility data guardian” for consumer-friendly data use), 2022, Düsseldorf, with further references.

1. POLITICAL FRAMEWORK

Consumers will only be able to drive with all-round connectivity if the legislator succeeds in convincingly ensuring trustworthy handling of mobility data via appropriate laws. The German government, in its Coalition Agreement of 2021, has intended a number of important projects to make mobility data more usable.

- "We are creating a mobility data law and ensuring free accessibility to traffic data."[5]
- "We continue to develop the mobility data space."[6]
- "In the autonomous driving bill, we will improve regulations, clarify liability issues and ensure user data sovereignty."[7]
- "We are leveraging the potential of data for all by supporting the development of data infrastructures[8] [...]" **and**
- "To ensure the competitively neutral use of vehicle data, we seek a trustee model that appropriately considers the access needs of users, private providers and government bodies, as well as the interests of affected companies and developers."[9]

The goal is to create a data infrastructure that provides not only vehicle manufacturers with direct access to vehicle-collected mobility data, but also a neutral third party – a data trustee. So far, however, the German government has not taken a concrete position – for example vis-à-vis the European Commission.

For several years, a discussion has been ongoing at the European level about access to data, functions and resources for the development of innovative data-driven mobility services. The European Commission is working to update EU legislation on vehicle type-approval with regard to some technical issues and access to vehicle data, functions and resources, taking into account technical progress.[10] The European Commission has announced a proposal for the second quarter of 2023.

---

[5] Social Democratic Party of Germany (SPD); Alliance 90/The Greens; Free Democratic Party (FDP): Mehr Fortschritt wagen – Bündnis für Freiheit, Gerechtigkeit und Nachhaltigkeit, Koalitionsvertrag 2021-2025 (Daring to Make More Progress – An Alliance for Freedom, Justice and Sustainability, Coalition Agreement 2021–2025), p. 52, https://www.bundesregierung.de/resource/blob/974430/1990812/04221173eef9a6720059cc353d759a2b/2021-12-10-koav2021-data.pdf?download=1, 17.11.2022.

[6] See footnote 5, p. 50.

[7] See footnote 5, p. 52.

[8] See footnote 5, p. 17.

[9] See footnote 5, p. 52.

[10] European Commission initiative: Access to Vehicle Data, Functions, and Resources, Ref. Ares(2022)2302201, 2022, https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13180-Zugang-zu-Fahrzeugdaten-funktionen-und-ressourcen_de,15.11.2022.

2. PROBLEM: FACTUAL DATA SOVEREIGNTY OF THE CAR MANUFACTURERS

The respective vehicle manufacturers currently technically and thus factually control access to mobility data. The access possibilities of the vehicle user(s) and other third parties are limited. If the vehicle has a mobile communications interface, the data is transmitted exclusively to a manufacturer's own server. Third parties are mainly dependent on the vehicle manufacturer for access or are restricted to (limited) data access via the on-board diagnostics (OBD) II interface.

As per the factory settings and due to the lack of interfaces, connected cars do not provide access to the data generated in the vehicle even for the vehicle user (usually a consumer). Besides the lack of an interface, the fact that it is not clear to the average vehicle user which data is generated by the vehicle, stored in the vehicle or transmitted externally, is also a serious factor. There are no direct data access options for the benefit of the vehicle user, i.e. there is currently no possibility to obtain an overview of the processed mobility data by display or even download. In this respect, there is no transparency for consumers, which leads to consequential problems, for example, in the exercise of their own data protection rights. As things stand at present, an expedient and enforceable claim to data access and/or data disclosure in favour of the vehicle user can also only be derived from statutory provisions to a limited extent. [11]

