

ACCESS TO EXTENDED VEHICLE DATA

1. CONTEXT

This document presents the agreed position of the French Automotive Industry on access to extended vehicle data (ExVe). It is the result of work requested during the Automotive Technical Committee of 10 March 2020 to specify the concept of the extended vehicle and the conditions for an effective dialogue, respecting the needs, rights and obligations of the many sectors and stakeholders concerned.

2. POSITIONS REGARDING ACCESS TO CONNECTED VEHICLE DATA

The PFA acknowledges the need for a common language within the Industry regarding the types of access to extended vehicle data. It confirms that the 2 accepted means of access are local access and remote access, which are defined as follows:

- Local access: access to a vehicle's data and functionalities through an interface located in the vehicle that has been approved¹ by the manufacturer or that complies with the requirements laid down by him in the underlying contract.
- Remote access: access to a vehicle's data and functionalities through an off-board interface. This type of access is subject to the terms of use defined by the manufacturer.

Direct access, as defined in this document, is not recommended by the Industry, and was not covered here.

The PFA confirms that within the extended vehicle:

- Remote access as set out in the ISO20078 series of standards meets data access needs; and
- Depending on the use case and the context, a local access solution (as may be available on the market like Android Automotive²) or such a solution combined with remote access may be relevant.

The combination of remote and local access covers all service use cases, by providing access to relevant vehicle data and functionalities.

The methods of access implemented in the extended vehicle are under the responsibility of the manufacturer, in accordance with the principles set out in the ISO 20077 standards. The method of access shall be determined by the manufacturer, with the access seeker, for the sake of the performance of the ecosystem and to ensure its optimisation (service/vehicle/infrastructure).

The PFA notes that the existence of a pre-defined list of data is less useful than having a common terminology to share the definition of the data and use cases and to understand the data sets and APIs provided by manufacturers.

The PFA supports a process for the analysis of an access request that is known and shared. It begins at a manufacturer's entry point and allows for a request to be processed in a way that guarantees to both parties – access seeker and manufacturer – a collaboration under equitable, fair and reasonable conditions, and which will factor-in their respective interests.

¹ *Approved by the manufacturer: agreement provided by the manufacturer to a third-party service application installed in the vehicle, allowing for access to the vehicle's data and functionalities in compliance with type-approval, cybersecurity, security, data protection and liability requirements.*

² *Solution defined by one of the use cases of the working group.*

2.1. Description of the methods of access to extended vehicle data (GT1)

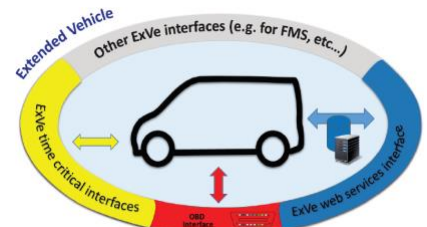
In order to use a common language within the Industry regarding the methods of access to vehicle data, members of the Industry have reached a consensus on a set of definitions and descriptions.

Definitions of the types of access to vehicle data

- Local data access: access to a vehicle's data and functionalities through an interface located in the vehicle that has been approved³ by the manufacturer or that complies with the requirements laid down by him in the underlying contract.
This type of access must be designed and validated during the vehicle's development phase to ensure compliance with relevant type-approval, performance, cybersecurity, security, data protection and liability requirements, and is subject to the terms of use defined by the manufacturer.
- Remote access to data: access to a vehicle's data and functionalities through an off-board interface. This type of access is subject to the terms of use defined by the manufacturer
- Direct access to data: gathering of vehicle data directly through the vehicle's internal electronic architecture without the manufacturer's supervision.

