Connected vehicle:

8 principles for a balanced ecosystem accessible to everyone

AUTOMOBILE CLUB ASSOCIATION

ffea FÉDÉRATION FRANÇAISE DE L'EXPERTISE AUTOMOBILE

FRANCE ASSUREURS
FAIRE AVANCER LA SOCIÉTÉ EN CONFIANCE

MOBILIANS Les entreprises de la mobilité

Mobivia

Sesamlld

SNSA SYNDICAT NATIONAL DES SOCIÉTÉS D'ASSISTANCE

UFE Union Française de l'Électricité

Vehicle connectivity opens an extremely wide field for the creation of innovative digital services and new solutions for the general public.

These new services will improve the comfort and lives of drivers and passengers. Other services will be broad in scope, contributing in particular to road safety, infrastructure optimisation, ecological transition and vehicle electrification.

Likewise, they will facilitate the sharing of public space between all mobility players.

Access to data is at the heart of these developments and a major concern for each of the stakeholders in this emerging ecosystem.

Technologies are also evolving very rapidly, enabling new global-sized entrants with dominant approaches.

To preserve European competitiveness and sovereignty, upstream and downstream operators in the automotive industry are invited to develop common, shared and balanced solutions in the fundamental interest of users.

It is in this spirit that the signatories of this document came up with the following eight principles:

1 All data, whatever their nature and subject to user consent, must be **accessible in all fairness** to all stakeholders. This also implies full transparency on the available data.

2 Vehicle **users' choices** must be made truly effective through smooth processes for obtaining their **consent.**

3 Several access methods must be provided in order to preserve **technological neutrality** and avoid market foreclosures or gatekeeping mechanisms.

4 These **accesses must take place under identical technical and economic conditions for all players,** from the manufacturer to the independent operator. Financial conditions must be reasonable and compatible with the development of innovative digital services.

5 **Access to vehicle data and resources** (including the human-machine interface) **must be direct and, when necessary, in real time** (i.e., without delay).

6 Stakeholders must, as part of a business need, be able to access essential data stored in the electronic control units themselves.

7 **A cross-sectoral and cooperative approach** should make it possible to work towards a shared objective of vehicle security and cybersecurity.

8 **European regulations are essential,** particularly in terms of standards and interoperability, in order to establish these principles and neutral governance.

ABOUT US, CONNECTED MOBILITY PLAYERS

AUTOMOBILE CLUB ASSOCIATION

1,595,095 members

Representative of drivers and road users in France

MOBILIANS Les entreprises de la mobilité

45 million vehicles

150,000 companies

4 families of trades related to the life of vehicles: maintenance, bodywork, painting, commerce and service.

SNSA SYNDICAT NATIONAL DES SOCIÉTÉS D'ASSISTANCE

More than 30 million vehicles covered for roadside assistance

€3,6 billion of sales in France

11,000 employees in France

ffea FÉDÉRATION FRANÇAISE DE L'EXPERTISE AUTOMOBILE

4 million vehicles appraised annually

€315 million of sales

5,500 jobs

Mobivia

30 million vehicles maintained each year

€3.1 billion of sales

23,000 jobs

UFE Union Française de l'Électricité

€40 billion of sales

200,000 jobs

FRANCE ASSUREURS
MOVE SOCIETY FORWARD CONFIDENTLY
A brand of Fédération Française de l'Assurance

55 million of vehicles insured

23 billion automobile insurance premiums

147,000 jobs

SesamlVd

2 million vehicles representing 25% of French vehicle registrations

€9 billion of sales

4,768 jobs

Vehicle connectivity opens an extremely wide field for the creation of innovative digital services and new solutions for the general public.

These new services will improve peaceful driving, comfort and life of drivers and passengers. Many of them are broad in scope, contributing in particular to road safety, infrastructure optimisation, ecological transition and vehicles electrification. Likewise, they facilitate the sharing of public space between all mobility players. All of them contribute, more broadly, in the development of increasingly connected, cooperative and autonomous mobility. As with any digital technology, data represent the key component in these developments.

Thus, the issue of access to vehicle data is at the centre of several debates today.

This is the case in France around the draft ordinance adopted in application of the Mobility Orientation Act ("LOM" article 32). This is also the case in Europe where the European Commission notably published, in February 2020, a European strategy for data. This strategy should lead to several standards and regulations, in particular the review, in the first quarter of 2021, of the legislation relating to vehicle type-approval[1] and the review of the ITS directive.

[1] Regulation No. 715/2007 of the European Parliament and Council of 20 June 2007 relating to the approval of motor vehicles with regard to the emissions of private and light commercial vehicles (Euro 5 and Euro 6) and to information about vehicle repair and maintenance - Regulation (EU) 2018/858 of 30 May 2018 relating to the approval and market surveillance of motor vehicles and their trailers, as well as of the systems, components and separate technical units intended for these vehicles.

This document has been drafted by several economic players (ACA, FFEA, France Assureurs, Mobilians, Mobivia, SesamIld, SNSA, UFE).

It aims to facilitate understanding of the different modes of access to vehicle data and resources and specify the main strategic, technical and economic issues, while keeping the general interest of users at the centre of concerns.

01

Automotive data are primarily **personal data that the user must be able to control.**

The draft guidelines of the European Data Protection Committee[2], such as the “Connected Vehicles & Personal Data” Compliance Pack[3] drawn up by the French Data Protection Agency (CNIL), specify that *“all vehicle data are considered as personal data which, alone or in combination, can be attached to an individual (driver, holder of the vehicle registration document, passenger, etc.), in particular through the vehicle’s serial number [...]. For example, personal data are data relating to journeys, the state of wear of parts, dates of technical inspections, number of kilometres or driving style [...].”*

No one can claim ownership of these data and moreover restrict access to them. Trade secret protection and intellectual property rights, which some players could invoke to protect the equipment and technologies needed to produce data, do not however give them any right of ownership or restriction on said data deemed the user’s personal data.

