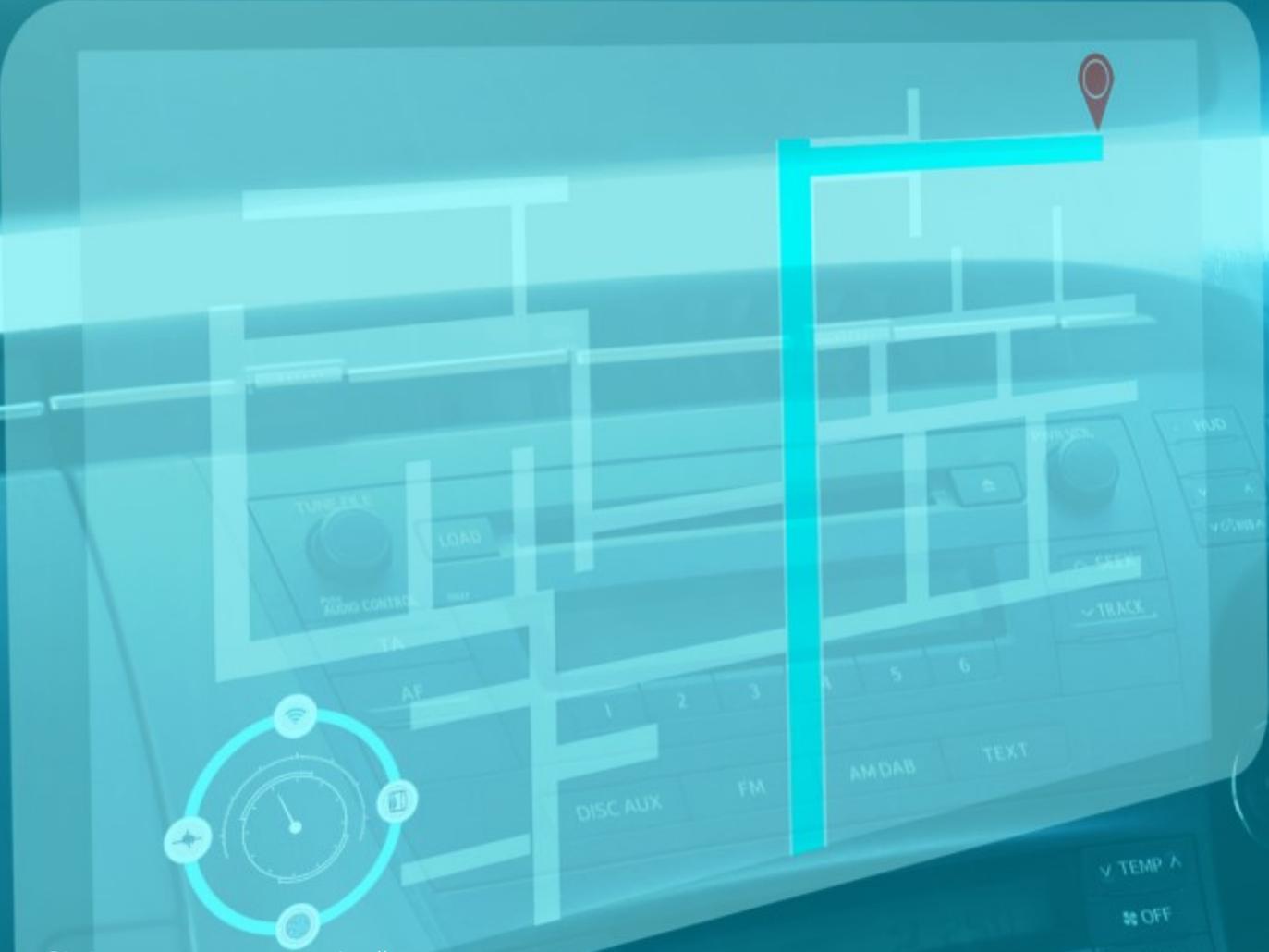


POSITION PAPER

Access to in-vehicle data and resources

On a regulatory framework ensuring a level playing field in automotive digitalisation





