VDA | German Association of the Automotive Industry

Position

ADAXO: Automotive Data Access – Extended and Open

VDA concept for access to vehicle-generated data

Contents

I Summary

1. Innovation through data – data value chain: from the generation of data to the service offering for the customer

The VDA member companies already make extensive data available for customer-oriented use cases and offer a wide range of technical access options. This proactive offering is continually being expanded.

The automotive industry’s commitment to fostering innovation and data-driven business models is reflected in the billions of euros invested in forward-looking operating systems, electrical/electronics architectures and connectivity.

These investments form the foundation for all business models based on vehicle data.

2. A common market for data – for our customers, mobility and the environment

The companies collaborating under the VDA umbrella believe in the added value that can be created by using and sharing data.

We enhance this added value by working proactively together to expand the data offering and secure technical access so that we can offer our customers added value through relevant data-based services and also improve the mobility of our customers and society – in a way that does not impact negatively on the environment or the climate while remaining secure. Customers have sovereignty over their data, subject to applicable legislation.

This is based on a stable and reliable regulatory framework that gives all those involved a level playing field and the space to develop the emerging data market.

Our commitment enables innovative business models for all stakeholders. All the companies in the VDA share a common understanding that any regulation of the data market will include rules of fair play applicable to all parties involved.

Data availability and data access will not be relevant solely to vehicles, but also to vehicle-related data held by service providers, insurance companies, financing companies and other downstream sectors in the automotive environment. This is the only way to develop new services in the interest of the customers.

3. A growing data offering – as the engine of a data-based business model

Only a comprehensive data offering supported by all vehicle manufacturers across all models will enable service providers to successfully roll out new business models.

The VDA member companies therefore support the development of a basic data set. It should be possible to make this data set available for all vehicles in compliance with legal requirements. A prerequisite for this is that the vehicles be equipped with the corresponding technologies.

The data set should be regarded as a common starting point. It will be continually expanded based on customer-oriented use cases. This expansion will be driven by those use cases demonstrating the greatest customer benefit and thus the greatest demand, and for which data can be supplied both rapidly and on a broad scale. Decisions on expansion of the use cases will be made together with the associations in a dialogue between partners.

The companies involved agree to create transparency concerning their entire online data offering available via extended vehicle (ExVe)[1] web services. These data are described using suitable semantic markups to guarantee interoperability.

4. ADAXO: Automotive Data Access – Extended & Open: confidentiality crucial to success

The VDA represents companies whose success is based on innovation and which support the protection of intellectual property and innovations accordingly. The confidentiality necessary for data-based business models is ensured by the ADAXO concept, which is a further development of the VDA's existing concept. The ADAXO concept also provides the option of disclosing neither the identities nor the business models of the accessing companies to the primary data collectors. The ADAXO neutrality concept can also be implemented in data spaces, and for us it represents the logical next step in neutral data provision. Ultimately full sovereignty over the data remains with the vehicle customer.

The ADAXO data offering includes the aforementioned initial data set that will be prepared via the use case approach described and continually expanded.

[1] Extended vehicle concept: Manufacturers route the data via an OEM back end.

5. FRAND – rules for collaboration between partners to the benefit of our customers

Fair, reasonable and non-discriminatory (FRAND) are the common rules for all participants in the data market. The VDA member companies offer FRAND access for data and functions to those companies that likewise commit to the FRAND principle.

The OEMs offer access to all data and functions that they themselves use to provide their own services. Non-discriminatory access to the data is provided either masked (e.g., neutral server) or directly via the OEM on the basis of B2C or B2B contracts, respectively.

Individual contracts are drafted for each company. From the perspective of the VDA member companies, efforts should be made to define standard contract components provided this is permissible under antitrust law. Fair data sharing is also based on transparent pricing that is not prohibitive.

6. Authorization management – creating added value in the interest of our customers

In accordance with applicable law, data are transferred only for a particular purpose, i.e., for the specific use case.

- From the customer's perspective and from that of data protection law, authorization management should be central, consistent and simple to use, and as such should rest with the manufacturer (OEM) as the central contact for data collection.

- The customers have sovereignty over the data. They decide, in accordance with the applicable law, which data are transmitted to which recipients. The manufacturers should comply with the customers' wishes.

- The commercial data flow is not monitored by the OEMs, unless this is required for legal, contractual or security reasons.

- Confidentiality clauses ensure that customer data are not analyzed, thus preventing reverse engineering. Authorizations for third-party services can be encrypted so that the business models of third parties do not become known to OEMs.

The manufacturers can make data accessible to OEM-operated and non-OEM-operated data marketplaces that satisfy the relevant prerequisites. The primary data collectors will ensure compliance with the legal requirements by means of an end-to-end authorization management system.

