Submitted by the expert from CITA

Informal document **GRVA-12-11**
12th GRVA, 24-28 January 2022
Provisional agenda item 5(c)

Access to in-vehicle data

I. Context

A. Technological developments

Introduction

1. Software updates over-the-air (OTA) on-road vehicles can have a significant impact on both safety-relevant systems and the emissions behaviour of the vehicles, as they change the corresponding systems during the life cycle of the vehicle. The current status of the relevant software identification, including its information on calibration, is initially only available in the vehicle and is then forwarded to the OEM backend. However, a feasible and secure solution for the exchange of relevant data with public authorities for the execution of sovereign tasks in the interest of society has not yet been established.

2. Considering the high degree of reliability of vehicle data for the application of sovereign use cases by authorities and entrusted services, a regulatory framework with binding requirements for remote access to in-vehicle data shall ensure independent and trusted access.

3. The objectives of this paper are:

   i. To assess the importance of in-vehicle data for sovereign tasks of the contracting parties for a safe, clean, and sustainable transport system;

   ii. To set the key principles to meet these tasks even better in the future;

   iii. To provide an extensive analysis of existing legal approaches around the globe and technical models to get access to in-vehicle data;

   iv. To identify challenges and opportunities;

   v. To provide policy recommendations.

Importance of data for a safe, clean, and sustainable transport system

4. An independent access to in-vehicle data is required to ensure whole life vehicle compliance, which addresses the appropriate individual coverage of safety and emissions relevant functions of the specific vehicle under test.

5. Future vehicles will be enabled to operate in automated driving modes (SAE Level 3, 4, 5) and not only with ADAS functions. The driver will no longer be available as a backup solution if technology fails.

6. Connectivity will enable these vehicles to receive safety and emissions relevant updates during their life cycle, and the vehicle will not always remain the same as when it was introduced during the type-approval and after the first registration. As already mentioned, the new (safety-relevant) functionality will be based on modified software updates/upgrades, especially over the air.

7. The range and characteristics of available data and functions must respect the technological status of the vehicle. The access point should be the respective telecommunication provider commissioned by the manufacturer.

Drawbacks of the current situation

(a) The urgency of the situation

-Reliability and trustworthiness for the application of sovereign tasks for authorities and technical services are of vital importance. The first vehicles with automated driving systems[1] (ADS) will shortly be available for consumers, and yet it is still only the OEM who can check how the ADS behave "in the field". Simultaneously, there is neither a technical nor legal solution to ensure that an independent third party can verify the safe operation of these systems. Moreover, other sovereign use cases, such as accident analysis, research, or prosecution, are equally not covered by any existing or foreseen legislation.

-Besides the challenges for sovereign use cases under the current situation, the user of the vehicle does not know how the data he generates by using his/her car, with whom this data is being shared, and he/she is not able to choose a potential different service provider.

(b) Overall (B2B only)

-At least at the European level, the access to data discussion focuses merely on B2B situations. There is no governance model for the performance of sovereign use cases by authorities and technical services. So far, this aspect has not been addressed. Neither in the discussions about the sector-specific in-vehicle data discussion nor in the horizontal Data Act.

(c) For the Authorities and vehicle inspection organizations

-State authorities, Technical services, vehicle inspection bodies, accident research bodies etc., must have assured confidence that data from the vehicle is original and unmodified. The highest level of tamper protection should be achieved by using appropriate high-security encryption of the data. Current technical specifications of OEM backend servers do not cover these critical requirements. The solution should be an approach ensuring that the data, which was sent by the vehicle, is complete and – as far as technically possible – has not been modified. To analyze it, the data history is necessary. During PTI, test procedures on safety status and legal status of the vehicle are carried out, and this process requires information about the data history of the individual vehicle, e.g. detection of a sensor or function failure, report of near misses, etc. Thus, the actual status of hardware/software needs to be known for implementing appropriate PTI testing.

B. Definitions

8. "*Trust centre*": means an independent body that performs access control for vehicle data. Both identification of participants in a transaction and authorization of access. It is entrusted by national/regional authorities.

9. "*Data trustee*": means a body that collects or processes data from vehicles (e.g. software information) of different manufacturers and suppliers and makes it available to authorized third parties, e.g. for Roadworthiness testing, DSSAD, on-board fuel consumption monitoring, field monitoring and other use cases.