Third parties, such as workshops, insurance companies and roadside assistance services, which rely on the processing of personal data on behalf of the vehicle owner for contract fulfilment, cannot directly access mobility data in the vehicle themselves due to the lack of a suitable interface. Instead they are dependent on the vehicle manufacturer to provide access to the corresponding data. With its NEVADA concept and the ADAXO extension, the German Association of the Automotive Industry (Verband der Automobilindustrie e.V. – VDA) stipulates that the data generated in the vehicle is first transferred to the respective manufacturer's server without exception. Contractual conditions for data access are regulated by each vehicle manufacturer at its own discretion. Vehicle manufacturers decide on the quality (for example, timing of data transfer and data format), quantity (for example, types of vehicle data, individually or only in a package) and price of the data. This limits consumers' freedom of choice, because in the competition for mobility services based on the resource of mobility data, vehicle manufacturers and their associated companies are currently pitted against each other as well as against other service providers. The vehicle manufacturer produces and sells vehicles, and also offers complementary services. Limited data access may act as a barrier to entry for third-party service providers with respect to markets for digital mobility data-based services. This creates the risk of market failure, which is to the detriment of vehicle users and can even lead to a situation where no new, innovative technologies are developed.

> The de facto data sovereignty of car manufacturers restricts the freedom of choice for consumers and prevents competition and innovation.

[11] Artt. 12, 15, 20 GDPR (Regulation (EU) 2016/679 of the European Parliament and of the Council dated 27 April 2016 on the protection of individuals with regard to the processing of personal data, on the free movement of such data and repealing Directive 95/46/EC).

3. RISK: INFORMATION OVERLOAD OF THE USERS AND OFTEN A LACK OF AWARENESS

Another power imbalance between vehicle manufacturer(s) and customer(s) exists in particular because it is virtually impossible for the majority of vehicle users to differentiate between the various data processing purposes or to understand which vehicle functions or digital services depend on which processing operations. The provision of information to the vehicle user is therefore of particular importance. The vehicle manufacturers provide information on the data processing procedures in comprehensive data protection notices. This primarily relies on linking to stored PDF documents, although the documents are sometimes only found deep down within the menu and are around 30 pages long.[12] The various, data-based services are explained in the data protection notices in detail with reference to the data processing operations. Only rarely will a vehicle user actually take note of the extensive data protection information. Many car buyers are probably not even aware that they are acquiring not only a means of transportation with their new vehicle, but also a data storage device.

Besides the wealth of information, the information channel is also challenging for consumers, not least because it must be adapted to whether the vehicle user receives the information in paper form, via the screen in the vehicle (with the respective screen size then also being a factor) or their smartphone. It will be difficult for the information provision system to cope with the flexible and dynamic data processing procedures. Other challenges include the addition of new processing purposes (for which new consent would regularly be required), the revocation of existing consent, and once again the fact that vehicles are used by different persons who may all be data subjects within the meaning of data protection law, but who have not necessarily individually declared their consent to data processing (“dual-use constellations”). Appropriate consent management is required in any case to ensure that personal mobility data is not processed in practice without a legal basis. The question is whether vehicle manufacturers can adequately offer such a system.

> The legislators must prevent information overload of the data subject so that they can exercise their data protection rights appropriately.