What are the implications of GDPR obligations for connected vehicles?

In addition to the principle of integrated personal privacy protection (“Privacy by Design”), which now applies to personal data from the design of any application, the main objective of the GDPR is to protect the rights of individuals in the processing of data concerning them, and in particular:

- **Obligation to inform and be transparent with the driver, owner or user of the vehicle** (purposes, recipients, retention periods, etc.);
- **Obtaining users’ explicit consent, which gives them control over how their data are used** and contributes to the principle of informational self-determination;
- **Data portability to users’ preferred service providers.** This principle guarantees the mechanisms of free competition and self-regulation of prices as well as the selection and permanent adjustment of the quality of services.

[2] Guidelines 1/2020 on processing personal data in the context of connected vehicles and mobility related applications

[3] “Connected Vehicles & Personal Data” Compliance Pack prepared by the CNIL (Commission Nationale Informatique & Liberté / French Data Protection Agency) in France in October 2017

Indeed, the user's interest lies in protecting and controlling his personal data, but also in the **quantity, variety, quality and competitiveness of the products and services** offered to him. It is in users' interest to be able to freely share their connected vehicle's data, **thereby encouraging a profusion of innovations and services.**

How to protect the user's interest?

- With a **data access architecture**, internal and external to the vehicle, which is **open and secure** to protect the personal nature of the data but also their **portability to service providers of the user's choice;**
- With **flawless and configurable management over time of the authentication and consent** integrated by design;
- With **standardisation of relevant data and how to access them, which promotes the interoperability of solutions;**
- Through decoupling of the sale of the vehicle including its connectivity and, on the other hand, the provision of offers and services related to the data;
- By removing any barrier to access automotive or mobility services operated by third parties.

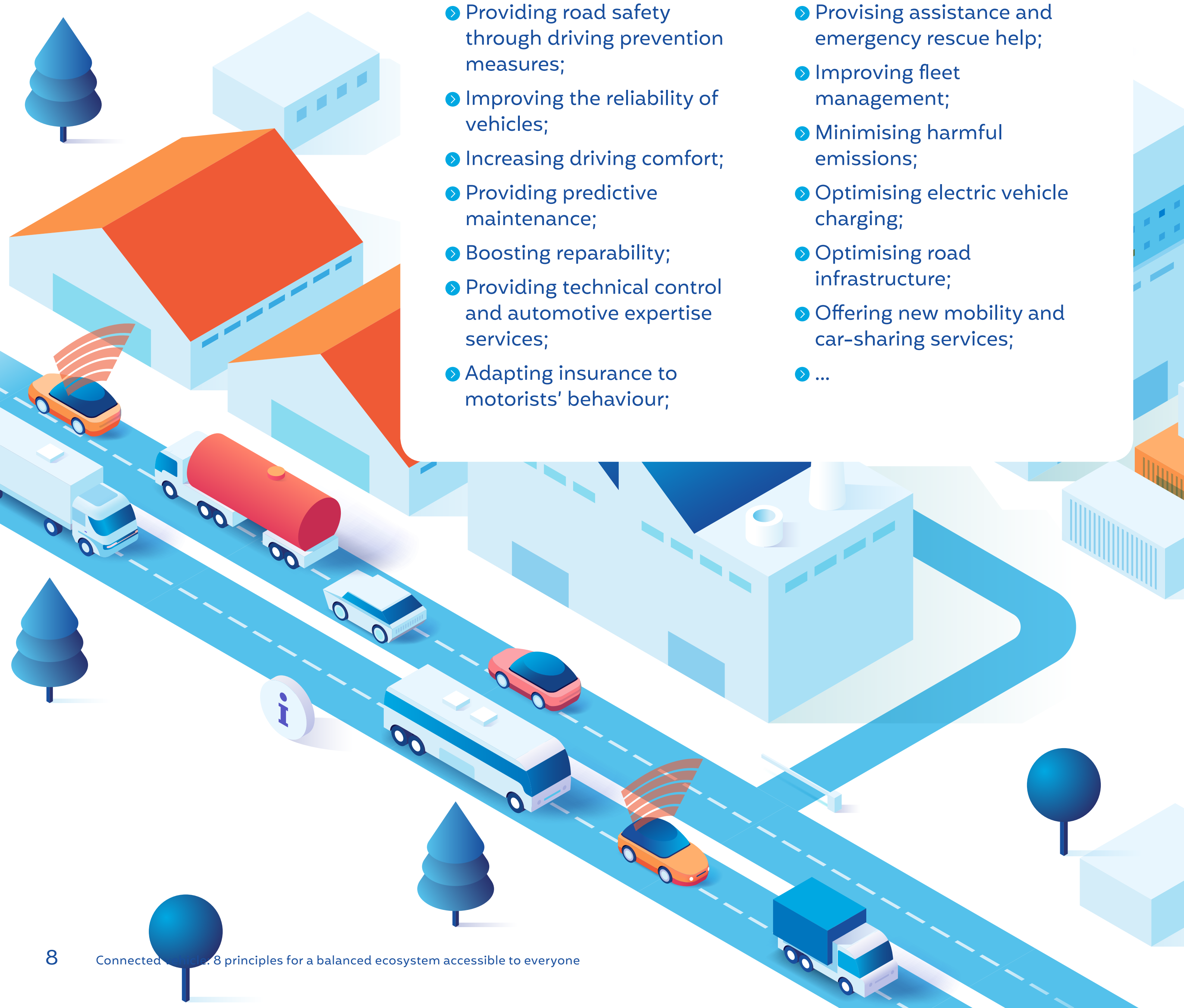
Personal data from a connected vehicle must be used in the interests of the motorist and in accordance with the provisions of the GDPR.

02

Modalities of access to data and resources directly impact the user.