10. "Sovereign tasks": means tasks that are performed by sovereign public bodies and authorities. This could, for example, be in the field of roadworthiness testing, road safety and environmental compatibility.

[1] The first passenger cars with ADS are in Europe officially homologated.

C. Specific input in the context of approval/assessment of vehicles

11. Key principles

Access to vehicle data must be:

(a) Fair

The access to vehicle data, costs and benefits are regulated in a reasonable and non-discriminatory manner.

(b) Non-discriminatory

In-Vehicle Data must be made available to everyone on the market in the same and easy way, without limitations, filters, time delays or any other discriminating factors. This also relates to personal data if the owner of the data (e.g. driver or vehicle owner) actively gives his permission to access the relevant data.

(c) Reasonable

Data must be made available to the market for an appropriate price and effort. Data used for sovereign activities must be made available free of charge.

(d) Cybersecure

Data protection must be assured at all times. Every participant in the chain of saving, transmitting, or receiving data must follow the state of the art cybersecurity standards and rules.

(e) Neutral

Handling of access rights to data should be the responsibility of a neutral body. Also, data storage of – especially – critical data, which could have a safety, insurance, tax, or legal relevance should be handled redundantly by a neutral body.

(f) Trustworthy

Data is free from any obfuscation or manipulation.

(g) Independent

Handling of data and data access is not influenced by business or other interests.

(h) Available for sovereign tasks

Member states are responsible for several sovereign tasks, which depend on in-vehicle data. This data must be made available for all these tasks, regardless of who the authorities entrusted with the task itself. Examples of sovereign tasks:

- Vehicle taxes,
- Traffic management and road safety,
- Vehicle type approval (vehicles change over their lifetime, e. g. due to software updates, type approval will become dynamic and a lifelong process, and others)
- Market surveillance,
- Field monitoring (e.g. Emissions, the performance of automated driving functions, and others)
- Research (e.g. road safety, accident research, traffic management, and others)
- Roadworthiness testing, e. g. Periodical Technical Inspection (PTI),

- Liability (e. g. DSSAD: who was responsible for driving the automated vehicle, …)
- …

III. Current developments and solutions proposed

A. National views (as understood by CITA)

12. The Federal Republic of Germany's view on access to vehicle data

CITA is aware of the government coalition paper, Germany wants to use the potential of data for all by supporting the development of data infrastructures and launching instruments such as data trustees, data hubs and data donations together with business, science, and civil society. The aim is to improve access to data, especially to enable start-ups as well as small and medium enterprises to create new innovative business models and social innovations in digitization. A data institute shall drive data availability and standardization and establish data trust centre/ data trustee models and licenses. For local authorities, they plan on creating access to data from companies under fair and competitive conditions, insofar as this is necessary for the provision of their sovereign use cases. They want to strengthen standardized and machine-readable access to self-generated data for all those who have contributed to the creation of data. With a data law, they want to create the necessary legal basis for these measures. Germany promotes anonymization techniques by creating legal certainty through standards and introducing criminal liability for unlawful de-anonymization. They plan on introducing a legal right to open data and improving the data expertise of public agencies.

13. The People's Republic of China

CITA is aware of three known areas:

(a) Electric driven vehicles (GB/T 32960.2 + GB/T 32960.3)

For electric driven vehicles, it is foreseen to send data of a real-time monitoring system (RTM) directly to test centres on both provincial and country levels. The current situation is that the data are sent first to the server owned by the manufacturer and afterwards (but in "real-time") transferred to the server of the test centre. The RTM should transfer, besides GPS data also vehicle data like acceleration, rotational speed, battery temperature, voltage, and others. All-Electric vehicles should be homologated for this RTM system.

(b) Truck for transport of dangerous goods and coaches (AQ3003 + AQ3004)

Trucks for the transport of dangerous goods and coaches have to be equipped with a system that should send data (e.g. speed, collision information, GPS) to a Chinese state supervision platform. This is mandatory for all trucks for the transport of dangerous goods and coaches. It includes retrofitting such a system to older vehicles.