7. Technical access – customer-focused and efficient provision of data

The VDA member companies already offer various technical access methods so that vehicle data are made available in a customer-oriented manner in compliance with legal requirements. All the companies support the ADAXO concept, which enables data – such as the jointly developed basic data set – to be obtained under FRAND conditions. In addition, the OEMs operate their own online portals through which companies can acquire data directly, based on B2B and B2C contracts. The Mobility Data Space (formerly the DRM “Datenraum Mobilität”) will add another marketplace that offers, in particular, the possibility of obtaining data from many different sources swiftly, efficiently and with high transparency using standardized data connectors. A large number of VDA members already support this approach and are promoting its further expansion.

8. Third-party data access – security first

Today third parties can already be granted direct access to vehicle data and functions if they satisfy the technical and legal requirements.

As development progresses, various vehicle manufacturers will offer the option of installing software from third-party providers in vehicles, subject to regulatory requirements (e.g., UNECE R155 on cybersecurity), certification aspects and the requirements for software update management systems (UNECE R156). To this end, guidelines should be developed in collaboration with the associations to provide a secure basis for the installation of third-party software in vehicles.

Fundamentally, though, only the company responsible for certifying the vehicle can approve software and manage vehicle resources (e.g., bandwidths for data transmission in the vehicle). When considering possible options or developments, all companies must give top priority to the safety of all road users.

II Classification and context

II.1. European and national data strategies as an innovation promotion

In 2020, the EU Commission published its vision for a data economy in Europe with the European data strategy[2]. The EU will work toward a common market for data, with data flows between the member states and sectors on the basis of European values and standards, and under the premise of fair, practical and clear rules. The objective is to increase the creation of value in Europe for both citizens and the industrial stakeholders. In particular, it should be ensured that there is a fair sharing of data between all involved in keeping with the idea of a level playing field. This is intended to preclude preferential treatment of individual interest groups, sectors or company sizes.

Against the backdrop of this EU strategy and also national data strategies, the EU Commission has issued consecutive regulations and is currently working on additional regulatory projects. Here are some examples:

1. A draft **Data Governance Act** (DGA) intended to strengthen the European data economy was submitted in November 2020. To this end, data sharing between companies, private persons and the public sector is to be simplified and trust in the data transfer established.

2. The **Data Act** (DA) addresses the expanded access to, and the use of, data of both public and private actors. It is intended to ensure fairness in the data market between the individual stakeholders involved. The DA explicitly address the sharing of business-to-business (B2B) data and business-to-government (B2G) data.

3. The **Digital Markets Act** (DMA), which establishes a number of narrowly defined criteria for qualifying large, online platforms as gatekeepers, is intended to balance market power on the data markets.

4. The **Digital Services Act** (DSA) is intended to ease the expansion of smaller platforms, SMEs and startups on the data market. It aims to create a safer digital space where the fundamental rights of users are protected and to establish a level playing field for businesses.

5. The **Implementation Act High Value Data Sets** is intended to release the socioeconomic potential of data.

All of the regulatory projects cited have one thing in common: They strengthen the customers and their rights to data sovereignty in addition to spurring innovation toward a European-level data market.

[2] https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_en.

But these efforts are not limited to the European level: EU member states are also developing national-level strategies to enable the transition to digitalization. The federal German government, for example, has prepared the **Data Strategy of the Federal German Government**[3]. This describes the innovation strategy for social progress and sustainable growth. The fundamental goal of this strategy is to create a data culture

- that protects the fundamental values, rights and freedoms of society
- while, at the same time, substantially increasing data provision, thus fostering innovation[4].

The basis for the implementation of the data strategy comprises the sustainable expansion of effective and secure data infrastructures, and the creation of sectoral data spaces, such as for industry, the Green Deal and mobility, among other things.

Other EU members are pursuing comparable objectives with their own national data strategies.

II.2. Regulatory framework as a level playing field

The EU's legislative initiatives are intended to ensure a level playing field in the internal market for companies with respect to data sharing. The basis for this is a stable and reliable regulatory framework that gives all those involved a level playing field and the space to develop the emerging data markets.

All the companies in the VDA share a common understanding that any regulation of the data market must include rules of fair play applicable to all parties involved. These rules regarding data availability and data access will not be relevant solely to vehicles, but also to vehicle-related data held by service providers, insurance companies, financing companies and other downstream sectors in the automotive environment.

A strategically meaningful expansion of the data offering across sectors in Europe requires a forum for all parties in which positions can be shared and the balancing of interests can be negotiated. Solutions for currently unclear or restrictive prerequisites within the planned regulations could be discussed and developed together here.

As the German automotive industry association, the VDA is prepared to substantially foster and drive the data culture in the European internal market.

