AD/BR8516/SMR Brussels, 17 October 2022

IRU Position Paper on Access to Vehicle Data, Functions and Resources

IRU Position Paper on Access to Vehicle Data, Functions and Resources

I. IRU POSITION

To improve the access and reuse of in-vehicle data for commercial purposes, the European Commission intends to propose a sector-specific legislation on access to vehicle data, functions and resources, in line with the principles established in the horizontal legislative proposal addressing data access and use, the Data Act.

IRU has consistently highlighted over the years that data flows must be regulated, specifically in business-to-business (B2B) contexts, in order to enhance trust among stakeholders, a prerequisite for data sharing. Representing the interests of commercial road transport operators, IRU welcomed the proposal for the Data Act as a horizontal piece of legislation that addresses, for the very first time, transport operators' right to access and share data generated by the use of connected vehicles and related services with third parties of their choice.

While the Data Act aims to provide a competitive, safe and secure foundation for future data-sharing practices and promotes trust among business partners, the specificities of the challenges in terms of technical, as well as safety, security and privacy requirements for access to in-vehicle data require a sector-specific approach.

As the European Commission is in the process of developing a legislative proposal on access to in-vehicle data and resources, the following **recommendations of IRU for sector-specific legislation on access to in-vehicle data must be taken into consideration:**

- The User's choice over third-party access to in-vehicle data should always be preserved, with such access requiring either an **existing contractual relationship** with the User for the provision of services or an **explicit consent from the User, i.e. that is freely given, specific for the purpose, informed and unambiguous.** For the purpose of the position paper, the term `User` refers to a data generator or a commercial transport operator.
- A carefully developed end-to-end **consent management system must be established**, as well as an opt-out system that is simple to understand and user-friendly.
- **Data types** that are made available (e.g. raw data, metadata and processed data) must be defined. For instance, processed data is of incredible value and should be made available to Users by manufacturers or providers of related services, with Users having the right to further share it with third parties of their choice.
- Rules should address specific **safety, (cyber)security, and privacy aspects**, for both drivers and operators, especially when it relates to potential on-board access to in-vehicle data.

- **Enforcement** of the sector-specific legislation must be based primarily on the text of the legislation, and not on enforcement powers of a 'control authority'.
- Sector-specific legislation should **not provide an additional legal basis for governmental access to data (B2G)**; rather, it should preserve the exceptional nature of public authorities' access to data, as envisioned in the Data Act.

II. ANALYSIS

Modern, connected vehicles, such as taxis, buses, coaches and goods vehicles, generate a large amount of data during their operations. The trend to collect, store, share and use/re-use the data generated, especially by businesses, will continue at an increasing pace with the development of autonomous vehicles, the internet of things (IoT), machine learning (ML) and artificial intelligence (AI). Data generation is coming from built-in on-board-diagnostics (OBD) and fleet management systems that collect information, such as tyre pressure, vehicle speed, mileage, fuel consumption, oil level, engine status, battery charge status, and much more.

According to the European Commission, modern vehicles generate around 25 gigabytes of data every hour[1]. The algorithms running the operations in autonomous vehicles will be trained to use data that the vehicle will gather about their surroundings. Such data has become a valuable resource for companies that use it to provide cutting-edge services other than repair and maintenance, such as usage-based insurance, predictive maintenance, route planning, smart parking information, or pay-as-you-go services.

However, while Users generate data that is becoming essential to business operations, access to in-vehicle data is often controlled by the manufacturer and/or a fleet company. Commercial road transport operators, as the Users of the vehicles, lack control over commercially sensitive data created during vehicle operations and lack visibility as to who receives that data. Furthermore, OEMs or fleet companies, as data holders, frequently use or distribute the data with third parties without the Users' explicit consent.

IRU welcomed the Data Act, which aims to provide a competitive, safe and secure foundation for future data-sharing practices and promotes trust among business partners. However, the specificities of the challenges in terms of technical, as well as safety, (cyber)security and privacy requirements for access to in-vehicle data, necessitate a sector-specific approach.

IRU contends that it is not acceptable to provide excessive access to in-vehicle data to parties without the User's explicit consent, i.e. that is freely given, specific for the purpose, informed and unambiguous, as it poses (cyber)security risks at the expense of the User for which neither the manufacturer nor fleet manager will bear responsibility. Taking this into consideration, **IRU has developed several key recommendations** regarding the sector-specific legislation on access to vehicle data:

1. User's choice over third-party access to data

User's choice over third-party access to in-vehicle data should be preserved in the sector-specific legislation, with third-party access requiring either a contractual relationship with the User (e.g. service providers hired by the User to perform repairs and maintenance) or User's explicit consent, i.e. that is freely given, specific for the purpose, informed and unambiguous. The User should be able to explicitly give permission to third parties to access vehicle data if there is no contractual relationship between the User and the third party. Data holders and/or third parties should provide the User with all relevant information regarding the processing and use of data generated by the User. Both the data holder and the third party will be responsible for providing such information to the User in a clear, concise and transparent manner.