(c) EDR/DSSAD (GB 7258)

From January 2022 new produced private cars must be equipped with EDR (Event Data Recorder). The data like speed, acceleration and collision should be stored properly. DSSAD is still based on the manufacturers' own decisions.

14. United States of America[2]

CITA is aware that several administrations have issued guidelines on many new vehicle technologies and defining state and federal responsibilities, but so far, they have not addressed vehicle data access concerns for independent third parties. The following legislation must be considered:

- 1990 Clean Air Act Amendments: Assured repairers the same emissions service information that franchised new car dealers receive.
- 2015 FAST Act: Vehicle owners were guaranteed access to a car's Electronic Data Recorder. For all other vehicle generated data, owners are at the mercy of manufacturers.
- In 2017 the Senate unanimously adopted a bi-partisan autonomous vehicle data access amendment to the Senate autonomous vehicle bill. However, federal autonomous vehicle legislation was not enacted in the 115th Congress, and the amendment, along with the House and Senate autonomous vehicle legislation considered by Congress, died at the end of 2018.
- On June 29th 2021, the National Highway Traffic Safety Administration issued a Standing General Order requiring manufacturers and operators of vehicles equipped with SAE Level 2 advanced driver assistance systems (ADAS) or SAE Levels 3-5 automated driving systems (ADS) to report crashes that occur on U.S. public roads.

B. Regional views: European Commission

15. DG GROW: Possible Regulation of access to in-vehicle data

The European Commission is currently outlining a strategy about regulating access to in-vehicle data, specifically over-the-air. The commission will build its regulatory framework on the outcome of a study performed by TRL. Three policy options have been proposed:

- Policy Option (PO)1: do not regulate, leaving the decision to the market
- PO2: regulate access to data according to FRAND principles
- PO3: require the implementation of an on-board application platform in vehicles for independent software applications and access to data

The discussions in the Motor Vehicles Working Group (MVWG) and the first official details of the TRL study show that the commission is so far focusing primarily on the competition.

The first draft of a possible regulation framework is expected within Q1 of 2022.

DG MOVE: recently addressed the regulatory need for clarification of remote access to in-vehicle data for authorities and independent parties such as inspection centres, technical services etc.

DG CONNECT: European Data Strategy, Digital Governance Act: For the benefit of the public, increased and reliable data sharing is to be encouraged through the involvement of intermediaries. Any sector-specific framework for data access and sharing should go hand in hand with the European Data Strategy.

[2] Congressional Research Service, Issues in autonomous vehicle testing and deployment, April 2021. https://crsreports.congress.govR45985

C. Views expressed at the WP.29 and GRVA

16. The representative of FIA presented WP.29-179-18 on consumer views on automated/autonomous vehicles emphasizing the challenges associated with the cybersecurity performance of vehicles over their lifetime. He offered a possible solution to address the challenges. He admitted that the solution proposed was not design-neutral. He explained that his purpose was to demonstrate that the challenge could be solved and that at least one solution would exist. He stated that the World Forum was the right place to address this issue. He proposed that WP.29 mandate GRVA regulate Information Technology (IT) security in automotive products over their lifetime at the ECE level within the framework of the 1958 Agreement.

17. The representative of FIA presented WP.29-181-10, introducing their report on the Protection Profile and Common Criteria methodology that could potentially address FIA's concern regarding the performance and the maintenance of vehicles regarding cyber security over their lifetime. WP.29 agreed that this report would be referred to the Working Party on Automated/Autonomous and Connected Vehicles (GRVA) as well as other relevant groups.

18. The expert from FIA presented GRVA-07-41, referring to WP.29-181-10 and proposing to insert in UN Regulation No. 155 the Protection Profiles that they developed in cooperation with TüVIT. The expert from OICA responded to the proposal (GRVA-07-36). The expert from FIA agreed to respond to the challenges raised by the expert from OICA.

19. The expert from ISO introduced GRVA-09-12, with a description of the Extended Vehicle concepts and the corresponding ISO standards. GRVA noted that ISO provided copies of ISO 20077-1 and ISO 20077-2 developed by the ISO Technical Committee (TC) 22 (GRVA-09-13 and GRVA-09-14).