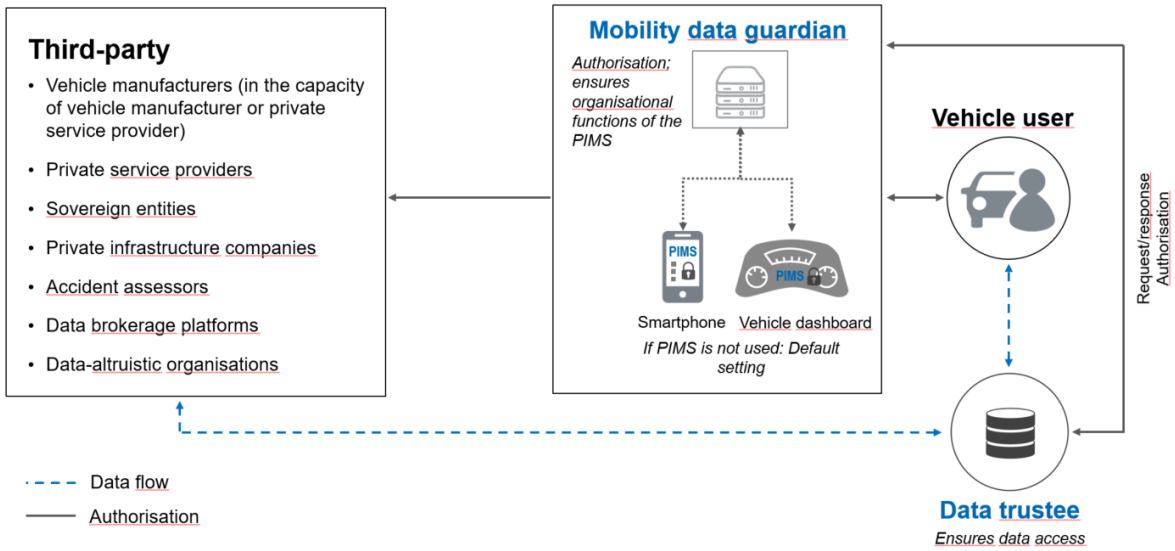
III. MOBILITY DATA GUARDIAN

Regulatory efforts up until now, such as government support for the Mobility Data Space (MDS), have focused on the relationship between different companies and on building mutual trust through regulatory compliance, with the aim of increasing the willingness to share data between companies. The interface to the users is thereby neglected, however. To ensure that consumers do not lose control and transparency over the mobility data they generate, vzbv is proposing the establishment of a “mobility data guardian” (see III.1.5 pages 11 to 12). On the one hand, this guardian is to ensure that mobility data is handled in accordance with data protection requirements and, on the other, to enable fair and non-discriminatory access to mobility data.

[12] Reiter, Julius; Methner, Olaf; Schenkel, Bénédict in cooperation with Bönninger, Jürgen: Einführung eines „Mobilitätsdatenwächters“ für eine verbrauchergerechte Datennutzung (Introduction of a “mobility data guardian” for consumer-friendly data use), 2022, page 20, Düsseldorf.

For illustration purposes, see the following graphic, created in cooperation with our experts (compare footnote 4).

Model: Mobility data guardian



From a consumer perspective, personal data should preferably be stored in the vehicle itself and, as far as possible, processed in the vehicle under the control of the data subjects. A standardised software environment and a hardware platform in the vehicle, i.e. a secure automotive telematics gateway in the vehicle, can be used to run applications provided by third-party suppliers. In addition, if outsourcing of data is necessary, this should be done to independent trustee third parties. As outlined in Chapter II.1, the German government has committed to a “trustee model.”

In order to counteract the vehicle manufacturer’s data sovereignty described above, direct data access should be technically granted to a mobility data trustee in the future. The mobility data trustee receives the data access from the vehicle and can cache it and/or forward it directly to the data recipient (“third party”), depending on the application and need. The information as to whether, to what extent and to whom mobility data may/should be disclosed is not at the disposal of the data trustee, but rather of the mobility data guardian according to the specifications of the vehicle user and the legal grounds for legitimacy. The latter operates a Personal Information Management System (PIMS) for this purpose, in which the vehicle user stores their data processing preferences, gives consent and can transparently track all data processing operations. If a “third party” asks the mobility data trustee to provide certain mobility data, the data trustee asks the mobility data guardian whether the authorised vehicle user has authorised this. If this is the case or if there is another legal ground the guardian issues the release and the data trustee carries out the requested data transfer. Data transmission from the vehicle to third parties is not the only possibility. Information (including updates, for example) can also be transmitted to the vehicle via the mobility data trustee in the opposite direction – provided authorisation or legal basis exists here as well.

The mobility data guardian does not have physical access to the data at any time. Only the data trustee has access to this, but the data trustee does not decide on the type or scope of data forwarding. The separation of duties between the data trustee (access to the vehicle, data forwarding) and the mobility data guardian (authorisation) ensures neutrality in the handling of mobility data and prevents conflicts of interest.

1. OPERATION OF A PERSONAL INFORMATION MANAGEMENT SYSTEM (PIMS)

1.1 Definition and functions

PIMS are technical tools designed to help users better instruct, monitor and control data processing. A PIMS is not a ready-made or rigid system. Rather, numerous functions are conceivable, the implementation of which depends on the specific application. In the future, a PIMS could also be used to assert the new access rights expected to accompany the Data Act.