Upstream and downstream players of the automotive industry are willing to develop new services aiming at:

- Providing road safety through driving prevention measures;
- Improving the reliability of vehicles;
- Increasing driving comfort;
- Providing predictive maintenance;
- Boosting reparability;
- Providing technical control and automotive expertise services;
- Adapting insurance to motorists' behaviour;
- Provising assistance and emergency rescue help;
- Improving fleet management;
- Minimising harmful emissions;
- Optimising electric vehicle charging;
- Optimising road infrastructure;
- Offering new mobility and car-sharing services;
- ...



Industry benchmarks

ROAD INSURANCE, ASSISTANCE AND PREVENTION

Access to data for insurers can help develop and significantly improve products and services for users, increase the quality and speed of assistance and, more broadly, contribute to a common goal and general interest in improving vehicle reliability and road safety. In doing so, these services make it possible to control the cost of insurance as well as public expenditures (intervention of emergency services and law enforcement).

This access will make possible the widest distribution of innovative insurance products better suited to user needs, such as "Pay How You Drive", which encourages and rewards virtuous behaviour. Drivers who have developed bad habits will be able to benefit from personalised support (coaching) to prevent dangerous situations during future trips. In the event of a claim, access to data can streamline the reporting process and speed up compensation.

Instant communication makes assistance services much faster and more efficient, in particular thanks to geolocation and detailed technical information transmitted by the vehicle itself in the event of a breakdown or accident.

Insurance can be more effective in combating vehicle theft, recovering stolen vehicles and preventing them from being unlawfully put back on the road.

Thanks to accident data and their detailed analysis (accidentology), a better and more precise understanding of claims and their causes enables the various players to contribute to the continuous improvement of vehicle technology and infrastructure.

User services may require access to data and to several vehicle resources, such as:

Two-way and secure interaction with vehicle controls, such as unlocking a door for a carsharing application;

Connectivity and data transfer solutions:
- internal vehicle systems or sub-systems[4],
- with on-board equipment in the passenger compartment[5],
- on the immediate surroundings[6] of the vehicle to communicate with other road users, or
- remotely[7] for Web or mobile applications for example;

Storage and computing capacity, in and out of the vehicle, to host this data but also the algorithms and on-board intelligence that make the services valuable to the user;

An **ability to interact with the user**, in particular through applications available via screens and other **HMI** (human-machine interfaces) devices of the vehicle, without distracting the driver and in compliance with road safety requirements.

[4] Internal CAN Bus or Ethernet communication network allowing data exchange between all of the vehicle's sensors and on-board computers.

[5] WiFi, Bluetooth or other type connectivity.

[6] V2X point-to-point communication: Vehicle to vehicle, vehicle to infrastructure, etc.

[7] GPRS mobile telecommunications, 2 to 5G, or LoRaWAN type low bandwidth radio.

Industry benchmarks

AUTOMOTIVE EXPERTISE

As part of his various missions, an automotive adjuster must be able to access all relevant technical data in order to perform his work.

This concerns his "road safety" position in the context of the highway code (certification of the vehicle after an accident) but also his position in the field of automobile insurance (damage assessment and search for the causes and circumstances after an accident) and trusted third parties who protect and manage consumer interests (finding faults/defects on a vehicle).

In all these settings and in full compliance with the adversarial principle, an automotive adjuster must be able, in complete independence and complete neutrality, to easily and quickly access any data deemed relevant in an Electronic Control Unit.

There are several ways to access vehicle data

1 Remote access via **proprietary data servers,** operated by each of the manufacturers for its own brands (This model is generally associated with the name of the **"Extended vehicle"**);

2 Remote access via a single, multi-brand server, which is added to the manufacturers' servers. It is referred to as a **"neutral server"** if it is non-profit, and **"data marketplace"** if it aims to monetise data;

3 Direct access to the vehicle via a **physical interface** such as the OBD port[1], which can receive a diagnostic device, a telematics device or any other solution for collecting, processing and broadcasting data;

4 Direct access to the vehicle's data via an embedded software platform, a kind of "car OS[2]" that can natively use essential data and resources and interact with the user via the vehicle's HMI[3] interfaces.

These data access methods, which all have their advantages, nevertheless have varying degrees of openness and maturity depending on the vehicle, brand and model.
Some of these methods also present constraints or limitations, of a technical or economic nature, which make it impossible to satisfactorily develop applications. Thus, the services offered to the user cannot be complete and adequate without the ability to **directly access data, resources and essential vehicle interfaces** *(see recommendations and detailed study below on pages 21 to 27).*

[1] OBD: On-board diagnostic - [2] OS: Operating System - [3] HMI: Human Machine Interface

Practical details *Principles*	Extended vehicle server	So-called neutral server	Data marketplace server	Vehicle physical interface	On-board application platform
Data accessibility	✗ Partial, remote, by manufacturer	? Partial, remote, harmonised	? Partial, remote, harmonised	? Partial, direct vehicle, standardised	✓ Direct vehicle, standardised
Consent	✗ Intermediated, monetisation of personal data	✓ Fluid	✗ Intermediated, monetisation of personal data	✓ Fluid	✓ Fluid
Market asymmetry	✗ Strong	? Average	? Average	✓ Low	✓ Low
Cost of data access*	✗ Base cost + margin	✓ Base cost	✗ Base cost + margin	? Base cost + equipment	✓ Base cost
Real time access	✗ Risk of latency	✗ Risk of latency	✗ Risk of latency	✓ Yes	✓ Yes
HMI integration	? Low	✗ No	✗ No	✗ No	✓ Yes
Electronic Control Unit data	✗ No, aggregated	✗ No, aggregated	✗ No, aggregated	✓ Possible	✓ Possible
Security and Cybersecurity**	✓ Yes	✓ Yes	✓ Yes	✓ Yes	✓ Yes
Assessment	**Unsatisfactory as is** ⚠	**Useful but not sufficient** ?	**Unsatisfactory as is** ⚠	**Necessary but not sufficient** ? ✓	**To implement** ✓

The diversity of the services and applications requires multiple ways to access data.

