AD/BR8243/SMR Brussels, 3 June 2022

European Commission's proposal for a regulation on harmonised rules on fair access and use of data

IRU Position on the Data Act proposal

I. IRU POSITION

The International Road Transport Union (IRU) welcomes the European Commission's (EC) legislative proposal on the harmonised rules on fair access and use of data (Data Act) as an important initiative to improve transparency in data sharing.

IRU has signalled for years the necessity of regulating data flows, in particular in business-to-business (B2B) contexts, to create trust, which is a basic enabler of data sharing. Transport operators, which generate large amounts of data, either through their activities or via their vehicles, have notoriously lacked visibility into how that data has been processed, used, re-used by data holders and passed on to third parties. While personal data has benefited from a level of protection under the general data protection legislation (GDPR), no equivalent regime has covered business-generated data so far. This has acted as a hindrance for operators to contribute confidently to building an EU data economy, as also stated in the joint statement of the key transport stakeholders of all modes issued in 2020.

The Data Act recognises the risk of exploitation of contractual imbalances by manufacturers of products and related services (**data holders**), and enacts rules to prevent that kind of behaviour. We appreciate and support the Data Act, in particular the provisions setting out the following rights for businesses that generate data (**users**) while using products or services sold/provided by data holders:

1. The right of users to access the data their business and vehicles generate, including information on how their data is processed, used, re-used and shared with third parties.
2. Portability measures to oblige a data holder to share information with a third party upon the user's request, which, for instance, allows a user to switch between different service providers.

In addition, we also appreciate a response to our call for the EU to promote interoperability standards for a seamless multi-vendor environment and provide access controls throughout the data value chain.

Despite the numerous positive aspects, we are calling for the following additional improvements of the Data Act to achieve its full potential. Also, as the obligations of data holders in the case of data generated by businesses in an online platform context seem to fall outside of the Data Act's scope, we trust that sector-specific legislation will further address such aspects.

1. **Clarify users' access to processed data.** The Data Act is clear regarding the users' access to the raw data generated by the vehicle purchased. However, it remains ambiguous to what extent the users have access also to data processed by the data holder, in which lies great value. Users' access should clearly cover processed data as well.

2. **Extend the scope to small and medium-sized enterprises (SMEs) in case of related services.** It is understandable to limit the scope of the Data Act by excluding manufacturers who are SMEs. This is due to the fact that manufacturers are typically large companies. If they are SMEs, it is unlikely such manufacturers enjoy considerable market power since they compete with larger enterprises. In such cases, the administrative burden set by the Data Act could indeed be disproportionately high compared to the risk of contractual imbalance and exploitation of the user and its data. However, services related to the main product are often provided by SMEs. Excluding SMEs in the case of related services would make the Data Act applicable only to manufacturers of main products on a factual basis.

3. **Specify the obligations of third parties, which receive data from the data holder**. While the Data Act clearly specifies the obligations of the third party receiving the data at the request of the user, it does not regulate the obligations of third parties when they receive data from a data holder, even if the user consented generically to such data sharing.

4. **Require the explicit consent of users for further re-use of data by the data holder, and/or for further passing on information to third parties**. The Data Act already requires the user's right to obtain information on data shared with third parties. However, being aware of the data which is passed on without any possibility to stop the process is insufficient from the users' perspective, since there is an imbalance in most contracts in the bargaining power.

5. **Recognise the right of users to seek compensation in case of data holders' inappropriate sharing of data with third parties**. Inappropriate sharing of data with third parties is one of transport operators' concerns. The Data Act should make specific reference to the right of the user to seek compensation if the data holder passes on information with third parties against the user's consent.

6. **Require data holders to automatically inform the users when data allowing user profiling is shared with authorities demonstrating an exceptional need (B2G data sharing).** If data enabling user profiling is shared for any other reason than a public emergency, users should provide explicit consent. In any case, data that enables user profiling should not be shared with any third parties, including other public authorities.