Core functionalities of PIMS are the consistent observance and enforcement of data protection law, the integration of consent management, and the guarantee of transparency and traceability of all data processing operations (where applicable, with regard to personal as well as non-personal data).[13] By enabling users of a PIMS to track and control their digital activities, illicit data processing is simultaneously prevented. Consumers should also be given an overview of consents that have already been given or revoked. This would increase the confidence of individuals in the use of digital networked systems. Trust is a prerequisite that is also fundamental to the further development of connected vehicle ecosystems and mobility platforms. Beyond the basic functions, identity management, i.e. the identification of the user with various online services, and the evaluation and a possibly monetisation of non-personal data are additional PIMS functions. However, data management, i.e. a possibly more personal data store, the merging of different data sources and data conversion would tend to be more the tasks of the data trustee (see also graphic).

1.2 Requirements

The successful implementation of a PIMS requires above all an obligation for data processors to cooperate with the PIMs, in addition to organisation and financing and standardised technical requirements[14]. The former point leads to a legal obligation for all data-processing entities to enable e.g. data subjects to make the desired data arrangements (consent management), to obtain information on data protection law, to track all processing operations, and to exercise other data protection rights via the

[13] Cf. also Krämer, Jan: Digital Self-Determination through Personal Information Management Systems? (Digitale Selbstbestimmung durch Personal Information Management Systems?), 2022, p. 4 f., https://www.verbraucherforschung.nrw/sites/default/files/2022-02/zth-4-kraemer-digitale-selbstbestimmung-durch-personal-information-management-systems.pdf, 15.11.2022; statement by Verbraucherzentrale Bundesverband e.V.: New Data Intermediaries – vzbv Requirements for Personal Information Management Systems (PIMS) and Data Trustees, (Neue Datenintermediäre – Anforderungen des vzbv an Personal Information Management Systeme (PIMS) und Datentreuhänder) 2020, p. 6, https://www.vzbv.de/publikationen/datenintermediaere-gesetzlich-regeln, 15.11.2022.

[14] Specht-Riemenschneider, Louisa; Kerber, Wolfgang, Designing Data Trustees – A Purpose-Based Approach (Datentreuhänder – Ein problemlösungsorientierter Ansatz), 2022, p. 34, Berlin, Konrad-Adenauer-Stiftung e. V.

PIMS.[15] The data processor should subsequently be prohibited from interacting with the person concerned outside the PIMS.[16]

Voluntary use of a PIMS by third parties and vehicle manufacturers, on the other hand, is very likely to fail due to a lack of acceptance, including on the part of those affected by the data sharing. Data arrangements, privacy information and processing operations would still not be accessible in a centralised manner even with partial use of the PIMS. The interest of users to use the PIMS (as one more system among many) would be lost.

1.3 Requirements in relation to mobility data

The mobility data guardian model is about the implementation of a PIMS that should be developed and used specifically for the processing of mobility data rather than in a general way. In line with this, suitable, sector-specific minimum PIMS functionalities should be selected. In view of the data protection challenges posed by the processing of mobility data and taking into account the assigned tasks of the “data trustee,” the following PIMS functions should be considered first.

- Effective and user-friendly consent management that includes non-personal data. Admittedly, this no longer concerns the data protection level. However, when designing and implementing a PIMS within the specific context of “mobility data”, care should be taken at the same time to ensure that the vehicle user, often also the owner of the vehicle, is given complete data sovereignty over the data generated in their vehicle.
- The transparent and comprehensible presentation of all processing operations that take place in the PIMS by means of comprehensible data protection information, adapted to the means of communication (smartphone, vehicle display, and so on) and which data protection rights can be enforced (in particular the right to information, rectification, deletion and data portability) and how. Existing discrepancies between consents given through consent management and actual processing operations that are supposed to be based on consent would become visible (in an automated way).