Status

Image licences
All rights reserved

April 2021
CLEPA, Adobe
European Association of Automotive Suppliers (CLEPA)

Contents

Executive summary.....	3
Background.....	4
1. What principles lie at the core matter?.....	5
2. Why is access to data so important?	6
3. How should type-approval rules be revised?	8
4. What are the roles and responsibilities of the economic actors?.....	10
Conclusion.....	12

Executive Summary

Fair and undistorted competition is a prerequisite to leverage Europe's full innovation power in mobility services. Any privileged position in the data stream or in the flow of information between a vehicle and the next point of communication has the potential of limiting or even excluding market players from providing services.

Automotive technology is rapidly advancing, with vehicles generating and collecting ever greater quantities of data to operate and monitor systems (e.g. system diagnostics, route planning...). This can provide significant benefits to drivers, passengers, and other road users. This data is also valuable to an expanding market that can make use of it, offer new services to consumers, or improve upon existing repair and maintenance services.

Innovation in this area, however, requires that car data must be shared amongst the different economic actors. Fair and undistorted competition is a prerequisite to leverage Europe's full innovation power in mobility services. Any privileged position in the data stream or in the flow of information between a vehicle and the next point of communication has the potential of limiting or even excluding market players from providing services.

Currently, vehicle manufacturers control the access to all communication devices and thus have a unique privileged position to also control the flow of in-vehicle data. This entails a risk of competition distortion, which will impede consumers from choosing alternative value-adding services from a variety of third-party service providers.

The European Commission intends to assess regulatory options on remote repair and maintenance and other services based on data generated by vehicles by amending the EU's type-approval legislation¹. In this context, CLEPA argues that regulating data access at EU level can and should help ensure fair and equal access for all providers of services to create a competitive market for the benefit and in the best interests of consumers.

Within the regulatory framework for vehicles, it is the homologation process for new vehicles that would be the appropriate instance to ensure that all technical aspects regarding connectivity and access to in-vehicle data and resources are disclosed. Vehicle manufacturers should provide full transparency on technically available data points at different levels in the vehicle, telematics capabilities, and the respective processes for third parties to allow an independent and unmonitored level of access to such in-vehicle data and resources.

In addition, CLEPA recommends that the European Commission put forward legal guidance, from a competition perspective, on the roles and responsibilities of the respective economic actors to ensure fair competition.

1. Para. 2.2 of the Work Programme on Automotive and Mobility Industries 2021-2022 dated Feb 4th, 2021 and communicated by DG GROW in the 145th Motor Vehicle Working Group



The pace of technological development and digitalisation within the automotive sector has increased exponentially. Electronic components already account for a third of a vehicle's value and it is estimated that, by 2025, 70% of the vehicle park will be connected. Today's modern vehicles generate around 25 gigabytes of data every hour and **autonomous cars will generate terabytes of data. This data can be used for existing repair and maintenance services, but could also allow for the emergence of innovative mobility services.**

Remote diagnostics and prognostics, service appointments from the dashboard, software updates over the air, car sharing functions, delivery to the boot, and parking are but a few of these services. Even payment services where the vehicle pays bills in parking garages or at fuel stations via a connectivity-based app are among the services in a **new market whose value could reach 34 billion euro in five years.** Existing markets, such as repair and maintenance which represents 130 billion euro of value for European suppliers, will also be fundamentally changed.²

Innovation in this area requires that car data be shared amongst the different economic actors. In its European strategy for data,³ the European Commission outlined its objective of "review[ing] the current EU type-approval legislation for motor vehicles (currently focused on wireless data sharing for repair and maintenance), to open it up to more car data-based services." This review will look at how data is made accessible by vehicle manufacturers, and which procedures are necessary to obtain it.