* Based on the actual costs of implementing the solution, and where applicable, a margin applied by an operator for data monetisation

** Provided that the solutions are implemented according to best practices.

Technically, in addition to the **cybersecurity** elements which are obviously a prerequisite, these methods must meet the needs of all players in the ecosystem by providing:

- Access to data in sufficient **volume, latency, nature, quality and granularity** to provide the proposed service;

- The ability to process these data, as close as possible to their source (edge-computing), using algorithms and embedded intelligence;

- **Interactions with the driver** as he operates and uses the vehicle – **consistent with** road safety **constraints**;

- The ability to share vehicle data with the vehicle's immediate surroundings and the information derived from such data (V2X: "Vehicle to infrastructure" or "vehicle to vehicle").

Solutions for accessing data and vehicle resources must be fully aligned with the needs of all ecosystem players.

03

It is essential to avoid market foreclosure and **promote technological neutrality.**

Access to vehicle data and resources concerns all players in the value chain. It must be **fair, unrestricted and take place without delay,** in order to protect consumer rights, promote innovation and **ensure fair and non-discriminatory competition in this market and comply with a principle of technological neutrality**[8].

Restricting access to data or unfair access would have the effect of limiting the services likely to be offered to the user (consumer, owner, driver, etc.), depriving civil society of improvements in terms of road safety, quality of life or reduction of polluting emissions.

In its strategy for future mobility[9], the European Commission recognises that "*Manufacturers have privileged access to car data and vehicle resources*". It also states "*that centralisation on platform servers of extended vehicle data could not, in itself, be sufficient to ensure fair and undistorted competition between service providers.*"

Indeed, the obligation to use centralised data platforms – whether operated by the manufacturer or by any for-profit organisation – would raise questions of governance of these data and risks of market asymmetry, or even of monopolies and speculation on the commercial value of these data:

- the systematic flow of data via a centralised platform would give its operator a global and complete view of the market and place it in a dominant position;

- a platform operator that obtained the user's consent, on behalf of an independent service provider, would constitute an intermediation for the service provider and an obstacle to the fluidity of its customer relationship;

- for users, a proprietary platform acting as a gatekeeper could limit the portability of their data to competing solutions, hampering the mechanisms of self-regulation of prices and quality of services;

[8] Idea taken up by BEUC in its study "Protecting European consumers with connected and automated cars" of November 2017: "*Car makers and service providers should guarantee fair access, storage and sharing of vehicle data while fully respecting data protection laws and the principles of privacy by design and by default.*"

[9] Commission, "On the road to automated mobility: an EU strategy for future mobility", 17 May 2018, COM (2018) 283 final.

- the centralisation of data by manufacturers (or marketplaces) carries risks of opacity on pricing and real costs;

- the provision of data via manufacturers' servers can lead to more complex access conditions for independent service providers, for whom their negotiating capacity would remain limited. These discriminatory conditions can be technical or economic.

- Finally, the risk of data filtering by manufacturers could lead to a **lack of transparency** (e.g., concerning vehicles' performance and reliability).

According to a study by the Fédération Internationale de l'Automobile (FIA)[10]...

... European consumers could incur up to €32 billion of additional expenditures if the freedom of choice of providers is not guaranteed. This would be due to:

- the costs imposed on providers for access to data generated by motorists;
- restrictions on access to certain data;
- the management of data transfer by car manufacturers, which would limit competitiveness.

[10] FIA Region I, « The automotive digital transformation and the economic impacts of existing data access models », March 2019.

Opening access to data to all players in the ecosystem can be done at marginal cost, insofar as vehicles are natively equipped with connectivity solutions – in accordance with regulatory requirements (European "eCall" emergency calls & "C-ITS" intelligent transport systems).

The interests of end users and all stakeholders are based on the general principles of **free competition, transparency and antitrust.** This allows a fair pricing as close as possible to the **marginal costs** (costs of the **equipment** and **data service necessary for sharing data**).

Indeed the provision and sharing of data that is already extracted to meet regulatory or manufacturer needs only generates a marginal cost compared to the one incurred by vehicle connectivity.

Furthermore, European directives, in particular eCall and C-ITS stipulate the implementation of communication solutions. In addition, the digitisation of the automotive sector requires connectivity and the exchange of data (Vehicle to Vehicle and Vehicle to land infrastructure).

It is essential to ensure complete technological neutrality in terms of data access and to avoid any market foreclosure or gatekeeping mechanisms.

04

Norms and standards can meet the ecosystem’s needs while ensuring vehicles’ cybersecurity.

The safety of the vehicle and its passengers and the **protection of access, data and system integrity** are **major and essential concerns** with the connected vehicle.

Unlike proprietary solutions which are heterogeneous by essence, **the use of standardised solutions allows systems to be interoperable, scalable and resilient** against the risks of malfunctions, faults or cyber threats.

The use of norms and standards, a common practice in the automotive world from the highway code to the approval of vehicles, is **not an obstacle to innovation or differentiation.**

Data security mechanisms for connected vehicle exist and are a priority for all players in the mobility ecosystem. They concern in particular:

- the principles of accreditations,
- authentication mechanisms,
- encryption of communication channels,
- the partitioning of essential systems and subsystems, intrusion detection,
- operation in fail-safe mode.