Description of the interfaces of the extended vehicle

The standardised concept of Extended Vehicle (ExVe) defines a set of rules and basic principles that must be complied with when developing the ExVe, provides a methodology for the exchange between the manufacturer and the service provider and defines interfaces for local and remote access to the vehicle, depending on the relevant use case. The extended vehicle standards describe 4 interfaces:



- OBD interface (red): local access enabling the interaction with the vehicle for diagnostic operations through a device plugged in the OBD connector, in a repair facility.
- Web services interface (blue): remote access enabling access to data of a vehicle available on the manufacturer's server, through a standardised protocol.
- Time-critical interface (yellow): local access enabling access to a vehicle's data for communications that require a low latency. The "critical" aspect refers to the fact that this interface is used for use-cases known by the manufacturer and which relate to road safety (e.g. C-ITS).
- Other interfaces (grey): local or remote access enabling an access to vehicle data through various physical or digital interfaces such as USB, Bluetooth, Wi-Fi, cellular network, CPL (power line carrier), API (programming interface for proprietary applications or third-party applications such as Android Automotive).

Assessment of an access solution

The choice of a given solution among those which may fulfil the same use-case is based on criteria described in the analysis below.

The use-cases studied highlight the fact that there are multiple solutions combining local and remote access which may fulfil the needs of a given service, from beginning to end, from data upload to the provision of the service to the end-user. This finding was confirmed in the 10 generic, non-exhaustive use cases reviewed by the working group. To ensure global performance and a balance between the quality of the data, the quality and fullness of the service, implementation and operational costs and the time required to provide the data or the solution, the method of access shall be determined by the manufacturer, in agreement with the access seeker. There is therefore no single solution for a given use case.

³ Approved by the manufacturer: agreement provided by the manufacturer to a third-party service application installed in the vehicle, allowing for access to the vehicle's data and functionalities in compliance with type-approval, cybersecurity, security, data protection and liability requirements.

2.2. Analysis of the Michelin and Plastic Omnium use-cases

Michelin case – Tyre health (WG 2.1)

This use case relates to the implementation of a tyre maintenance service that can be developed through remote or local access, with a value proposition for the end user that can be summarised as follows:

- Prevent a slow tyre leak very early on,
- Provide a range of solutions to this issue.

The solutions were examined as part of an implementation in the ecosystems of the Renault and Stellantis Groups. They illustrate different modes of interaction with the user depending on the solution chosen.

Plastic Omnium Case – SCR (WG 2.2)

The 3 Plastic Omnium-Stellantis use cases were the following:

- Use case 1: predictive maintenance of the SCR system (B2B),
- Use case 2: AdBlue refuelling at a station (B2B2C),
- Use case 3: reduction of the SCR system's energy consumption (and thus of CO₂) in cold zones (B2B).

Use cases 1 and 3 could not be implemented in the allotted time, with the constraint of not modifying the vehicle (use case 1: data in the SCR ECU, not available on the communication architecture; use case 3: no write access possible on an actuator of the pollution control system).

Use case 2 on AdBlue refuelling was carried out through remote access via a manufacturer's server using the ExVe methodology with existing tools and definitions. It also included the interaction with the vehicle driver.

Sub-group 2.2 thus demonstrated the end-to-end real application of the ExVe methodology in remote access via a web server. WG 2.2 demonstrated that the partner / manufacturer collaboration can extend services provided to customers, as well as to the manufacturer and to suppliers, for example in the context of quality improvement actions.






The elements relating to the solutions analysed are presented in the tables below :