In the present position paper, CLEPA therefore outlines the views of automotive suppliers on how a revised regulatory framework could **ensure a fair and equal access to in-vehicle data and resources** for all third-party service providers.

2. Roland Berger in ETRMA/Quantalyse report "Connected & Automated Mobility – Tyre Industry Use Cases That Require Direct Access to In-Vehicle Data," June 2019.

3. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, A European strategy for data, COM(2020) 66 final, <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0066&from=EN>.

1. What principles lie at the core matter?

Any privileged position in the data stream or in the flow of information between a vehicle and the next point of communication has the potential of limiting or even excluding market players from providing services, thus diminishing the variety of services available to consumers.

Today's vehicles generate vast amounts of data and are widely equipped with communication interfaces. Most of these vehicles route data exclusively via the servers of the vehicle manufacturer. Only from there can data then be made available to third parties. **Any privileged position in the data stream or in the flow of information between a vehicle and the next point of communication has the potential of limiting or even excluding market players from providing services**, thus diminishing the variety of services available to consumers.

In recent cross-industry discussions, vehicle manufacturers have shown openness to share data with third parties, but not all concerns have yet been resolved. CLEPA has laid out the principles required to **ensure fair and equal access for all providers of services and to create a competitive market for the benefit and in the best interests of consumers**. These principles are also relevant for any regulatory approach, and aim to ensure businesses have access to in-vehicle data and resources in the following manner:

✂ The routing of data via vehicle manufacturers or any other party in between the data and the service provider should be organised in an **unmonitored manner**, without the need for a service provider to disclose data usage, business model, or customer/data subject information to any other competing party;

✂ Service providers should be granted transparency on and access to **all in-vehicle data, functions, and resources that are technically available via bi-directional communication**, independent from whether these data are used by the vehicle manufacturer for their own services;

✂ For the purpose of collecting, processing and analysing data that is generated in the vehicle, third parties should be granted the possibility to **operate their own applications and software** in the vehicle;

✂ Service providers should have the option/ accessibility to **interact safely with the driver** via access to the vehicle resources, such as displays and audio systems (voice command).

CLEPA underlines the need for safe and secure communication with the vehicles, as a prerequisite for access to in-vehicle data and resources as laid out in the principles above.

The scope of the data considered in this context should be understood as restricted to data which is generated by the original source (in this case the vehicle) and not to be confused with data in platform services that have been subject to data processing and/or refinement and made available as a service and may be covered by IP rights, depending on the relevant legal criteria.

2. Why is access to data so important?

The manufacturers control the access to all communication devices and thus have a unique privileged position in the data flow. This entails a risk of competition distortion, in turn hindering the opportunity for consumers to choose alternative value-adding services from a variety of third-party service providers.

Digitalisation is fundamentally transforming the automotive industry. The breakthrough of connected vehicles is gaining substantial momentum, along with the capability to make use of in-vehicle data and resources. Vehicle manufacturers, automotive suppliers, and many other market participants (such as independent repair shops or location technology service providers) are already offering in-vehicle data-based services. This is the first step along the path to a data economy, as laid out by the Commission in its European strategy for data.

Currently, connected vehicles are communicating only with their manufacturer's server over the air and do not support any other access method, while safety related data (e.g. detecting accidents or dangerous road conditions) is still difficult to obtain, despite being required under existing EU law.⁴ At the same time, **existing communication interfaces, such as OBD connectors, are increasingly limited** in the data and functions they support and are restricted to authorised-access only, granted by vehicle manufacturers. Therefore, the manufacturers control the access to all communication devices and thus have a **unique privileged position in the data flow**. This entails a **risk of competition distortion**, in turn hindering the opportunity for consumers to choose alternative value-adding services from a variety of third-party service providers.