20. The expert from FIGIEFA introduced GRVA-10-09, informing on the activities of the alliance for the freedom of car repair in Europe and describing the Secure Onboard Telematic Platform (S-OTP) as an alternative to the Extended Vehicle model presented by the expert from the International Standards Organization (ISO) at the ninth session of GRVA.

21. The IWG on PTI reviewed the document GRVA-11-15, with positive feedback regarding considering sovereign use cases. The group agreed to keep this subject in the agenda as appropriate.

D. Listing of different models

The content of the models is not exhaustive and just gives an overview of the famous models. The collection of models is orientated by a recent discussion at the GRVA.

22. Dongle-solution

Data from the OBD port can be captured by plugging a "dongle" into the port. These retrofitted devices can communicate data over short distances via USB wire, Bluetooth or Wifi to a smartphone and SIM card, or directly over longer distances via an embedded SIM card. Some dongles come with a built-in GPS; others use the GPS in the smartphone to bypass the car's GPS system.

OBD-based applications are not tested and certified in the course of a type approval and are added at the discretion of the owner/driver. Remote access via the OBD plug-in devices has already proven security flaws that could interfere with car safety. A general problem with all security applications for OBD plug-in devices is that they are subject to hacking and may require regular updates of security features in order to protect against

the latest detected flaws. However, some OEMs have started to offer their own brand of retrofitted OBD dongles mainly in order to bring older models that still have a long life ahead into their data ecosystem.

23. Extended Vehicle Concept/ADAXO[3]

"*ADAXO*" means Automotive data access – extended and open

"*Extended*" means ADAXO is based on the ISO standardized Extended Vehicle concept (only a single access interface).

"*Open*" means open to other server platforms (NEVADA approach) as well as connectable to various data marketplaces and data trustees that are currently emerging around the world

Vehicle manufacturers offer the possibility of installing third-party software in the vehicle, considering regulatory requirements (e.g., UN R155 Cybersecurity), certification aspects and the requirements for software update management systems (UN R156).

Essentially, the release of the software and the management of vehicle resources (e.g. bandwidths for data transmissions in the vehicle) can only be carried out by the company responsible for the homologation of the vehicle model.

24. S-OTP

The Secure On-Board Telematics Platform (S-OTP) is composed of a sum of basic services in the vehicle (e.g., computing power, storage space, interfaces to actuators and sensors (data)) and of interfaces to the driver (vehicle display and controls), combined with a clear access and authorization concept for transparent and secure regulation of access to vehicle data and functions. The aim of the S-OTP is to modify the existing hardware and software components of the vehicles.

25. "Man in the middle"

There is a necessity to receive data from a vehicle. For sovereign use cases, it must be ensured that the vehicle data are complete, unaltered and their history is available. The Mobile network operator (MNO) operates as a “Man in the Middle” and has to transfer (copy) to the data trustee (DT) the data which are sent by the vehicle to the manufacturer. The first task of the DT is to store (independently from the backend of the manufacturer) a copy of the data which are sent by the vehicle. The second task of the DT is to allow access for a certified stakeholder to selected data. The DT includes the option for consumers to choose directly which stakeholder may receive access to which selected data.

26. Trust Centre

Fair and trusted access for sovereign public bodies and independent service providers can only be achieved through an independent governance model in compliance with the principle of separation of duties.

The separate tasks of data exchange participants identification, authorization of access to in-vehicle data and functions, as well as the resource provision, will be carried out independently of each other.

Access management would be handled by independent Trust Centres. Such an independent and trustworthy body, entrusted by national or regional authorities, performs access control for in-vehicle data and functions. This includes both identifications of

[3] ACEA, Policy recommendations on the upcoming regulation on access to in-vehicle data, November 2021 https://www.acea.auto/files/ACEA_position_paper-Access_to_in-vehicle_data.pdf

participants in a transaction and authorization of access and guarantees fair and independent access for all stakeholders.

For sovereign use cases, the Trust centre should be mandated by national/regional authorities. Several Trust Centres can emerge in the market.

Data Trustees collect and/or process data from vehicles of different manufacturers and suppliers and make it available to authorized data users in a secure and legally compliant manner. Data Trustees are independent of the resource provider and the authorization process and can be use-case specific. The concept of data trustees falls in line with the European Data strategy.