Relevant cybersecurity responses require a **cross-sectoral, cooperative and scalable approach.**

Only a standardised and secure technological solution, accessible and shared with as many people as possible, will be able to meet the motorists' needs, by:

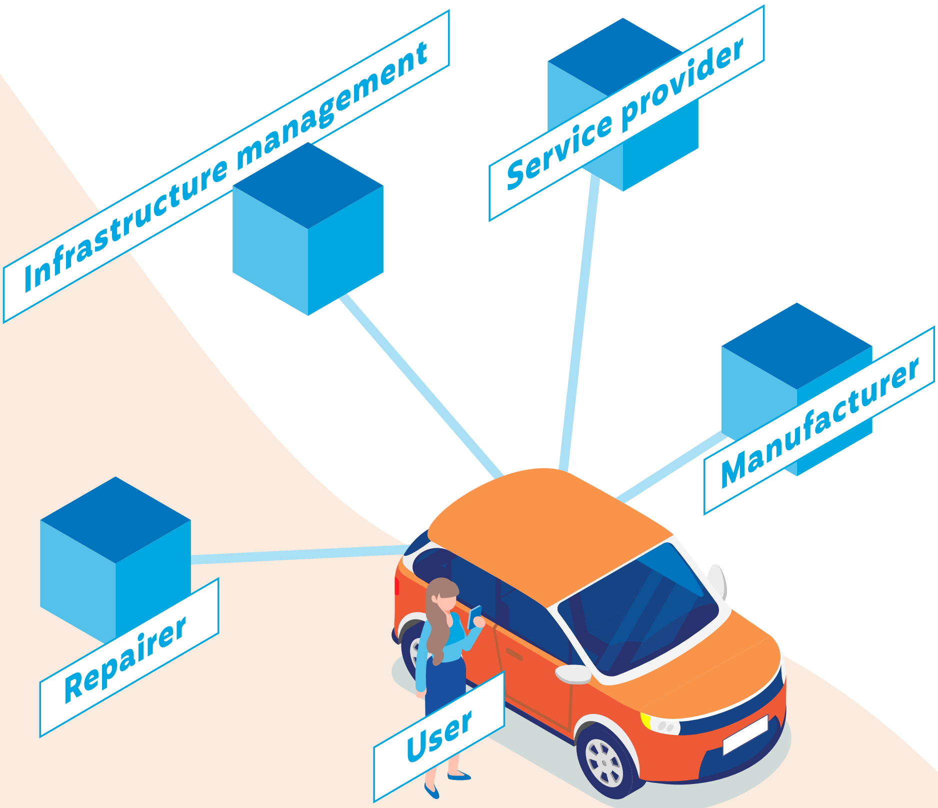
- offering more resilience to possible cyber-attacks;
- facilitating interoperability;
- promoting innovation; and
- limiting the risks of market asymmetry and monopoly.

The principle of open access to vehicle data is in no way contradictory with state-of-the-art cybersecurity practices.

05

Liabilities of the players in the automotive field are clearly identified and **remain unchanged for connected vehicles.**

Liabilities in the automotive sector are **well identified** between the various stakeholders, whether it is the manufacturer, users, repairers, service providers, infrastructure managers or any other player in the value chain. **Each player enters into his own contractual relationship with the vehicle's user** and under these conditions, his potential **liability is limited to breaches of his own obligations.** The digitisation of vehicles and associated services does not and should not change this fact, forcing everyone to operate with the utmost professionalism in order to preserve this framework.



Industry benchmarks

SERVICE OPERATORS' LIABILITY

Every vehicle must remain functional throughout its lifetime, for its intended use and for keeping it in perfect condition. To this end and to preserve user choice, any service operator must be able to freely access all the data it needs to provide excellent services, for which it accepts full liability.

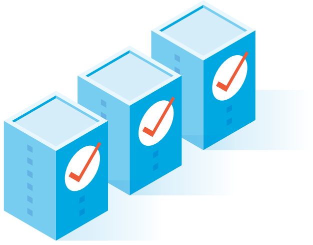
Regarding maintenance, any vehicle released on the market must allow full reparability by any operator. The entry into force in September 2020 of Regulation 2018/858 will contribute to this, in particular through the provisions relating to the obligations for manufacturers to provide the information necessary for repairs (Article 61).

However, this is not sufficient to guarantee access to all relevant vehicle data and resources, whether technical or not, and to the required interfaces.

More broadly, regulations must aim to provide simple, standardised and interoperable access to vehicle data so market players can responsibly operate homogeneous, efficient and multi-brand applications for their entire automobile fleet.

Just as a repairer's liability is incurred in the event of faulty work while replacing a part, it can be incurred for failure to comply with the rules and procedures for updating the software or implementing a function in the vehicle's electronic control units. **Consequently, digitisation does not modify in any way the chain of liability as we know it.**

More broadly, third parties are liable for neglecting or circumventing authorisation rules and access security rules, and for any abusive and non-compliant use of the data they may access. Therefore the signatories of this document fully subscribe to a responsible approach to respecting the safety rules in force.



Liabilities between the various connected vehicle stakeholders have always been well identified.

P

Technologies evolve rapidly, enabling new global-sized entrants to deploy dominant approaches. To preserve European competitiveness and sovereignty, upstream and downstream operators in the automotive industry are invited to develop common, shared and balanced solutions in the fundamental interest of users.

It is in this spirit that the signatories of this document came up with the following eight principles:

1 All data, whatever their nature and subject to user consent, must be **accessible in all fairness** to all **stakeholders. This also implies full transparency on the available data.**

2 Vehicle **users' choices** must be made truly effective through smooth processes for obtaining their **consent**.

3 Several access methods must be provided in order to preserve **technological neutrality** and avoid market foreclosures or gatekeeping mechanisms.

4 These **accesses must take place under identical technical and economic conditions for all players,** from the manufacturer to the independent operator. Financial conditions must be reasonable and compatible with the development of innovative digital services.

5 **Access to vehicle data and resources** (including the human-machine interface) **must be direct and, when necessary, in real time** (i.e., without delay).

6 Stakeholders must, as part of a business need, be able to access essential data stored in the electronic control units themselves.

7 **A cross-sectoral and cooperative approach** should make it possible to work towards a shared objective of vehicle security and cybersecurity.

8 **European regulations are essential,** particularly in terms of standards and interoperability, in order to establish these principles and neutral governance.

In addition, in order to maintain European sovereignty, strengthen the competitiveness of businesses and consumer protection, the signatories make the following additional recommendations:

1 Allow all European players to benefit from a world-class framework for innovation and development of information technologies, while respecting our ethical and competitive choices.