7. **Provide additional powers to the responsible competent authority for the application and enforcement of the Data Act** in order to run random checks of data holders' duly compliance with this regulation, even in the absence of an open investigation.

II. ANALYSIS

Data-driven technologies have had a transformative effect on the economy at large, and the transport industry in particular. Connected vehicles, smart cities and digital platforms are expected to increase data generation in the future, making the transport sector heavily reliant on non-personal data processing and exchange. Modern, connected vehicles can gather a large amount of data on traffic conditions, vehicle location, tyre pressure or vehicle speed. Such vehicles generate up to 25 gigabytes of data per hour, with autonomous vehicles predicted to generate terabytes of data that can be used for innovative mobility-related services as well as repair and maintenance services.

Data generated by transport operators is not only commercially sensitive but also has an impact on vehicle safety and security, and is regularly shared with third parties without the transport operators' knowledge or approval. Currently, the in-vehicle data generated by the transport operators is almost instantly transferred to the manufacturer (or other data holder), who then processes the raw data further.

The proposed Data Act aims to reallocate the value provided by data by adopting rules to ensure fairness and transparency in the future data economy. The new

proposal's primary goal is to establish a harmonised framework for data sharing in the European Union, as well as to ensure measures for data portability for users and future interoperability standards. As a horizontal proposal, the Data Act will apply to a wide range of products and services, including the connected objects (Internet of Things), vehicles, medical or health devices and virtual assistants.

IRU has previously called on policymakers to develop a legal framework for the access and use of data generated by the transport operators. In this respect, the IRU welcomes the new provisions of the Data Act as a substantial part of the suggestions addressed in the draft proposal. Despite its many positive aspects, we believe the Data Act's provisions could be improved.

1. Right to access and use of data in business-to-business (B2B) context

The proposal ensures that users of products or related services have access to and use the data they generated, including the ability to share such data with third parties of their choosing. Data holders (e.g. manufacturers) will still be able to use the data generated by the user, and will inform the user on the intended use of its data. Prior to entering into a contract[1], the user will also receive specific information about the data that will be generated, the methods of accessing such data, and the potential future data sharing with third parties by the data holder. Manufacturers and designers will have to design the products in a way that makes the data easily accessible by default, and they will have to be transparent on what data will be accessible and how to access it.

IRU is particularly pleased to see a proposal for a binding legal framework for the provision of B2B data, as well as an overview of how users' data is stored, processed, used and reused. While the current proposal is a good starting point, IRU believes there is room for improvement.

IRU calls for:

a) User's access to processed data to be ensured and clarified. For legal clarity, we suggest clearly defining types of data that can be provided to the user (e.g. raw data, metadata and processed data). The Data Act remains ambiguous as to the extent to which users also have access to data processed by the data holder, which is of great value to them.

b) Extend scope to small and medium-sized enterprises (SMEs) in case of related services. It is understandable to restrict the scope of the Data Act by excluding SMEs that are manufacturers. This is because manufacturers are typically large companies. Due to the fact that they compete with such large companies, SMEs are unlikely to have significant market power. In such cases, the Data Act's administrative burden may be disproportionately high in comparison to the risk of contractual imbalance and exploitation of the user and its data. SMEs, on the other hand, frequently provide services related to the main product. Excluding SMEs that provide related services would make the Data Act only applicable to manufacturers.

2. Portability measures and third party data sharing

In its proposal, the EC provides portability measures to oblige a data holder to share information with a third party upon the user's request, which allow a user to switch between different service providers. In such cases, third parties will only process the data for the purpose it was given, and in the manner agreed with the user. They will then delete the data when it is no longer needed, with additional safeguards ensuring an appropriate use of the data by the third party (e.g. confidentiality, privacy and trade secret measures). The proposal establishes contractual, commercial and technical minimum regulatory requirements for data processing services, allowing for switching between such services.

[1] Contract for purchase, rent, lease or use.

IRU welcomes the data portability provisions aiming to avoid vendor lock-in and reliance on a single operator. However, we believe that provisions regarding the third-party data sharing could be improved and further specified.