[1] European Commission (2020), *A European Strategy for Data*, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0066&from=EN, Accessed: 07/09/2022

Unrestricted access to vehicle data by all parties (e.g. independent service provider, public authorities) without the consent of the User, would pose unacceptable risks to safety and the (cyber)security of the vehicle, as well as liability issues when such access is enabled via the vehicle's human-machine interface (HMI).

IRU calls for:

a) Sector-specific legislation to distinguish between two possible scenarios:

   (1) The third party has a contractual relationship with the User, whereby the User contracts the third party to conduct specific services, and whereby the consent to access vehicle data, functions and/or resources is a part of the contractual agreement between the third party and the User; and

   (2) The third party does not have a contractual relationship with the User, in which case consent must be requested from the User prior to any data being shared with a third party.

   The main purpose of this feature is to enable the provision of services that do not have to depend on the manufacturer's systems, such as route optimising, improved training of new drivers, or repair and maintenance services, based on the will and consent of the User, while at the same time protecting the User from unauthorised access to vehicle data.

b) In cases where there is no contractual relationship between the User and the third party, the User should provide an explicit consent, i.e. that is freely given, specific for the purpose, informed and unambiguous to third-party data sharing. For consent to be 'informed', the User must be informed of the third party's identity, what kind of data will be shared and processed, by whom, for how long, for which purpose, and whether the third party intends to further share the data with other third parties.

c) An obligation to establish an end-to-end consent management system, as well as an opt-out system, which should be simple to understand and user-friendly; and should be provided by the manufacturer without acting as a gatekeeper. Consent should be as easy to revoke as it is to grant.

d) The consent management system can be designed to allow consent giving and revocation via a user interface or Human-Machine Interface (HMI). Firstly, consent would be given by fleet manager(s), followed by the driver's consent for any additional requests. Fleet managers and drivers will both need training regarding the rights and obligations under the future sector-specific legislation as well as the GDPR regarding the protection of personal data, and the protection of commercial interests of the User when authorising third-party data access. It would be necessary for the commercial transport operators as Users to receive further financial incentives to organise and accomplish such training.

e) As a general principle, information for Users should be provided in a concise, transparent, understandable, and easily available form regarding data that is being processed, by whom, for how long, and for what purpose. Transparency is a prerequisite to obtain a valid consent from Users.

2. Access to data in business-to-business context (B2B)

All data holders should make their data available to Users, as well as to third parties upon Users' request. With the increased use of related services in vehicles, access to data gathered using such services installed in the vehicle would be critical for the provision of aftermarket services.

IRU calls for:

a) Defining the data types that can be made available (e.g. raw data, metadata and processed data). Processed data is of incredible value to Users and should be made available to them by manufacturers or providers of related services, with Users having the right to further share it with third parties.

b) Recognising the right of Users to seek compensation in case of data holders' inappropriate sharing of data with third parties.

c) Limiting the use or re-use of data collected by manufacturers or third parties beyond the reason for which the access was granted or shared without the User's explicit consent, i.e. that was not freely given, not specific for the purpose, not informed adequately and ambiguous.

3. Safety of vehicles and (cyber)security of Users

The safety and security of users, both commercial transport operators and drivers, should always come first, when addressing specific safety, (cyber)security, and privacy aspects, especially when it relates to potential on-board access to vehicle data. IRU recognises that vehicles generate a large amount of data that is not standardised and is formatted differently depending on the manufacturer. As a result, neither the User, the manufacturer, nor third parties can make the best use of the data. Therefore, interoperability and standardisation are necessary to achieve the provision of services by a third party of the user's choice.

IRU calls for:

a) Means of access to be standardised, and adequate safeguards to be put in place to protect Users from potential safety and cybersecurity risks. Any access to in-vehicle data should not jeopardise or expose Users to privacy and cybersecurity threats.

b) Clarity regarding the possible means of access, especially when it becomes increasingly clear that it would be upon the manufacturer (or provider of related services) to enable access either through on-board data storage or from a remote server.

c) Should the legislator choose any or several means of access, the right of access needs to be regulated as per the strictest security and safety legal requirements, with clearly defined and specified liability provisions to address the risks, should the third party gain access to vehicle data via the on-board access.

d) Certain service providers who perform such services as to necessitate on-board access to the vehicle should receive the User's permission that is freely given and specific for the purpose. In any case, the service provider should demonstrate the highest cybersecurity standards.

e) The portability measures should be kept in the sector-specific legislation, with the User being able to switch between different service providers of their choice without incurring excessive costs and being exposed to higher risks.

f) The enforcement of future sector-specific legislation must be based primarily on the text of the legislation, and not on enforcement powers of a 'control authority' which would be comprised of industry representatives. It is the experience of the road transport industry that enforcement conducted by 'control authorities', even when such authorities are comprised of police and enforcement bodies, is very difficult to conduct for over 335 million vehicles on the road.

4. Public authorities' access to data (B2G)

Principles of legitimate data use and minimisation should be respected in B2G data sharing. Sector-specific legislation should not provide an additional legal basis for governmental access to data; rather, it should preserve the exceptional nature of public authorities' access to data, as envisioned in the Data Act. Commercially sensitive and confidential business data should only be accessed in exceptional circumstances and in accordance with existing legal instruments that provide an adequate legal basis for such access. In all other cases, data sharing with public authorities (B2G) should be done voluntarily.

* * * * *