bitkom

Position Paper

Public Consultation on the Access to Vehicle Data, Functions and Resources

August 2022

General Remarks

Nathalie Teer
Policy Officer Mobility & Logistics

T +49 30 27576-250
n.teer@bitkom.org

Nils Heller
Policy Officer Mobility

T +49 30 27576-251
n.heller@bitkom.org

Albrechtstraße 10
10117 Berlin

With its initiative on the access to vehicle data, functions and resources, the European Commission is addressing an issue that has been under discussion for quite a while.

In general, Bitkom welcomes the intention to facilitate the use of data for a smarter, safer, and sustainable mobility ecosystem. Bitkom recognizes the potential benefits of data sharing not only for the mobility sector, but for the entire digital economy. In our view, third parties should be given equal access to data, resources, and functions wherever it is appropriate, secure, and facilitates the emergence of innovative services under fair, reasonable, and non-discriminatory (FRAND) conditions. Above all, data privacy and cyber security must, however, be ensured at all times. Nonetheless, they should not be misused as a pretext for restrictive measures. With this initiative, the Commission considers complementing the Data Act with more specific provisions for the automotive sector. On that note, we would like to point at Bitkom's overarching concerns on the Data Act, including but not limited to mandatory data sharing with other businesses, essentially extending transparency obligations to B2B settings, as well as unequal treatment of market participants. These concerns (details on Bitkom's Data Act position are available here) remain valid for any sector-specific regulation as well.

In the light of Bitkom's broad spectrum of members from different industries, we would like to contribute to this ongoing policy debate with the goal of reaching a satisfactory legislative framework for all parties involved. Overall, Bitkom underlines that relying on market principles will be key for fostering the enormous potential of data-driven solutions in the field of mobility. Thus, Bitkom advocates for a careful approach to legislative action on access to vehicle data, functions and resources. As we explain in greater detail below, we generally support assuring fair, reasonable, non-discriminatory access and transparency around data. However, given that functions and resources are significantly different from accessing data, we urge the Commission to develop a differentiated regulatory approach and carefully consider whether the access to data, functions and resources can and should be regulated in one initiative. Wherever

45%

of German companies wish for more political support for data spaces (Bitkom study, May 2022)

legislative initiatives are taken, they should aim at fostering data markets and leveraging the potential of scalable, non-discriminatory data spaces. In particular, potential dependencies to the Data Governance Act (i.e. data intermediation services) should be clarified from the early beginning. Safety and security concerns should be addressed, and the risks mitigated.

Specific Comments

Status quo and justification for the Commission's proposed initiative

There are currently various legislative frameworks defining terms of reference for the access to vehicle data. To provide some examples, this includes Regulation (EC) 2007/715, amended through Regulation (EU) 2018/858 for repair and maintenance, Directive (EU) 2014/45 and its Implementing Regulation (EU) 2019/621 for sovereign tasks or UN Regulations 155/156 on cyber security. On that note, however, it must be underlined that the absence of one generic regulation on a specific issue does not in itself provide grounds for legislative action. Rather, any initiative must carefully look at the status quo and only address areas where there is clear evidence for a market failure.

Innovation in the automotive sector goes – partially - along with opening opportunities for data-driven use cases that bear the potential to make mobility safer, easier and more sustainable. Many such use cases depend on efficient access to in-vehicle data and resources. This applies, for example, to the insurance industry. Insurers would, e.g., like to incentivise safer driving through usage-based insurance, launch advanced breakdown services, improve stolen-vehicle recovery or better understand accident circumstances. There are already some use cases, e.g. related to "pay as you drive" solutions, actively enabled by OEMs. However, such solutions are fragmented and partially lack the uniformity across vehicle brands and models that would be needed for scalable insurance solutions. As another example, transport and logistics operators could use, for example, in-vehicle GPS and consumption data to optimise efficiency and in doing so reduce emissions. Increased access to vehicle data could support vehicle operators (SME's as well as global players) in collecting, evaluating and exchanging more exact data with value chain partners and customers, for example in the context of the EU Taxonomy or upcoming data exchange standards like the ISO 14083:2022 (the standard describes the quantification and reporting of greenhouse gas emissions arising from transport chain operations).

At the same time, it should be noted that data generated by vehicles is typically not a direct by-product generated as a collateral event, but (for instance on sensor data) the result of sizeable monetary investments and the basis of new business models needed for the development of new use-cases such as automated driving services. On that note, it is important to clarify that data generated in vehicles primarily serves functional

purposes. While the costs associated with the provision/development of data accesses or operation need to be considered, however, pricing must always be fair.