[3] Data Strategy of the Federal German Government, Cabinet Version dated 27 January 2021.
[4] Datenstrategien: Was passiert in Deutschland und der EU? (Data strategies: What's happening in Germany and the EU?") › BASECAMP.

II.3. Regulatory density from the perspective of the automotive industry

The introductory remarks illustrate the regulatory density and the associated requirements complexity that directly – and also negatively – influence the innovative capability of the automotive sector. So far, hardly any synergies or interconnections between the regulatory projects are evident. In addition, individual directorates-general of the EU Commission have commissioned studies that describe the requirements with respect to access to vehicle data and propose very detailed solutions (see Annex V.1). There should be better coordination of the projects of the various directorates-general.

Furthermore, the parallel and largely decoupled approach within the framework of the European legislative initiatives overlooks the existing and practice-tested concepts and initiatives of the OEMs with respect to the derivation of vehicle data within the context of access to in-vehicle data.

From the perspective of the VDA, no additional specific regulations regarding data are necessary. These generate additional complexity in the technical implementation and design of data-driven business models. Both inhibit innovation activities – not just in the automotive industry, but also on the part of those providing data-based services.

The greater need is for the harmonization of cross-sector regulations. Only by doing so are innovations within the context of digitalization and the cross-sector sharing of data for the creation of new business models possible.

II.4. Support of data-driven business models and innovations

The VDA and its members proactively support data generation and the sharing of data with innovations along the value-added chain: from data generation to the establishment of the conditions required for functioning cross-manufacturer and cross-sector data markets. For years, large investments have been made here to develop and establish sustainable competitive models that can successfully compete with international competitors and which meet with great interest from the markets.

Furthermore, the VDA and its members have long endorsed and supported the secure connection to public sector data spaces for the harmonized and cross-sector sharing of data.

II.5. Secure access to vehicle data

One focus topic of the various data strategies is protection against cybercriminal activities. This applies to the strategies of both the political sector and the industry. Digitalization in the automotive sector has given rise to the threat of potential attacks against the technical interfaces in the vehicle and the risk of unauthorized access to sensitive vehicle functions. It is not just the provision of interfaces for data sharing with third parties that requires additional security efforts. Bidirectional connections for third-party write access or the installation of software in the vehicle by third parties must also be protected. Risks associated with any desired use of the interfaces must be minimized.

The vehicle manufacturer is largely responsible for securing any interfaces in the vehicle that connect to the outside world, since they can perform the necessary actions on the vehicle architecture safely and efficiently. Another important consideration here is that, given the rapid pace of digitalization, the requirements for these safeguards require increasingly complex solutions.

In light of this, the vehicle manufacturers developed the extended vehicle concept (ExVe) for secure access to vehicle data years ago. ExVe addresses the sharing of data between the vehicle and the manufacturer's server via the cellular interface. The ExVe web interface is available in all modern vehicles and ensures secure communication between the vehicle and the manufacturer's[5] server. Third parties can – on the basis of corresponding B2B contracts – access the vehicle data via a standardized interface according to ISO 20078. There is no possibility of interference with the vehicle architecture by an ISO-certified[6] and standardized interface.

ExVe has been used successfully for many years now and has proven itself on a broad front. Millions of vehicles in Europe are currently connected in this way to vehicle manufacturers' servers and make data available to third parties. The primary strength of this concept is the openness with respect to the type and amount of data transferred, which opens up a wide range of innovative application options to vehicle users, service providers and manufacturers while simultaneously complying with the provisions of the law (EU GDPR).

With the ADAXO concept, of which the ExVe concept is an integral component, the VDA presents a modern and future-safe model for the sharing of vehicle-generated data between all stakeholders, and also requirements for bidirectional connections and third-party software in the vehicle This concept will be presented in greater detail in the subsequent sections of this document.

[5] Other interfaces, such as the interface between the mobile phone and vehicle or vehicle-to-vehicle communication (V2V), are not affected by the concept. Likewise, access to vehicle data for repair and maintenance measures continues to be available via the OBD-2 diagnostic interface installed in the vehicle.

[6] ISO 20077/20078/20080.