2 Foster cooperation between the various players in the ecosystem, especially by earmarking public R&I budgets for projects that consolidate the sector's upstream and downstream players.

3 Encourage all stakeholders to use data to help improve road safety, reduce CO_2 emissions, noise and pollutants, optimise energy consumption, remedy congestion and develop more accessible and inclusive mobility.

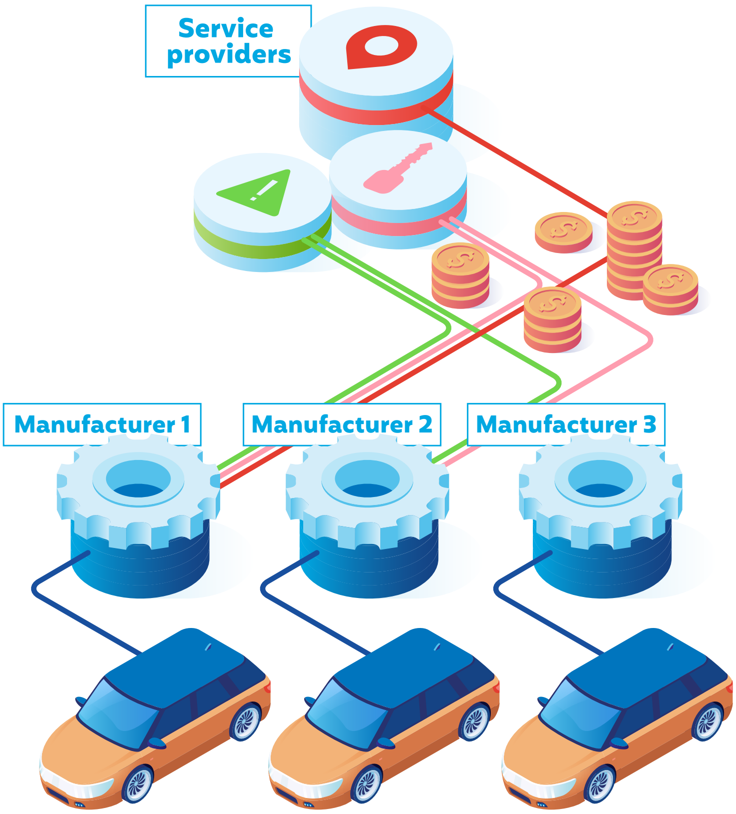
Advantages and disadvantages of the different technological solutions

A set of sensors and probes collect information on the vehicle's operation and condition (temperature, pressure, position, etc.). This information is then used by the various electronic control units to optimise the vehicle's performance and execute the driver's commands. These data circulate in the vehicle through embedded networks and, depending on the architecture and the communication strategies implemented, are also exported remotely to the manufacturer's proprietary servers for quality control, monitoring or product improvement (the vehicle) and associated services. Consequently these data can be accessed either in the vehicle itself, by connecting to the networks or embedded gateways (e.g., OBD port) or to the manufacturer's proprietary servers with, in this case, the constraint of only being able to access the data that the manufacturer has previously chosen to export to its servers. **Several access methods were identified during the work of C-ITS / WG6*.**

* To find out more, visit the European Commission website.

METHOD 1

The manufacturer's server or "extended vehicle"



General principle: The third party connects directly to each manufacturer's server (thus there will be as many connections to set up and operate as there are manufacturers) and submits a data transmission request. The server identifies the querier and transmits the requested information. This operation can be automated.

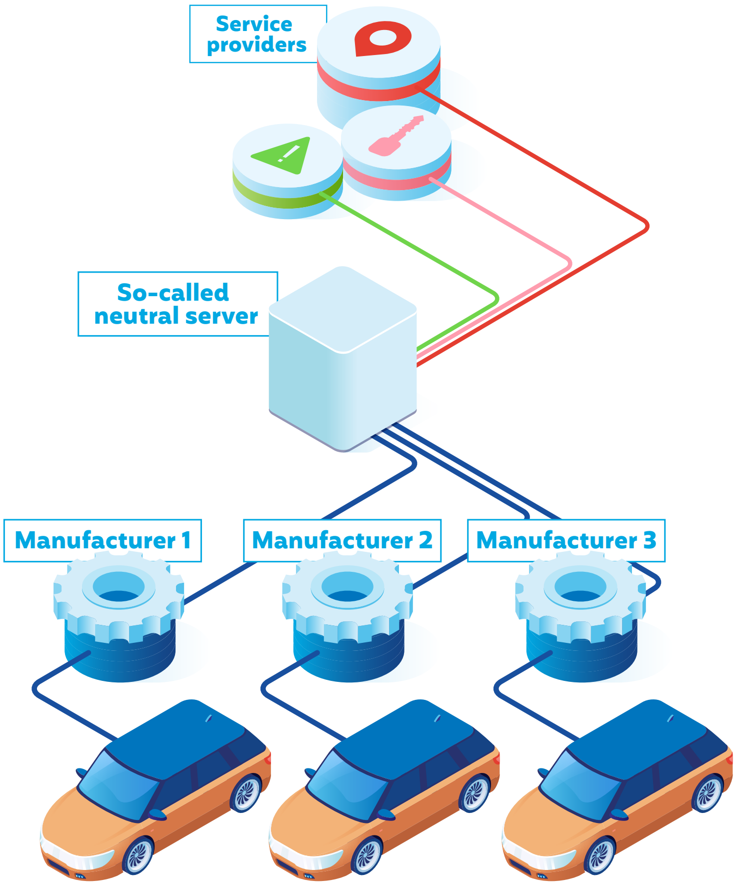
According to the principles recommended in this document (page 21), this access method responds to each of them as follows.