IV. Way forward

A. The role of institutions

27. Contracting parties have full latitude to regulate the access to the vehicle data independently. This would raise the issue of harmonization between the contracting parties.

28. Standardization institutions can provide standards and technical guidelines supporting the contracting parties.

29. Regional organizations, for instance, European Union, can support giving regulatory clarity to the EU member states.

30. In the international arena, UNECE' WP.29 has the tools to regulate and harmonize access to vehicle data. This can be done at the GRVA as it has been mandated by the WP.29 to address this issue.

B. Potential role of GRVA

31. GRVA is the place where the technical elements can be put in place to support the necessary remote in-vehicle data access.

32. The GRVA has instruments that can ease regulating the access to the vehicle data:

(a) UN Regs, UN Rules and UN GTRs

- GRVA shall regulate from the technical point of view all aspects needed, for instance:
  - i. Data to be collected
  - ii. Transmission of data
  - iii. Authenticity and non-repudiation of data.
  - iv. Encryption requirements of data to be transmitted
    - Transmission control via trust centre
    - Conditions of transmission: Transmission only in compliance with rules for access to safety relevant and other sensitive data.
- Identification of data that shall be available for sovereign tasks
- Requirements to the stakeholders (Manufactures, Technical Services, Authorities, etc.) and auditing.

(b) Recommendations

- Provide advice to Contracting Parties on the establishment of the national trust centre and the rules to provide access
- Advice on the penalties of non-compliance with the rules when it happens.

V. Proposal and Guiding Principles

33. The trusted and fair access to in-vehicle data for sovereign public bodies and entrusted service providers (e.g. Technical Services) may be achieved through an independent governance model in compliance with the principle of separation of duties. The separate tasks of data exchange participants identification, authorization of access to in-vehicle data and functions, as well as the resource provision must be carried out independently of each other.

34. The independent access management can be handled by a Trust centre. Such an independent and trustworthy body, entrusted by national or regional authorities, performs access control for in-vehicle data and functions. This includes both the identification of participants in a transaction and authorization of access and guarantees fair and independent access for all stakeholders.

35. For sovereign use cases, it is important to have access to the data of the vehicle, which should be original, trustworthy and include the history. It must be ensured that the vehicle defines the range of available data and functions and should not be limited to a scope used by the manufacturer as a service provider. The variation in data formats that already exists today and will initially continue to exist can be handled by reference to the provided diagnostic information by the OEM. This avoids an unnecessarily restricted minimum data and function set.

36. GRVA, as part of WP.29, is addressing the international harmonization of technical aspects of vehicles. The vehicles which are currently coming to the market and used on the roads create an amount of in-vehicle data. It should be of global interest to have a discussion on this global level on how to handle these data (e.g. "How is a sufficient way to store what data?") in front of different use cases (B2B or B2G). It may also be of interest for the industry to have as far as possible a kind of global harmonization on how to go on with the in-vehicle data. Otherwise, they may have to adapt their vehicle configuration to several different acting markets. These discussions may result in a regulation concerning this topic.

37. Currently, there are different possible ways (models) how to handle in-vehicle data. Every model which proposes to handle the in-vehicle data includes its own advantages and disadvantages. The diversity of the models creates an overview of the different possibilities. Therefore, an evaluation covering a wide range of different items may be helpful to realize what model includes what. The evaluation of existing models will create knowledge concerning the necessities and the challenges of a harmonized way to handle in-vehicle data. A draft of the evaluation is included in the annexe.

38. A GRVA task force or informal working group should assess the existing access models regarding their readiness for sovereign tasks (discuss if it is necessary to add more items to the structure, the subcategories or existing items; discuss and clarify how to handle proposed items and its answers).

Annex I

Abbreviations

ADAXO - Automotive data access – extended and open

B2B - Business to Business

B2G – Business to Government

FRAND - Fair Reasonable and Non-Discriminatory

MVWG - Motor Vehicles Working Group

MNO - Mobile Network Operator

OBD – On-Board Diagnostic

PTI - Periodical Technical Inspection

RTM - real time monitoring system

SME – Small + Medium Enterprises

Secure On-board Telematic Platform (S-OTP)

Annex II

Proposal for model assessment

A2 Proposal for model assessment

1 Structure

The following scheme is an open draft. Open includes that proposals for improvements are welcome. The structure of the evaluation scheme contains four main categories.