Vehicle manufacturers act as data processors, data controllers, and service providers that compete with other market participants.⁵ **Fair and undistorted competition is a prerequisite to leverage Europe's full innovation power in mobility services.** "Key areas for safeguarding fair competition are ensuring equal access to resources (HMI) and data (both in terms of types of data available and timeliness) and avoiding the ability of any market participant to delay, dilute or deny access to data."⁶ How and to what extent such access is granted has a substantial impact on the performance and competitiveness of use cases.

Regulatory guidance should address concerns related to privileged access to in-vehicle data and resources. Currently, "third-party marketplaces and platforms still depend on data supplies and access to the HMI that are controlled by the [vehicle manufacturers]."⁷

Fair and undistorted competition is a prerequisite to leverage Europe's full innovation power in mobility services

4. Commission Delegated Regulation (EU) 886/2013 of 15 May 2013 supplementing Directive 2010/40/EU.

5. p. 9. Guidelines 1/2020 on processing personal data in the context of connected vehicles and mobility related applications, Version 1.0 Adopted on 28 January 2020, European Data Protection Board, https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_202001_connectedvehicles.pdf.

6. p. 9. Access to In-vehicle Data and Resources Final Report, May 2017, TRL, <https://ec.europa.eu/transport/sites/transport/files/2017-05-access-to-in-vehicle-data-and-resources.pdf>.

7. p. 24. JRC Digital Economy Working Paper 2018-06, Access to digital car data and competition in aftersales services, JRC, <https://ec.europa.eu/jrc/sites/jrcsh/files/jrc112634.pdf>.



SOCIAL BENEFITS OF IN-VEHICLE DATA



Traffic flow improvement

Advising on safest route, avoiding traffic jams



Vehicle monitoring

Reporting on maintenance and efficiency



Emergency assistance

Automatically calling emergency services in case of accident



Automatic payment

Speeding up processes in parking or tolls



Travel comfort

Personalising services and entertainment for passengers

In this context, **CLEPA supports the Commission's objective to look through the lens of the type-approval legislation** for motor vehicles, with regards to potential new requirements on access to in-vehicle data and resources. We believe that **vehicle connectivity interfaces should be accessible to all stakeholders**, assuming that the data is collected from data subjects⁸ and processed in compliance with the relevant legal bases.⁹

This means that, as part of the homologation process for new vehicles (type-approval framework regulation 858/2018), all technical aspects regarding connectivity and access to in-vehicle data and resources should be included. Like the existing requirements on Repair and Maintenance Information (RMI), **the**

homologation process should ensure that vehicle manufacturers provide full transparency on technically available information and in-vehicle data at different levels (communication interface, data and functions definitions, control units, OBD, etc.) in the vehicle. In addition, **it should be ensured that data flow between economic actors is not restricted** in cases where one stakeholder has control over the consent process. CLEPA's views on how the type-approval regulation should be amended are outlined in the next section.

The type-approval regulation, however, only covers the technical requirements. Therefore, CLEPA also recommends that the Commission put forward legal guidance from a competition perspective on the roles and responsibilities of the respective economic actors (see section 4).

8. p. 9, Guidelines 1/2020 on processing personal data in the context of connected vehicles and mobility related applications Version 1.0 Adopted on 28 January 2020, European Data Protection Board, https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_202001_connectedvehicles.pdf; the data subject is the natural person to whom the data covered by the processing relate. In the context of connected vehicles, it can, in particular, be the driver (main or occasional), the passenger, or the owner of the vehicle.