1.4 Design

In addition to the appropriate PIMS functions, a user-friendly user interface is crucial to the success of the mobility data guardian system. A structured menu, self-explanatory (or briefly explained) toolbars, buttons, switches and sliders or other selection lists should enable the user to easily adjust their preferred settings or retrieve the information they are looking for. The interface should be designed neutrally to prevent the system’s use from being influenced by the interests of a data-processing agency. Operation of the PIMS should be possible from different places, but first and foremost

[15] Federal Government Data Ethics Committee: Expert Opinion of the Data Ethics Commission, 2019, p. 134, https://www.bundesregierung.de/breg-de/service/publikationen/gutachten-der-datenethikkommission-langfassung-1685238, 15/11/2022.
[16] See footnote 14, there p. 33.

inside the vehicle itself via the vehicle display (“data cockpit”). At the same time, however, computer and smartphone operation should also be possible. In the context of extended functionality, operation via a smartphone app would have the advantage that the settings stored on a smartphone can be transferred to any (compatible) connected car.[17] The vehicle, which is new to the user, can then connect to the smartphone, and the PIMS settings are taken into account. This would also be a way of addressing the problem that a vehicle can be used by different persons affected by data protection law (i.e. the driver, passenger, holder, buyer and owner).

1.5 Institutional design, quality assurance and funding

The specific tasks of the mobility data guardian are not yet performed in their entirety by any specific body. With a view to the institutional design, quality assurance and financing of the mobility data guardian model, the question therefore arises as to which existing or newly created organisations could or should take on the tasks described. Companies from the private sector should be considered first. Alternatively, the state could take on these tasks. In making this selection, it is important to keep in mind that the implementation of the mobility data guardian model involves the state taking regulatory action – on the one hand against the failure of mobility data-based markets, and on the other for the consistent observance and enforcement of data protection law. In compliance with the principle of market freedom, the state intervenes to prevent market failures only to the extent necessary, as long as the markets otherwise regulate themselves. Above all, the state must observe the principle of proportionality in its regulatory activities. If existing regulatory law is insufficient to achieve the intended goals, the state will only make improvements to the extent that this is absolutely necessary and appropriate.

The mobility data guardian acts as an authorisation body vis-à-vis the mobility data trustee. This task requires, above all, the establishment of interfaces so that mobility data guardians and data trustees can communicate with each other. However, the main focus of the mobility data guardian is on operating a PIMS, the setup and operation of which, compared to the authorisation process, is a much more extensive task. The selection of a suitable institution to perform the tasks of the mobility data guardian must therefore be based on who is suited to setting up and operating a PIMS.

Both private companies and government agencies can be considered for performing the tasks of the mobility data guardian. The argument in favour of a private company is that government intervention is less intensive and limited to the mandatory involvement of a mobility data guardian. In addition, private companies are are ideally suited for making investment decisions and have the potential to innovate in complex data economy markets. However, the future viability of financing is a compelling reason against the assignment of tasks to a private company, which could also economically collide with the need to avoid conflicts of interest. Even though PIMS have been considered a suitable means of implementing data protection law for several years, a

[17] Federation of German Consumer Organisations: Transporting everyone driver-free – Automated and Connected Mobility from a Consumer Perspective (Verbraucherzentrale Bundesverband e.V.Fahrerlos alle mitnehmen – Automatisierte und vernetzte Mobilität aus Verbrauchersicht), 2021, p. 15, https://www.vzbv.de/pressemitteilungen/gesetz-zum-autonomen-fahren-muss-alle-mitnehmen, 15.11.2022.

commercially viable business model has yet to establish itself.[18] For now, it is only the vehicle manufacturers and third parties that would need to upstream the special mobility data-based PIMS. Vehicle users are not expected to be willing to pay a fee for the use of a PIMS. Due to the relatively small number of vehicle manufacturers and third parties, financing from them is virtually inconceivable due to lack of scalability. If a "data trustee" subsequently requests authorisation from the "mobility data guardian", a fee could be charged to the third party for this process. The potential frequency of authorisation requests would probably also allow for scaling. Until this happens, however, a significant amount of upfront financing would be required, which could deter private investors. Although the financing problem could be countered by government subsidisation of already recognised or certified PIMS of private operators,[19] it should be noted that private companies generally have no interest in neutrality and instead pursue economic self-interest, whereas the state can perform tasks without any profit motive. However, a neutral attitude towards vehicle users, vehicle manufacturers and other third parties should be a fundamental characteristic of the mobility data guardian. In particular, neutrality is intended to prevent users of the PIMS from making decisions that are unconsciously determined by others ("dark patterns"). The PIMS must be a tool that exclusively supports self-determined decision-making authority.[20] This is usually not guaranteed in the case of companies that pursue economic self-interest.