Principles' compliance scale

Data accessibility	⊗ **Partial, remote, by manufacturer**
Consent	⊗ **Intermediated, monetisation of personal data**
Market asymmetry	⊗ **Strong**
Cost of access to data	⊗ **Base cost + margin**
Real time access	⊗ **Risk of latency**
HMI integration	? **Low**
Electronic Control Unit data	⊗ **No, aggregated**
Security and Cybersecurity	✓ **Yes**

METHOD 2

The so-called neutral server



General principle: This is an additional server, set up «behind» the manufacturers' servers, that centralises the connections (thus there is only one connection to set up and operate for third parties). Created, set up and managed by state institutions, it is non-profit. This neutral server also serves the function of standardising data, managing access and billing transactions. Some servers can also preprocess the data by aggregating it or adding contextual information such as weather or traffic conditions.

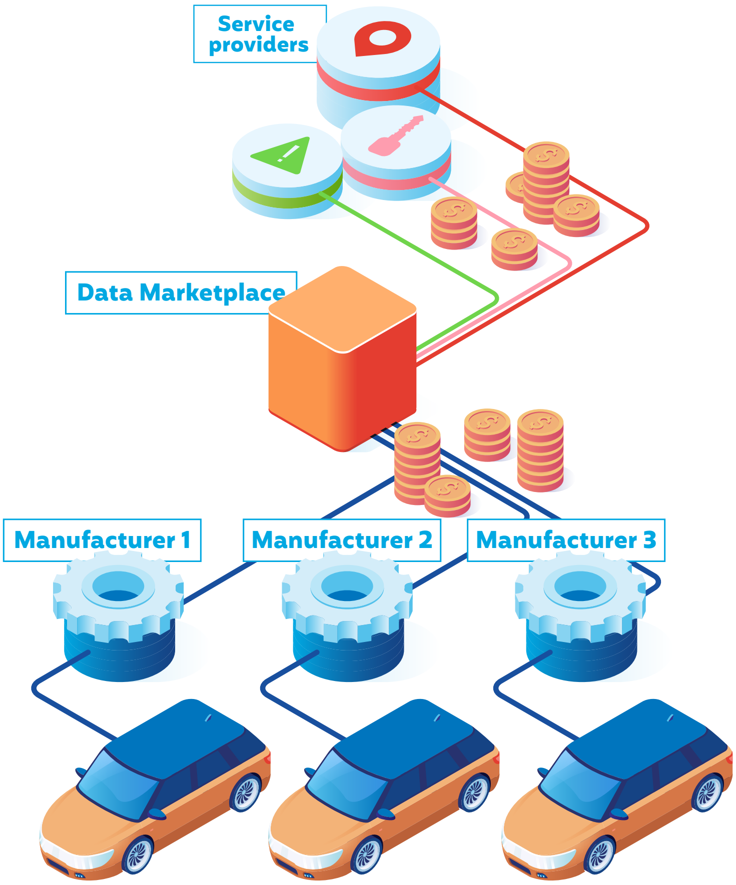
According to the principles recommended in this document (page 21), this access method responds to each of them as follows.

Principles' compliance scale

Data accessibility	? Partial, remote, harmonised
Consent	✓ Fluid
Market asymmetry	? Average
Cost of access to data	✓ Base cost
Real time access	✗ Risk of latency
HMI integration	✗ No
Electronic Control Unit data	✗ No, aggregated
Security and Cybersecurity	✓ Yes

METHOD 2 BIS

Data marketplace server



General principle: This is an additional server, set up «behind» the manufacturers' servers and which centralises the connections. Unlike the so-called "Neutral" server, this server is created and managed by private for-profit companies. This data marketplace also serves the function of standardising data, managing access and billing transactions. Some marketplaces can also preprocess the data by aggregating it or adding contextual information such as weather or traffic conditions.

According to the principles recommended in this document (page 21), this access method responds to each of them as follows.

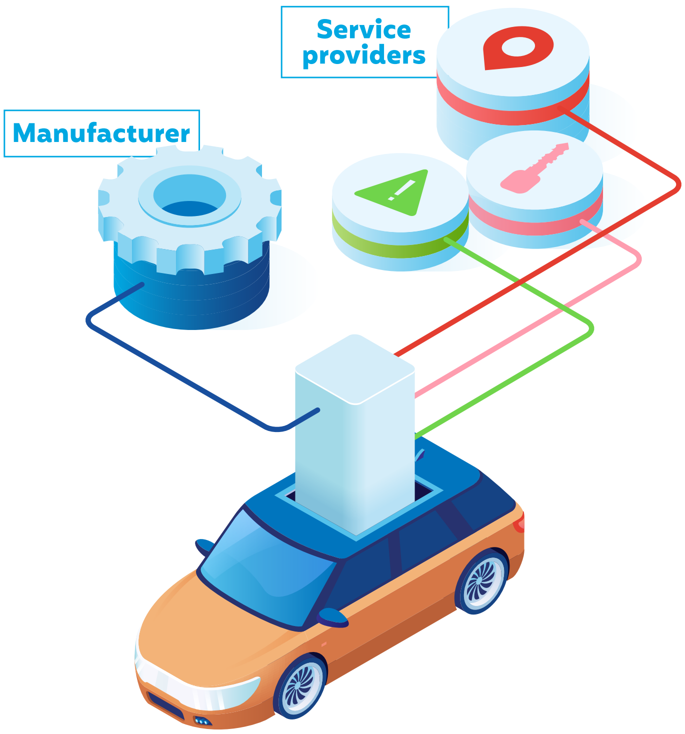
Principles' compliance scale

Data accessibility	? **Partial, remote, harmonised**
Consent	⊗ **Intermediated, monetisation of personal data**
Market asymmetry	? **Average**
Cost of access to data	⊗ **Base cost + margin**
Real time access	⊗ **Risk of latency**
HMI integration	⊗ **No**
Electronic Control Unit data	⊗ **No, aggregated**
Security and Cybersecurity	✓ **Yes**

? ✓

METHOD 3

Physical access by OBD or other port



General principle: Set up for pollution standards and regulated, it is little or poorly standardised both from a mechanical (location, spaces, etc.) and electronic point of view (the information available is not identical or expressed the same way depending on the brands and models of vehicles). However, the data are available immediately without an intermediary (no server). In this case the third party is responsible for collecting, interpreting and transmitting the information.