IRU calls for:

a) The obligations of third parties receiving the data from the data holder to be specified. While the Data Act outlines the obligations of the third party receiving the data at the request of the user, such provisions are lacking in cases where the third party is receiving the data from the data holder.

b) The user should be required to provide explicit consent to the data holder to further reuse and/or pass the data to third parties. According to the current proposal, the user will have the right to be informed about any future third-party sharing by the data holder prior to entering into a contract. While such an obligation can be interpreted as de facto consent, it is necessary for users to be able to stop the process actively. Such consent should be specific, clear and limited in scope.

c) The future framework must also ensure that users can request and receive financial compensation in exchange for the data they provide, in particular in the case of inappropriate data sharing by the data holder. The Data Act should make specific reference to the right of the user to seek compensation if the data holder passes on information with third parties against the user's consent.

3. Exceptional nature of public authorities' right to request access to data and business-to-government (B2G) data sharing

The proposal also requires data holders to make data available to public authorities in Member States and to the Union's institutions, agencies or bodies in cases where there is an exceptional need. Such exceptional need primarily pertains to public emergencies, but there are other exceptional circumstances in which mandatory B2G data sharing is provided for, in order to support evidence-based, effective, efficient and performance-driven public policies and services.

IRU understands that obtaining data by the public authorities is sometimes necessary and beneficial for all parties, in particular taking into account significant time constraints when such data is requested in order to respond to public emergency. We commend the exceptional nature of the public authorities' right to request access to data, as well as additional safeguards regarding compensation, data use and later disposal of data. However, additional protections are necessary in order to avoid data misappropriation in cases where data requested by the public authority enables user profiling.

IRU calls for:

a) Requiring data holders to notify users automatically about data shared with authorities, if such data allows user profiling. The Data Act provides for exceptional circumstances under which public authorities may request data from data holders. When a data holder provides authorities with data that is specific enough to identify the user who generated the data, the user should be automatically informed of the content and scope of the information provided.

b) In cases where the public authority requests data for reasons other than responding to a public emergency, and such data enables user profiling, users should provide explicit consent before any data that could identify them is shared. In such cases, transport operators should be able to make data available to governmental entities strictly on a voluntary basis and avoid actions that force data provision, in particular data identifying the users, which can harm the competitiveness of transport operators due to the risk of data misappropriation, the protection of economic interests and security concerns.

c) In any case, data profiling users should not be shared with third parties, including other public authorities or non-governmental organizations.

4. Enforcement of the Data Act

Currently, the proposal ensures that competent authorities as designated by the Member States will have the power to conduct investigations arising from complaints citing alleged violations of the regulation, including on the basis of information received from competent authorities of another Member States or other public authority. However, the text does not clearly provide for the competent authority to conduct *ex officio* investigations, on its own initiative, in cases where market circumstances suggest that the data sharing obligation was misused or data was misappropriated by the data holder or third parties. Moreover, as both authorities and users, particularly SMEs, may have very limited insight into how data holders further shared and re-use data, it is necessary to empower the competent authorities to run random inspections to check compliance with this regulation. Lacking such power may seriously hinder effective enforcement because complaints have to be based on *prima facie* evidence of infringement. Such evidence may be very difficult to gather by the aggrieved party.

The IRU calls for:

a) Additional powers to the responsible competent authority for the application and enforcement of the Data Act in order to run random checks of data holders' duly compliance with this regulation, even in the absence of an open investigation.

Final considerations

IRU also welcomes the EC's initiative to develop simple, uniform and accessible interoperability standards, particularly in the transport sector. This provides a seamless multi-vendor environment and access controls throughout the data value chain, with the hope that such provisions will be expanded in sector-specific legislation. Transport operators require APIs/data formats that are simple, uniform and accessible.

Furthermore, we advocate for future sector-specific legislation to address the current lack of rules governing data generated by businesses using an online platform. Indeed, the obligations of data holders appear to fall outside the scope of the Data Act in such cases.

* * * * *