Alternatively, in the case of the mobility data guardian, it would be possible to establish a company owned by the federal government. This body could perform the tasks of a mobility data guardian. Due to the operation of a PIMS and the focus on data protection law, the legal and technical supervision of the mobility data guardian could be assigned to the Federal Commissioner for Data Protection and Information Security (BfDI) after a corresponding amendment to the law on jurisdiction.[21] The foundation of a state mobility data guardian would not preclude private companies from establishing a corresponding body in parallel. Multiple mobility data guardians could operate side by side in a competitive manner, which would have the advantage of allowing consumers to decide which guardian they want to work with. However, the licensing and operation of additional mobility data watchdogs should be subject to appropriate certification and oversight to ensure compliance with quality and neutrality standards.[22]

---

[18] Cf. also Krämer, Jan: Digital Self-Determination through Personal Information Management Systems? (Digitale Selbstbestimmung durch Personal Information Management Systems?), 2022, p. 16, https://www.verbraucherforschung.nrw/sites/default/files/2022-02/zth-4-kraemer-digitale-selbstbestimmung-durch-personal-information-management-systems.pdf, 15.11.2022.

[19] Specht-Riemenschneider, Louisa; Kerber, Wolfgang, Designing Data Trustees – A Purpose-Based Approach (Datentreuhänder – Ein problemlösungsorientierter Ansatz), 2022, p. 41, Berlin, Konrad-Adenauer-Stiftung e.V.

[20] Federal Government Data Ethics Committee: Expert Opinion of the Data Ethics Commission", 2019, p. 133, https://www.bundesregierung.de/breg-de/service/publikationen/gutachten-der-datenethikkommission-langfassung-1685238, 15/11/2022.

[21] Entsprechende Tendenz:
Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI):
Vernetzte Fahrzeuge – Datenschutz im Auto (Corresponding trend: Federal Commissioner for Data Protection and Freedom of Information (BfDI): Connected Vehicles – Data Protection in Cars), 2020, p. 19, https://www.bfdi.bund.de/SharedDocs/Downloads/DE/Flyer/VernetzteFahrzeuge.html, 15.11.2022.

[22] See footnote 20.

IV. LEGAL IMPLEMENTATION

1. NATIONAL LEGISLATION

If the European legislature does not advance regulations along the lines of the mobility data guardian model presented here, the German legislature can and should take action at the national level and lead the way. In doing so, it must pay attention to the protection of mobility data and their processing. The “Mobility Data Act” announced by the German government for 2024 is a suitable vehicle for regulation. The focus in this act would lie on the following regulatory areas.

- The definition of the mobility data guardian and its tasks
- An obligation for data processors (data controllers within the meaning of the GDPR) to cooperate with the mobility data guardian (specifically with the PIMS)
- Interoperability in collaboration between (different) “mobility data guardian(s)” and “data trustee(s)”.
- A certification and monitoring system in the event of the establishment of further “mobility data guardians”
- Financially support private-sector mobility data guardians or establish an entrusted entity charged with establishing and running a mobility data guardian.

2. SECTOR-SPECIFIC REGULATION

In addition to the planned regulatory framework of the Data Act, sector-specific regulation for access to mobility data at the European level is also possible. Currently, the European legislator plans to address this issue in sector-specific regulation by amending the Type Approval Regulation.[23] Whether alongside such European regulation other or more far-reaching data access options can be prescribed by national legislation depends on whether and to what extent the European legislator will undertake full harmonisation with the amendment of the Type Approval Regulation. In the European legislative process for sector-specific regulation, the German government should work to ensure that the introduction of a PIMS and Mobility Data Guardian concept are also regulated there. If its efforts are unsuccessful, a national regulation could still be considered with regard to the introduction of a PIMS.

[23] REGULATION (EU) 2018/858 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL, 2018, https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=celex%3A32018R0858, 15.11.2022; see also footnote 10.