PROPOSED RESPONSE TO THE REQUIREMENTS OF THE MICHELIN USE CASE

Local Access/Android Automotive (Renault)		Remote Access /ExVe web interface (Stellantis)	
Renault group's implementation proposal is based on Google's Android Automotive technology. Through a certain number of APIs made available by the manufacturer and subject to authorisation, it allows for access to vehicle data through "local access", the installation of an application in the vehicle to perform on-board calculations and the exchange of information with an external server (e.g. tyre size). It also allows for access to the human-machine interface in the vehicle's infotainment system.		Stellantis group's implementation proposal is based on the remote processing and uploading of the necessary data to the manufacturer's servers, based on the ExVe's ISO standards. These data are then used by the manager of the service on its own servers to perform the calculations relevant to its service. Interaction with the user is done through their mobile phone (with or without screen mirroring) or via information pages displayed on the vehicle's entertainment system.	
DATA AVAILABILITY			
In both cases, data was partially available. In a real case, data would be made available by the manufacturer based on the dialogue he would have had the service provider.			
Intellectual property: data sharing through these solutions ensures that every service provider has access to the data available on all vehicles and protects the intellectual property of each partner.			
GLOBAL COST			
Advantages		Disadvantages	
Limitation of data communication costs for use, remote storage and minimisation of the risks associated with the exposure of data on different servers.		Capacity impact: the on-board hardware platform that hosts the local access must be able to support additional services during the lifetime of the vehicle, which results in additional costs, depending on the choice of the manufacturer and may be different depending on the precise model of vehicle.	
		Advantages The telematics box need not be oversized to support applications. A single upload of the data to the server can serve several services, subject to the consent of the data subject.	
		Disadvantages Environmental impact due to the large volume of data collected: it may be necessary to set up a suitable device to temporarily store and filter the data before sending it.	
DEVELOPMENT KIT			
Both manufacturers provide a software development kit to service developers. This kit makes it possible to use systems that will allow the service provider to interact with the user, via a smartphone or the vehicle's infotainment system. The choice of providing remote, local or hybrid access is up to the manufacturer.			
The Renault solution is based on "Android Open Source Project" (AOSP) technology, offering a large ecosystem, and providing a development and test kit (Android SDK) which allows users to: <ul style="list-style-type: none"> • Ensure compliance with the manufacturer's specifications regarding the data that is accessed and the methods of access (e.g. read-only access in the Michelin use case analysed here), • Facilitate the work of the service developer. Once they have accepted the general conditions of use defined by Renault, the service developer may freely develop and test their service offers by limiting their interaction with the manufacturer (interaction is nevertheless required to define the business model, the types and volumes of relevant vehicles, and supply the signatures so that the application may access specific manufacturer data). 		The development kit is based on a solution which itself is based on international ISO standards (ExVe) and on market standards (REST, OpenID, OAUTH2, etc.), which are widespread and thus widely available.	
HMI			
The solutions enable the seamless integration of the service into the cockpit's HMI, thus preserving the user experience designed by the Manufacturer, and complying with the display prioritisation and driver distraction policies.		Remotely, display is possible on off-board devices (e.g. smartphone, tablet).	

DEPLOYMENT	
Several means of deploying the service are possible, depending on the needs: <ul style="list-style-type: none"> • Via the Play Store application catalogue (when the vehicle is appropriately equipped), or • Via Renault's remote update infrastructure (available on all vehicles equipped with Android Automotive), 	The service provider is free to choose the means of deploying its service and the application platform (market store, specific brand store, etc.).
SERVICE QUALITY	
In order for the system to function correctly in all circumstances (borderline cases), the service provider must carry out intensive "stress" tests, in collaboration with the manufacturer.	
<ul style="list-style-type: none"> • The system dynamically manages the services that have been allowed to operate simultaneously, based on available resources. • If the system is saturated, it may need to temporarily deactivate a service to preserve those established as priority services by the manufacturer. 	Service continuity is ensured by the service provider's IT infrastructure on which the application is installed. This allows scalable sizing over time to support an increase in the number of application and of their computing power requirements.
SCALABILITY (ability to accept new services)	
Local access scalability is limited by the capacity of the hardware platform that hosts it (RAM, Flash, CPU). This capacity is defined by the manufacturer, it is fixed for any given vehicle, and may be different depending on the Manufacturer, the vehicle type or its level of equipment for a given vehicle range.	The solution enables the creation of services without interfering with the capacity of on-board resources, which by definition are limited. This allows a large number of applications to run concurrently.
CYBERSECURITY, ATTACK RISKS	
<ul style="list-style-type: none"> • Renault guarantees a level of protection against cyber-attacks on par with "the level of market standards" by implementing solutions that satisfy the requirements of UN Regulation R155 on Cybersecurity. • The manufacturer remains liable for the consequences of an attack, but may, where relevant, seek redress from the service provider suspected of being the vector of the attack. 	<ul style="list-style-type: none"> • The manufacturer complies with the applicable law and applies state of the art market standards regarding the protection against cyber-attacks. • Furthermore, off-board access via the manufacturer's server provides an additional protection layer which limits the risk of direct cyber-attacks against the vehicle. • Finally, as applications are not deployed on-board the vehicle, there is no risk from this angle.
USER INFORMATION and DATA PROTECTION	
The protection of privacy must be ensured by a precise categorisation (controller, subcontractor, co-manager) of each actor (the manufacturer, and the supplier for the part of the service for which he is in contact with the end user).	
The definition of the roles of each actor must be clearly specified as it is integral to the technical solution. The user is informed, directly through the infotainment system interface, of the list of data leaving the vehicle that are necessary for the proper functioning of the service, depending on the solution.	The Manufacturer's and the service developer's systems are distinct. The roles are therefore predefined by design. The ExVe web interface system ensures that the service provider can only have access to data to which he has been granted access.