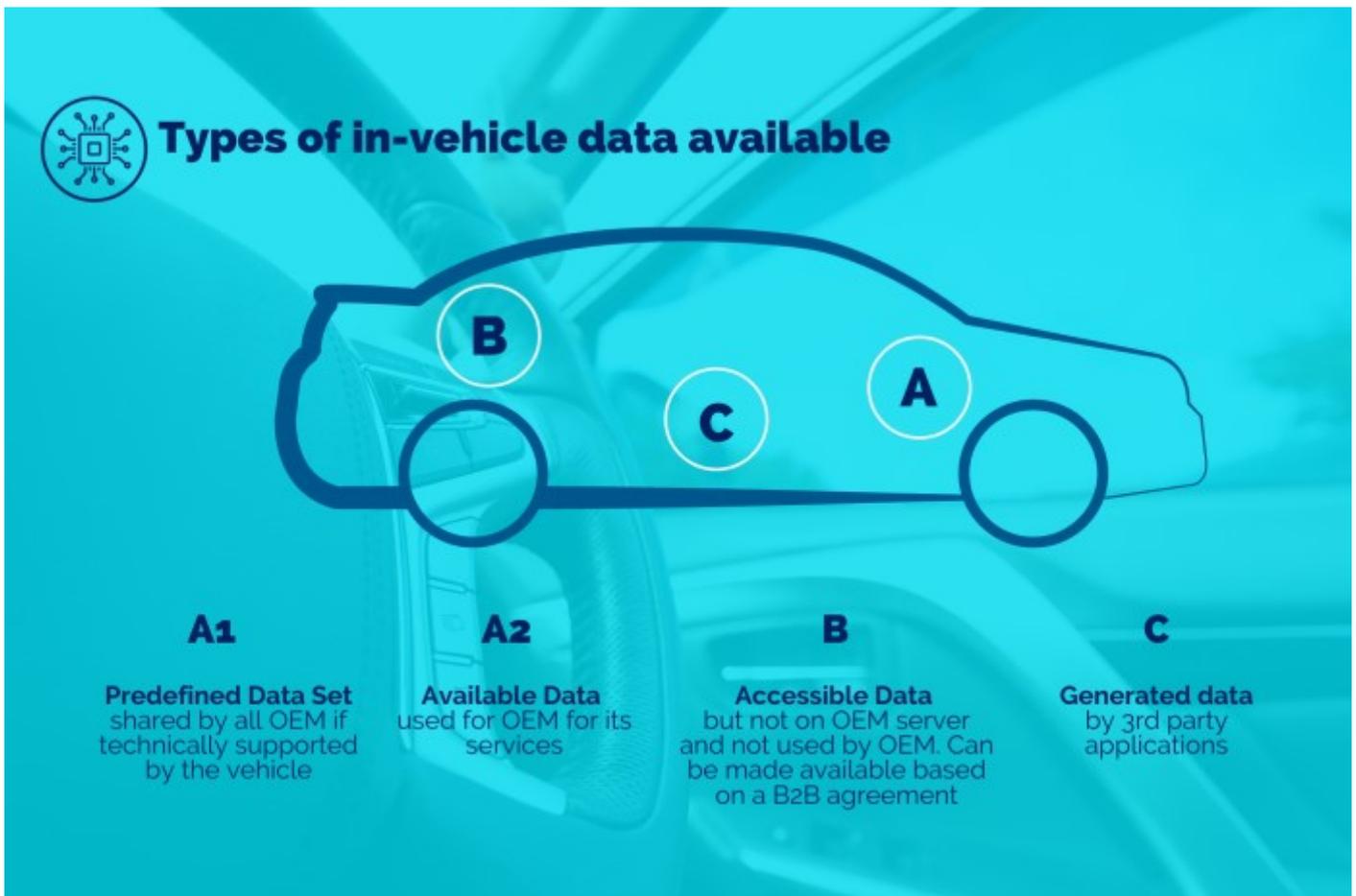
9. Legal grounds for the collection and processing of data are defined in several legislative texts. For personal data, this includes the GDPR and the e-Privacy Directive, where legal grounds include consent and legitimate interest.

3. How should type-approval rules be revised?

CLEPA asks to ensure transparency on the technically available in-vehicle data points and functions defined for each vehicle type, and on the variations specific to each vehicle built.