1 Data,
2 Processes,
3 Regulatory requirements and
4 Financial requirements.

The main category "Data" includes the subcategories
1.1 Data source
1.2 Data access
1.3 Data quality

The main category "Processes" is related to the involved parties. The requested items are equal for the different parties.
2.1 Vehicle / manufacturer (industry)
2.2 Trust Centre / Data Trustee
2.3 Mobile Network Operator (MNO)
2.4 Third parties

The main categories "Regulatory requirements" and "Financial requirements" do (currently) not include subcategories.

2 Explanation of assessment tool

The tool includes answering options. If the answering options do not fit the current situation, there is an optionfor a special answer in the column "Comment".

The interesting items are not only to be answered with the intended answering options (e.g. yes/no). It is also of interest to know which model is able to fulfil which criteria at what level.

2.1 Explanation in detail main category "Data"

2.1.1 Sub-category Data Source

Depending on the model there is a basic selection concerning the source of the data: from the vehicle or from the manufacturer. In case of vehicle as a source an additional item is "how to acquire the data from the vehicle?" (OBD-2, internet, detour on the transport). In case the manufacturer is the data source, an interesting topic is how the model ensures that the data are correct, consistent and reliable.

2.1.2 Sub-category Data Access

There are three different access points for third parties:
- vehicle
- Manufacturer backend
- Trust Centre / Data Trustee

One of the possibilities is the access point for the model.

In case of vehicle it is additional asked whether:
- dedicated access while it is in operation is requested,
- bi-directional communication is requested,
- additional data from the manufacturer and/or the Trust Center / Data Trustee is requested

2.1.3 Sub-category Data Quality

The first aspect requests how the data (from the data source) should be (raw data or processed data). How is it ensured that the data are complete? Is the structure of the data known? How often will the data request happen? Is the data history known? Is the model affecting cyber security or GDPR?

2.2 Explanation in detail main category "Processes"

For every involved party (2.1 up to 2.4) the same items have to be answered:
- Account management process,
- Authentication process (check of identity),
- Key management process,
- encryption process including tunnelling,
- Persistence management,
- Storage and compute,
- Connectivity.

To every process category the question is: "Are there amendments required?" The level of amendments may not be the same, therefore the degree of amendments is requested (strong degree, some degree, marginal degree and not applicable). The degree is visualized in a separate column (red, yellow, green and white).

2.3 Explanation in detail main category "Regulatory requirements"

Are multinational or national regulations required (Y/N)?

2.4 Explanation in detail main category "Financial requirements"

Depending on the model the funding is different. Therefore, the intended financing of several aspects is requested. This addresses the aspects initial and ongoing funding, funding of process changes in the vehicle at the manufacturer, funding of a Trust Centre / Data Trustee and funding of Third-Party processes.

3**. Short handling description**

Select in each subcategory the column which is fitting best to the assessed model.

The intended answering options must be used as far as possible; if no answer fits, the column "comment" offers a possibility to add a further answer and / or a comment.

If there is something missing (item in a subcategory, an additional subcategory or a main category) please give us feedback.

1	Data				
1.1	Data source				Comment
	A choice must be made between sources of data: Vehicle or manufacturer.		Vehicle	Manufacturer	
	1.1.1	Source required	Please make a choice	Please make a choice	
	1.1.2	If you intend to acquire data from the vehicle, how would you like this to be achieved?	Please make a choice		
	1.1.3	If you intend to acquire data from the manufacturer, how would you like to make sure that the data are correct, consistent and reliable?		Please make a choice	

1.2	Data Access for third Parties				Comment
	A choice must be made between variants of access to data: Vehicle, Manufacturer Backend and Trust Center/Data Trustee.		Vehicle	Manufacturer Backend	Trust Center/Data Trustee
	1.2.1	How would you like to access the acquired data?	Please make a choice	Please make a choice	Please make a choice
	1.2.2	Does your approach require dedicated access to the vehicle while it is in operation?	Please make a choice		
	1.2.3	Do you require a bi-directional communication channel to the vehicle?	Please make a choice		
	1.2.4	Do you require either the manufacturer or the trust center/ data trustee to acquire data according to demand?	Please make a choice		