PROPOSED RESPONSE (Stellantis) TO THE REQUIREMENTS OF THE PLASTIC OMNIUM USE CASE

Remote /ExVe web interface (Stellantis)	
<p>The tests have shown that the performance of an ExVe system with its Web interface allows Plastic Omnium to perform calculations and interact with the customer by displaying messages on the on-board HMI (vehicle infotainment system), via the customer's smartphone and the Car Easy Apps protocol, within a timeframe that matches the performance expected for the service (despite the fact that the POC solution was not enhanced). The POC demonstrated the end-to-end, real-world use of the ExVe methodology in remote access via a web server.</p>	
 DATA AVAILABILITY	<p>Not all internal vehicle data is available, in particular those which are internal to an ECU or on a private CAN between 2 ECUs (use case 1). Making them available would require modifying the architecture but this process limited by the resources available in the architectures, which are scaled and limited (network saturation problem, CPU power, memory resources, etc.). A one-off access upon request could solve some limitations, as long as the resources the vehicle allows for it. Specific analysis and developments, provided in a contract, would be required to fully implement these three services. Depending on the need expressed by the partner, it may be necessary to take this into account as early as possible in the development of the vehicle in order to anticipate the needs and possible impacts on the electrical architecture and its communication networks, with a view to make additional data available. During the analysis of the request, data exchanges between the manufacturer and the service provider must also be limited to what is strictly necessary to ensure that the choice of the location of the calculations is optimal, i.e. on the ExVe's on-board or off-board systems, or on the service provider's cloud. Intellectual property: data sharing through the ExVe web interface ensures that every service provider has access to the data available on all vehicles and protects the intellectual property of each partner.</p>
 DEVELOPMENT KIT	<p>A more detailed description of the data uploaded on the platform would give a better understanding of its potential for use. Use case 3 was not implemented due to the fact that remote actions on the vehicle's pollution control actuator could not be implemented (time allotted to the development of the POC, liability issues and also potentially inviolability issues, including cybersecurity and road safety). In addition, the architecture developed must make it possible to implement feedback to the driver, allowing for a certain level of interaction with the vehicle via the manufacturer's server, while respecting the principles and safety rules established by the manufacturer. The need for customer consent to implement these extended services or functionalities must be noted.</p>
 QUALITY OF SERVICE/SCALABILITY (ABILITY TO ACCEPT NEW SERVICES)	<p>The remote solution allows each service provider to size the resources needed on its own servers based on its applications computing power requirements. In addition, this allows for a scalable system that is not limited in resources.</p>
 CYBERSECURITY, ATTACK RISKS	<p>The manufacturer complies with applicable law and implements state of the art standards regarding the protection against Cyber-attacks. Furthermore, off-board access via the manufacturer's server provides an additional protection layer which limits the risk of direct cyber-attacks against the vehicle. Finally, as applications are not deployed on-board the vehicle, there is no risk from this angle.</p>
 USER INFORMATION and DATA PROTECTION	<p>The protection of privacy must be ensured by a precise categorisation (controller, subcontractor, co-manager) of each actor (the manufacturer, and the supplier for the part of the service for which he is in contact with the end user). The Manufacturer's and the service developer's systems are distinct. The roles are therefore predefined by design. The ExVe web interface system ensures that the service provider can only access to data to which he has been granted access.</p>

2.3. Implementation of a pre-established set of data – success conditions (GT 3)

Essential principles of data sharing to allow for the development of services focus more on sharing the description of data and use cases and the comparison of the data and API available from the manufacturers (notion of Manufacturer's catalogue), rather than on the existence of a pre-established list.