Data can be available at different locations in the vehicle or can even be calculated within an application in the vehicle. Currently, vehicle manufacturers are the only ones with an overview of available data points and functions at the different levels in their vehicles, or of available embedded routines which can be activated remotely.

Regarding the technical aspects to be covered by the type-approval regulation, CLEPA asks to **ensure transparency on the technically available in-vehicle data points and functions** defined for each vehicle type, and on the variations specific to each vehicle built.



*Infographic based on 5th meeting of the "Access to Vehicle Data & Cybersecurity" Expert Group - Workshop on Access to vehicle data, Brussels, 13 March 2020



Following the legislative logic already present for Repair and Maintenance Information (RMI), whereby diagnostics' purposes must be made transparent and accessible to third parties, CLEPA believes that this should be extended to data points, functions, and embedded routines. **Specifically, automotive suppliers are keen on including the following elements:**

- ✿ There should be **full transparency on all available data points and functions available** at the vehicle manufacturer's backend, at the level of the vehicle's communication interface, and at any other place in the vehicle where it is possible to make such data available. Such a list of data points (shown as A1, A2, and B in the chart above), including related functions, should be **subject to regular updates** consecutive to new features being added to the vehicle with software updates or new vehicle equipment. CLEPA has already identified **529 data points** for currently planned use cases by third parties, which were submitted to the Commission's Motor Vehicle Working Group (MVWG). CLEPA considers this list to be a first summary of most relevant data points which should get extended with the introduction of further use cases.
- ✿ **A minimum set of around 40-50 mandatory data points**, as proposed by ACEA in the MVWG (shown as A1 in the chart above), should **always be made available to third parties**, if these data points are supported by the vehicle. Access should be made possible at the vehicle's communication interface and **include attributes and formats binding for all vehicle manufacturers** in the EU. Such a data point list should also be **subject to regular review** by the Commission.
- ✿ There should be **a description of the process for third parties to retrieve information on available data points** by VIN number. In line with existing regulatory principles, this information should be "made available, in the form of machine readable and electronically processable datasets, in a database that is easily accessible to independent operators."¹⁰
- ✿ There should also be **a description of the process for third parties to get access to in-vehicle resources**, such as:
 - ✿ How to **interact with the driver** through visual displays and/or audio devices (e.g., voice command).
 - ✿ How to **access embedded software routines and functions** utilised by the vehicle manufacturer to activate components and functions (e.g., the opening of doors or the boot, or the activation of diagnostic routines).
 - ✿ How to **install software routines or applications** inside the vehicle, including how to receive approval from the vehicle manufacturer for the installation of such third-party applications and software routines.
 - ✿ This should include information on **processes for users to grant and withdraw their consent** for personal data collecting and processing, when applicable, which should be designed according to the latest state-of-the-art user experience.

Vehicle manufacturers should be required to **provide an application programming interface (API) to allow third-party software to be executed** in the vehicle.

10. Regulation (EU) 2018/858 of the European Parliament and of the Council of 30 May 2018, Annex 10, 6.1.

4. What are the roles and responsibilities of the economic actors?

All connectivity interfaces in new vehicles are designed in such a way that the entire data transfer is routed exclusively via the vehicle manufacturer backend servers. Even if access to such data is granted, utilisation of this data will depend on contractual agreements between dependent—and to some extent competing—business partners.

Currently, all connectivity interfaces in new vehicles are designed in such a way that the entire data transfer is routed exclusively via the vehicle manufacturer backend servers. This leaves all third-party service providers dependent on the data offering made by the vehicle manufacturers. Even if access to such data is granted, utilisation of this data will depend on contractual agreements between dependent—and to some extent competing—business partners. CLEPA sees the **need that the roles and responsibilities of vehicle manufacturers and third-party service providers follow certain rules:**