Besides above-mentioned regulations on access to vehicle repair and maintenance information and on-board diagnostic (OBD) systems, vehicle manufacturers currently allow for third parties to access data primarily through a so-called Extended Vehicle concept (ExVe concept). To date, however, there are still aspects of this concept that require improvements when viewed from the perspective of certain third-party actors and users. While there is a trend towards harmonising certain data sets, there is currently no uniformity across vehicle brands, which complicates data-driven business models and increases the costs of using and exchanging data. Furthermore, there is no transparency across vehicle brands in terms of what data points are made available by OEMs. In order to improve this existing concept and allow for a strategically meaningful expansion of the data offering across sectors, we recommend establishing a forum in which all relevant stakeholders can exchange their positions and balance their interests. As we discuss further below, such a forum would be particularly helpful for identifying a minimum list of data to be made available.

The interplay between Data Act and sector-specific regulation

The Data Act already lays the foundation for providing users access to vehicle data as well as the right to share this data with third parties. Despite our general concerns on the Data Act, we welcome the Data Act's intention of increasing the breadth and depth of data usage and innovation within the European Single Market. However, the Commission has noted that the Data Act provisions may not go into sufficient details of access to functions and resources in the automotive sector. Furthermore, the current logic of the Data Act does not reflect the industrial reality since, for example, the role of automotive suppliers is not considered. In view of the sector's specificities, e.g. related to questions of safety and security, Bitkom acknowledges that a targeted sector-specific regulation might be needed to complement horizontal legislation. We urge the Commission and all legislative stakeholders, however, to keep in mind that such sector specific regulation needs to fit into the overarching framework and should not create new barriers for the interchange of data and information, the use of (inter-sectoral) data spaces and the growth of the EU data economy more broadly. Having in mind these principles, we recognise that where there are opportunities to enhance new use cases and mobility through data access – e.g. by making transport more efficient, safe and sustainable – these need to be explored. Equally, however, Bitkom opposes unrestrained access to data by governments, other businesses or the general public without appropriate safeguards that take into account existing sector-specific rules and requirements as well as general principles such as the protection of intellectual property rights. This is a key area for the Commission to address given the current breadth and vagueness of key terms such as "data holder" contained in the Data Act and "resources and functions" contained in the proposed initiative discussed here. To avoid potential asymmetries between the Data Act and corresponding sector-specific regulation, the latter must be built upon existing rules. Beginning to define sector-specific rules prior to concluding the to be based upon regulation is essentially contradicting the better regulation principle and ultimately might result in gradual uncertainties, thus costs for all involved parties.

Policy option 2 – an option with potential but several open questions

In order to balance the various interests arising through increasingly connected vehicles, Bitkom sees potential in a balanced and carefully drafted initiative based on option 2. We generally appreciate the benefits of making available a minimum set of data in addition to the proposal of option 1 to assure equal, non-discriminatory access and transparency. However, we question the inclusion of functions and resources as we explain in greater detail below. Overall, a standardisation of in-vehicle data could facilitate their use by various actors of the ecosystem and foster innovation in services building on such data. This would streamline data sharing and facilitate the activities necessary for their proper use.

However, when pursuing option 2, there are several concerns that require further attention. As a general word of caution, it needs to be highlighted that option 2 not only suggests assuring equal, non-discriminatory access and transparency relating to data but also to functions and resources. Whereas the availability of a minimum list of data appears to be part of the latest positioning papers of both OEMs and third parties, the approach to extend this explicitly to functions and resources must be done with utmost consideration of negative consequences for the vehicle's integrity – thus safety and security. Today's vehicles typically include more than 100 control units, sensors, and actuators. The data is transferred between these via an internal controller network. All software deployed in the vehicle is – secured by deployment through the ExVe – tested and verified. In case of unknown run code, any malfunctioning might lead to a malfunctioning network. Thus, no actuation is triggered although the sensor would require (after processing) an immediate action with severe consequences for the user's safety. Hence, access could be granted only with strict rules and processes, which are necessary to ensure adequate safety and security for the vehicle. Bitkom urges the Commission to carefully consider whether, given their different characteristics, the access to data, functions and resources can and should be regulated in one initiative.