The analysis of connected data carried out by ACEA, CLEPA and the analysis carried out by GENIVI highlight the difficulty of describing data and providing a common definition with the same level of precision.

Beyond the volume of data and the groupings proposed by type or by functional origin of the vehicle, the debate on the choice of data to factor-in remains difficult. The need for stakeholders to share an understanding of the nature of the data, their conditions of publication and use and their characteristics and availability among the manufacturers appeared early on.

In this context, it appears difficult to establish a definite list of data to be published in a standardised format common to all stakeholders.

On the other hand, it seems desirable to standardise the description of the characteristics of these data to facilitate their use by the actors of the ecosystem. This would streamline data sharing and facilitate the activities necessary for their proper use. The recommendation is therefore to initiate above all initiatives to define a common framework for the description of vehicle data.

A clear understanding by stakeholders in the value chain of the description of the data is a prerequisite to the establishment of a common list of data.

The discussions showed that it was also necessary to discuss the purpose and use of data so that all stakeholders could agree on a format and a content adapted to their need. This notion of purpose is naturally associated with the notion of API (Application Programming Interface) and can provide context when sharing data or a set of data or function(s).

This principle, which groups together the characteristics of the data, the methods of access and sharing, seems better suited to sharing between access seekers and data providers. Furthermore, as it adds a level of abstraction, it provides guarantees for the operation and the security of the vehicle and of data access. It applies both to remote and local access.

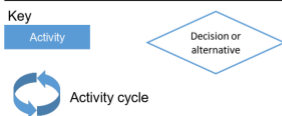
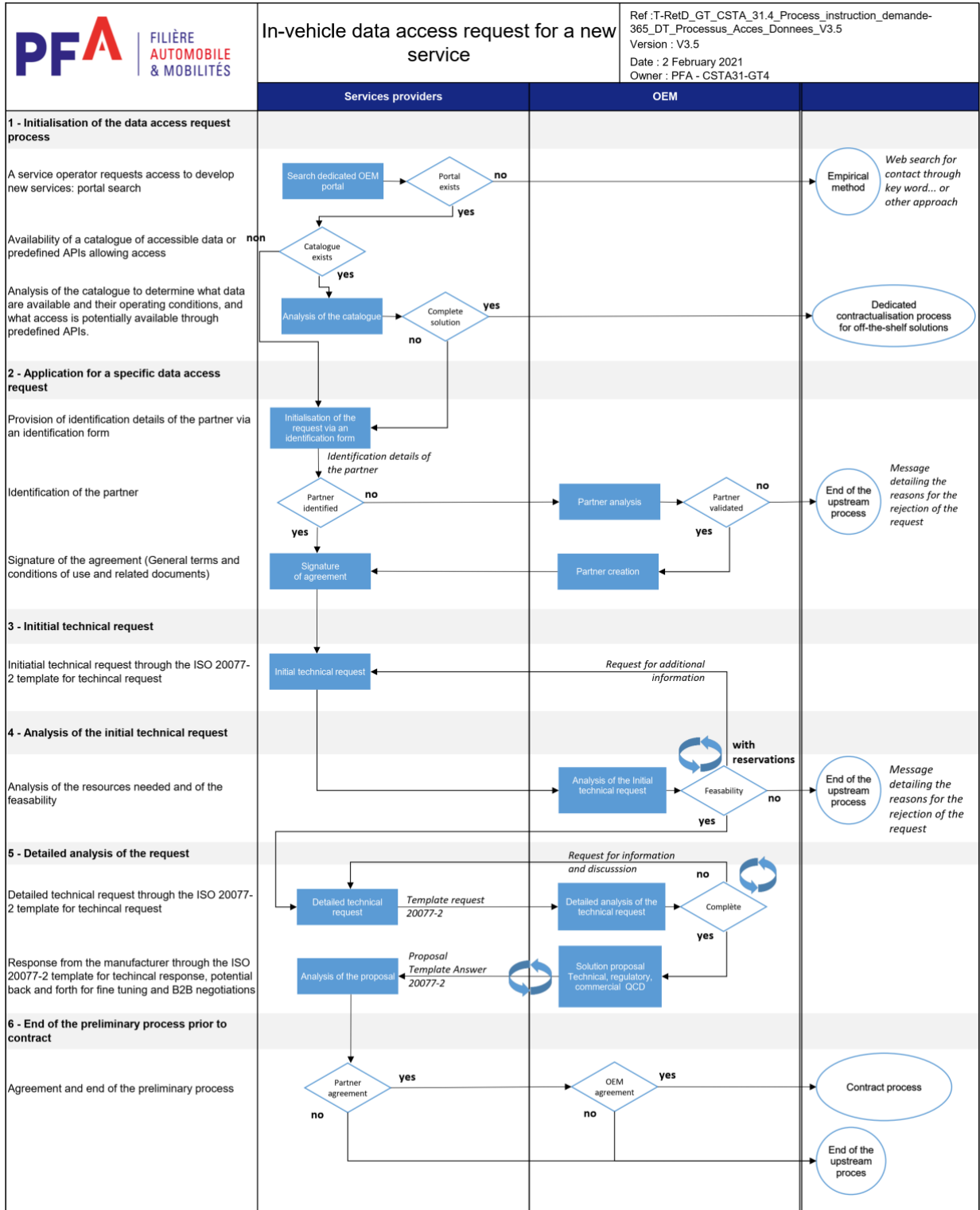
2.4. In-vehicle data access request for new services (GT 4)