Responsibilities of vehicle manufacturers

- ✿ At the very least, they should **not be allowed to detect or monitor data flows** between the vehicle and third-party service providers, **nor make use of third-party data**.
- ✿ They should **not be permitted to ask for end-customer information**, except for legal obligations, such as requests from law enforcement authorities.
- ✿ They should be **independent of any competitive concern**, and not discriminate between economic actors.
- ✿ They should **establish a clear process for third parties to gain access** to additional data points, install software, and handle complaints. They should also be under the obligation to answer requests for access within a reasonable timeframe.
- ✿ When granting authorisation to a third party, vehicle manufacturers should **not be allowed to make use of the authorisation information**.
- ✿ They should ensure **transparency on network operation costs** within their contractual relations with third-party service providers, to allow the latter to understand what they may be charged.
- ✿ Costs charged to third-party service providers for network operation, vehicle generated data, and data access should **remain reasonable and be directly related to the real costs incurred** by the vehicle manufacturers.
- ✿ Handling of data should always be done in compliance with the existing EU rules on **personal data protection and privacy**.
- ✿ Vehicle manufacturers should be **liable for safety, integrity, and cybersecurity**. In addition, such concerns should not be unreasonably invoked to limit data access for third parties or the creation of use cases.
- ✿ There should be some form of the **supervision of vehicle manufacturers**, to ensure that they respect the obligations outlined in the previous points.



Responsibilities of third-party service providers

- ✂ They should **abide by defined rules when requesting access**, and follow the processes established by the vehicle manufacturers to this effect.
- ✂ They should apply state-of-the-art methods and standards to **ensure data protection, privacy, and security** when handling the data, for example by following ISO standard 21434 on cybersecurity management systems and of course by respecting EU legislation on personal data protection.
- ✂ They should be **liable for what they do with the in-vehicle data and resources**, including for any action that they carry out on the vehicle through the access they have been granted. There should also be a liability trail for possible audits.

Currently all connectivity interfaces are designed in such a way that the entire data transfer is routed exclusively via the vehicle manufacturer



Conclusion

CLEPA advocates for fair competition, a level playing field amongst market participants and giving consumers access to services from a broad choice of providers while maintaining safety, cybersecurity, and full compliance with the prevailing legislation on competition and the protection of personal data such as user consent for data sharing.

European automotive suppliers are committed to the ongoing dialogue (i.e., on the NEVADA extended vehicle concept) with vehicle manufacturers and other stakeholders in pursuit of a result that would fully satisfy the criteria outlined in the present position paper. CLEPA also recognises that significantly more progress is needed to reach a fruitful conclusion.

CLEPA acknowledges the fact that the European regulator is exploring legislative options with the aim of ensuring fair competition. In this context, CLEPA maintains that regulatory guidance can create the clarity and certainty needed for all stakeholders involved, provided that certain key principles are incorporated. These principles are laid out in more detail in this position paper.

Without these principles in place, the developing digital market in automotive incurs the risk of further distortion of competition in aftersales and on the market for new mobility services due to economic actors gaining or cementing a gatekeeping position in the market for such services. Conversely, fair competition will ensure increased choice for consumers and amplification of innovative services.

Would like to know more? You can contact:

CLEPA's Senior Consultant Market Affairs

Frank Schlehuber at consultant.MA@clepa.be

CLEPA's Policy Manager | Government Affairs

William Moreau at w.moreau@clepa.be

CLEPA, the European Association of Automotive Suppliers, represents over 3,000 companies supplying state-of-the-art components and innovative technologies for safe, smart, and sustainable mobility.

CLEPA brings together over 120 global suppliers of car parts, systems, and modules and more than 20 national trade associations and European sector associations. CLEPA is the voice of the EU automotive supplier industry linking the sector to policy makers.

- The automotive sector accounts for **30% of R&D** in the EU, making it the number one investor.
- European automotive suppliers invest over **30 billion euros** yearly in research and development.
- Automotive suppliers register over **9,000 new patents** each year.
- Automotive suppliers in Europe generate **1.7 million** direct jobs.