1.3	Data Quality			Comment
	1.3.1	How would you like the data to be?	Please make a choice	
	1.3.2	How would you make sure that the data are complete?	Please make a choice	
	1.3.3	Would you like the structure and meaning of data to be known at any time?	Please make a choice	
	1.3.4	Would you request the available data being clear text at any time?	Please make a choice	
	1.3.5	Who has to take care of the history of data in your approach?	Please make a choice	
	1.3.6	How would you evaluate impacts of your approach on cyber security?	Please make a choice	
	1.3.7	How to evaluate impacts on GDPR?	Please make a choice	

2 Processes

Amendments may be required to processes at vehicles, manufacturers, MNOs and third parties to enable the data access your approach involves. A distinction is made between applicability to a category (vehicles, manufacturer etc.) and the degree of expression.

2.1	Vehicle or manufacturer		Vehicle	Degree		Manufacturer	Degree		Comment
	2.1.1	Account management process (grant access)	Please make a choice	Please make a choice	####	Please make a choice	Please make a choice	####	
	2.1.2	Authentication process (check of identity)	Please make a choice	Please make a choice	####	Please make a choice	Please make a choice	####	
	2.1.3	Key management process	Please make a choice	Please make a choice	####	Please make a choice	Please make a choice	####	
	2.1.4	Encryption process including tunneling	Please make a choice	Please make a choice	####	Please make a choice	Please make a choice	####	
	2.1.5	Data acquisition process	Please make a choice	Please make a choice	####	Please make a choice	Please make a choice	####	
	2.1.6	Data transmission process	Please make a choice	Please make a choice	####	Please make a choice	Please make a choice	####	

2.2	Trust Center / Data Trustee		Requirement	Degree		Comment
	2.2.1	Account management process (grant access)	Please make a choice	Please make a choice	####	
	2.2.2	Authentication process (check of identity)	Please make a choice	Please make a choice	####	
	2.2.3	Key management process	Please make a choice	Please make a choice	####	
	2.2.4	Encryption process including tunneling	Please make a choice	Please make a choice	####	
	2.2.5	Persistence Management	Please make a choice	Please make a choice	####	
	2.2.6	Storage & Compute	Please make a choice	Please make a choice	####	
	2.2.7	Connectivity	Please make a choice	Please make a choice	####	

2.3	MNOs		Requirement	Degree		Comment
	2.3.1	Account management process (grant access)	Amendments required	Please make a choice	####	
	2.3.2	Authentication process (check of identity)	Amendments required	Please make a choice	####	
	2.3.3	Key management process	Amendments required	Please make a choice	####	
	2.3.4	Encryption process including tunneling	Amendments required	Please make a choice	####	
	2.3.5	Persistence Management	Amendments required	Please make a choice	####	
	2.3.6	Storage & Compute	Amendments required	Please make a choice	####	
	2.3.7	Connectivity	Amendments required	Please make a choice	####	

2.4	Third Parties					
	Third party have to bear expenses in order to access data at the preferred access point by their own processes.		Requirement	Degree		Comment
	2.4.1	Account management process (grant access)	Please make a choice	Please make a choice	####	
	2.4.2	Authentication process (check of identity)	Please make a choice	Please make a choice	####	
	2.4.3	Key management process	Please make a choice	Please make a choice	####	
	2.4.4	Encryption process including tunneling	Please make a choice	Please make a choice	####	
	2.4.5	Persistence Management	Please make a choice	Please make a choice	####	
	2.4.6	Storage & Compute	Please make a choice	Please make a choice	####	
	2.4.7	Connectivity	Please make a choice	Please make a choice	####	

3	Regulatory Requirements		Requirement		Comment
	3.1	Multinational regulation required	Please make a choice		
	3.2	National legislation required	Please make a choice		

4	Financial Requirements		Requirement		Comment
	4.1	Initial Funding	Please make a choice		
	4.2	Ongoing Funding	Please make a choice		
	4.3	Who should fund the changes to vehicle and manufacturer´s processes?	Please make a choice		
	4.4	Who should fund the implementation of a Trust Center / Data Trustee?	Please make a choice		
	4.5	Who should fund the changes to third party processes?	Please make a choice		