Vehicle data access requests must be processed through a collaborative process that begins at the manufacturer's portal. The objective is to guarantee to both parties, the access seeker and the manufacturer, a collaboration under equitable, fair and reasonable conditions, and which will factor-in their respective interests.

The process described on the next page provides an overview of how this collaboration should take place.

Particular attention must be paid to the General Conditions of Use of the portal, which may not be amended, and in particular to the confidentiality clauses (Non-Disclosure Agreement) and general terms of cooperation between the parties:

- Terms of the collaboration and monitoring of the activities
- Commitment to comply with personal data protection rules (GDPR),
- Commitment to respect intellectual property rights
- Reciprocal commitment not to use the information exchanged for purposes or activities other than those necessary for the collaboration
- Measures to be taken in the event of an infringement by one of the parties or in case of a dispute.



2.5. Context and legal perspectives regarding access to data (GT 5)

A set of rules applicable today at French and European levels must be taken into account by manufacturers and service providers, which relates to several aspects: privacy and personal data protection, security and safety, including cyber security, economic, competition and liability rules.

- Privacy and data protection rules: Regulation 2016/679 of 27 April 2016 (GDPR) and French Act n° 78-17 of 6 January 1978 amended Information Technology, Data Files and Civil Liberties (Data protection, data minimisation, stakeholders' roles and responsibilities).
- Connected vehicles data access security and cybersecurity: to be taken into account for the legal compliance of undertakings pursuant to several provisions (GDPR for security breaches, NIS directive regarding the reporting of cybersecurity breaches, LOM ordinance bill).
- Economic, competition and liability aspects: To be considered:
 - Article 32 of the French Mobility Act provides for non-discriminatory access to relevant vehicle data in B2B, in particular for repair, maintenance and innovative vehicle-related mobility services.
 - Commercial conditions pursuant to the French Civil and Commercial Codes regarding the confidentiality of partnerships as well as respect for intellectual property and liability rules.
 - Rules applicable to application publishers and to platforms for services using downloadable applications in the vehicle.

Some of these rules are provided for by French legislation while others are set out in soft law (e.g. CNIL connected vehicle compliance package, which helps applying this legislation).

The main regulatory initiatives which the Commission will present by the end of 2021 and later are the following:

- The data strategy with the "Data Governance Act" and the "Data Act"
- The digital services strategy with the "Digital Services Package",
- The strategy on cybersecurity (e.g. "NIS 2")
- A proposal for a regulation on access to connected vehicles data.