According to the principles recommended in this document (page 21), this access method responds to each of them as follows.

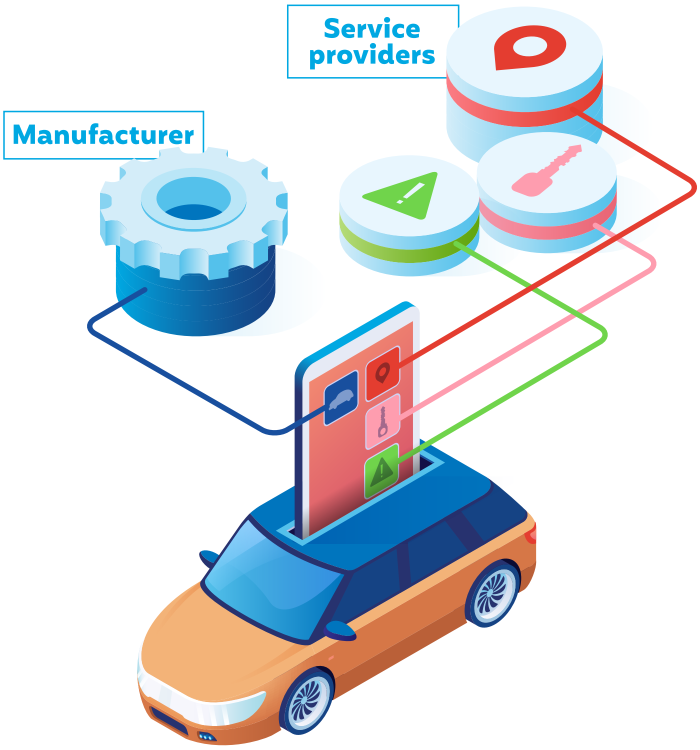
Principles' compliance scale

Data accessibility	? Partial, direct vehicle, standardised
Consent	✓ Fluid
Market asymmetry	✓ Low
Cost of access to data	? Base cost + equipment
Real time access	✓ Yes
HMI integration	✗ No
Electronic Control Unit data	✓ Possible
Security and Cybersecurity	✓ Yes

✓

METHOD 4

On-board application platform



General principle: The digitisation of vehicles is leading to the deployment of «embedded software platforms» (equivalent to the operating system of a computer or smartphone), a screen and controls (buttons and other features) so the user can interact with the system.

Just like a computer or smartphone, the applications installed on this platform make it possible to perform specific tasks and to provide access to functionalities, services or digital products (multimedia, contextualised information - fuel, traffic, services -, internet browser, messaging, etc.).

Therefore third parties can develop and run their own application in this system, thereby directly accessing the information available in the vehicle by exploiting existing resources and offering the user an experience comparable to what he would have with the features, services and products implemented by the manufacturer.

Finally, the vehicle's safety and integrity can be easily preserved by setting up specific accesses to data for each category of player (manufacturer, institutions, services, insurers, etc.) and by partitioning these accesses from each other.

According to the principles recommended in this document (page 21), this access method responds to each of them as follows.

Principles' compliance scale

Data accessibility	✓ **Direct vehicle, standardised**
Consent	✓ **Fluid**
Market asymmetry	✓ **Low**
Cost of access to data	✓ **Base cost**
Real time access	✓ **Yes**
HMI integration	✓ **Yes**
Electronic Control Unit data	✓ **Possible**
Security and Cybersecurity	✓ **Yes**

Notes

Notes

Notes

Automobile Club Association

Céline GENZWURKER-KASTNER
Legal and Public Policy Director
+33 3 68 00 38 00
cgenzwurker@automobileclub.org

38 avenue du Rhin
67100 Strasbourg

FFEA

Lionel NAMIN
Secretary General
lnamin@anea.fr

41 Rue des Plantes
75014 Paris

France Assureurs

Jérôme BALMES
Director, Business management & technology
Phone: +33 1 42 47 93 30
j.balmes@franceassureurs.fr

Hugues RIBIERE
European Affairs - Public Affairs Department
Phone: +32 2 894 30 99
h.ribiere@franceassureurs.fr

26 Boulevard Haussmann
75009 Paris - France

Mobilians

Yves RIOU
Director of the Inspection, Maintenance and Repair Division
+33 1 40 99 47 21
yriou@mobilians.fr

Dorothée DAYRAUT JULLIAN
Director of the Public Affairs and Communication Unit
+33 1 40 99 47 15
ddayrautjullian@mobilians.fr

43 bis route de Vaugirard
92197 Meudon Cedex

Mobivia

Bénédicte BARBRY
Director of Public Affairs and CSR
bbarbry@mobivia.com

Stéphane DERVILLE
Director of Innovation Projects
sderville@mgts.com

511/589 Rue des Seringats
59262 Sainghin-en-Mélantois

Sesamlld

Anne-Claire FOREL
Secretary General
acforel@sesamlld.com

Immeuble ARC en Ciel
17 Rue de la Vanne Batiment B
92120 Montrouge

SNSA

Claude SARCIA
President
claude.sarcia@ima.eu

59 Rue des Petits Champs
75001 Paris

UFE

Mathias LAFFONT
Business, Mobility and Construction Director
Tél. : +33 6 65 54 95 84
+33 1 70 60 76 59
mathias.laffont@ufe-electricite.fr

Viktoriia LEONENKO
Project leader for economic and mobility studies
viktoriia.leonenko@ufe-electricite.fr

3 Rue du 4 septembre
75002 Paris

FEBRUARY 2022

Graphic design: Vanessa Vansteelandt - Illustrations: Shutterstock