To ensure that service providers can offer services to their customers across different brands and models, stakeholders require that common sets of data are established that would be made available to third parties. Details of such data sets should be drafted by the industry to reflect the needs of the market and be discussed with relevant access seekers in a structured format. Here, standardisation can be helpful to spell out the envisaged common particular format, identification and further qualifying attributes. In order to accelerate the standardisation process, an open standard could be co-developed by industry players for various domains with the ultimate goal to address the need for emerging use cases evolving over time. Generally, careful consideration is needed when identifying the items on the minimum list of data. It must be outlined for what reason a specific type of data is to be made available - if it is not already available through a data space already in use. As a basic hypothesis, it should be emphasized that the current data basis will fundamentally and constantly expand and continue to develop due to new vehicle generations. The fast-moving development of data topics and volatile demands for data availability speaks against a static dataset stipulated by law. Instead, this list should not be regarded as static but rather be updated according to technical developments, market needs and other factors of relevance to data-driven business models. We suggest establishing a direct exchange between all relevant data

users and OEMs on requested and demanded data. Within such a forum, concrete demand of third parties on (new) data (points) can be discussed and solutions be found. In this way, required data can be made accessible to third parties while ensuring the generation of new data points according to FRAND conditions. To maintain the essential neutrality of the forum, the Commission could play a leading role, for example as the organiser and moderator.

Moreover, the question of data privacy requires further attention, as option 2 may increase the processing of personal data. In addition to the bilateral commercial agreements between consumers and manufacturers (e.g. automotive OEMs), any data sharing extends the original scope of this agreement out of the control of the original data processor. This can be mitigated by a consistent definition of necessary anonymization and pseudonymization measures for the shared data. A consistent consent management either by the OEM or through a third party can also mitigate this risk. This could apply, for example, when a workshop requires data for a specific vehicle and receives the agreement from the vehicle owner. It needs to be pointed out, too, that some use-cases, particularly in the insurance industry, will require non-anonymized data. Generally, safeguards must be in place to give consumers, i.e. the owners or drivers of a vehicle, transparent insights into how their data is accessed as well as options to limit this access. Furthermore, it is not always clear how to ensure that every affected user of a vehicles gives valid consent to the processing of their data in settings with multiple users on a single account/device. We would also like to mention uncertainties in the Data Act relating to persons who own/rent/lease/drive/use/... a smart object and which rights they are entitled to.

Regarding the proposed access to the on-board diagnostics port, we believe that this might remain an important interface for the repair and maintenance of vehicles. Enabling access would be one way to preserve the availability of vehicle generated data to the extent necessary for vehicle repair and maintenance (as specified under 2018/858). Furthermore, there is a need for clarifying both why and how the “continuous and secure access to the on-board diagnostic port” should be facilitated. These questions are particularly pressing when viewed in light of safety and security concerns. In order to comply with the requirements of UNECE regulation R155 on cybersecurity, vehicle manufacturers must implement all necessary measures to protect their vehicles. As we already outlined above, these measures should, however, not be unreasonably restrictive especially in light of repair and maintenance purposes. We believe that complying with cyber security requirements while allowing authorised access to OBD for the purpose of repair and maintenance is possible. However, concrete solutions for this issue are yet to be agreed on by all relevant industry players.

Finally, if the Commission decides to initiate a legislative proposal, and regardless of the option chosen, the legislation must aim for a clear split of responsibilities with regard to homologation (of software) and liability. For example, if access to body control functions is given, there should be defined interface up to which soft- and hardware is relevant to homologation for which the OEM is responsible. Generally, challenges arise when it comes to the liability for software. These challenges deserve further scrutiny.

Cybersecurity

When considering the implementation of option 2, particularly relating to functions and resources, questions as to how safety and right functional performance of the vehicle can be ensured arise: in a system in which multiple entities can have direct write access to the vehicle and its functionalities but no entity is responsible to ensure the integrity of the system, compliance with UN Regulation 155 on cybersecurity would be very challenging.

Direct illegitimate access can produce numerous safety risks, e.g.:

- loss of control over the vehicle by the driver, which may be caused by services directly or indirectly influencing the vehicle's movements and systems;
- unauthorized access to the vehicle's data and systems (e.g., hacking) which creates critical safety issues;
- with respect to the vehicle's fundamental functionalities (e.g. braking, steering, guidance);
- overload of the vehicle's communications network with messages from applications, which could impede or prevent other critical safety messages from being processed correctly.

In consequence, a potential legislation must not only be consistent with existing rules, but also restrict access rights in such way as to safeguard security and safety relevant functions and resources. There must not be a trade-off between access rights and security and safety compliance. Concepts taking this principle into account should be developed in greater detail by relevant industry stakeholders.

Ultimately, we would like to underline that this position paper merely marks the beginning of a debate but does not consider itself as providing an exhaustive account on the Commission's proposed initiative. When it comes to pursuing and implementing any sector specific regulation, several questions remain to be answered, e.g. how would "remote access" be designed? Who would manage the access? Have other policy options been considered? We look forward to continuing the discussion on these and related questions as the initiative progresses.