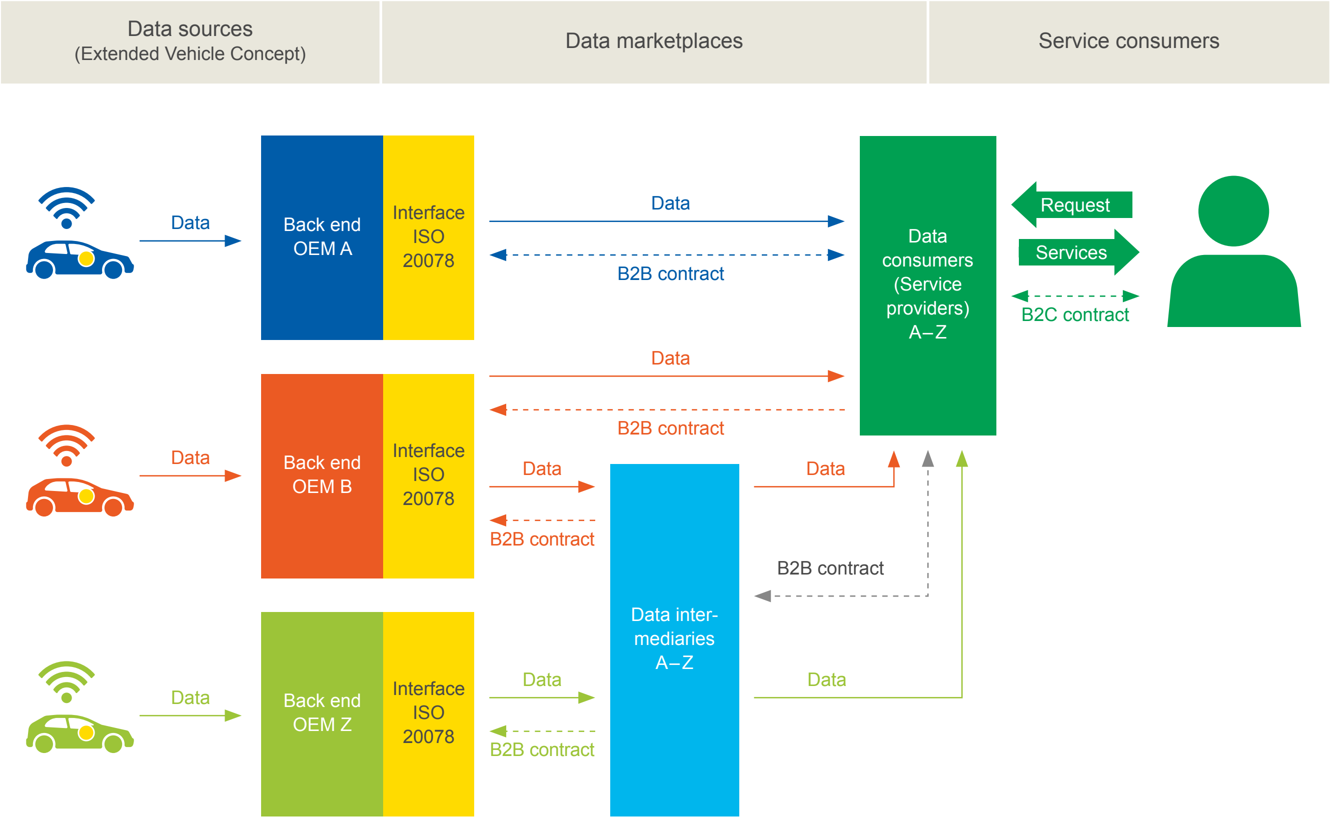
III ADAXO concept – technical details

ADAXO describes principles for the free, non-discriminatory access to data and functions of the corresponding authorization management under the aspect of cybersecurity. ADAXO thus establishes the foundations upon which platforms for data sharing can be created without being such a platform itself.

III.1. Data flow and contractual relationships in the ADAXO concept

A key pillar of the European digital and data strategies is to simplify the use and sharing of data so that new business models can be created on this basis. It also opens up the possibility for third parties to establish bidirectional connections to the vehicle and to integrate software into the vehicle. The German automotive industry welcomes this and is pushing the sharing of data with third parties to account for the potential harbored by services based on vehicle-generated data.

Data flow and contractual relationships in ADAXO



● ODB interface for services to the vehicle

The VDA member companies already make extensive data available for customer-oriented use cases and offer a wide range of solutions for sharing data. The incorporation of third-party software into the vehicle – in compliance with regulatory requirements – should be further expanded. Furthermore, additional types of access, such as third-party write access to vehicle systems in accordance with cybersecurity requirements, should be increasingly possible. This proactive offering is continually being expanded.

Data are provided via the extended vehicle concept, which sends the data to the OEM back end via a cellular interface in the vehicle. Access to the data is via an interface standardized according to ISO 20077/20078/20080.

The sharing and use of data are dependent on the respective use case or offer and may take place via connected data marketplaces. Data sharing can either be on the basis of a B2B contract between the OEM and the data consumer or optionally with an intermediary (e.g., neutral servers, proprietary platform) between them. This may result in the decoupling of the business relationship between the data sources and data consumers required for various business models, and may also simplify management of the relationships between the OEM and the intermediary/the intermediary and the data consumer.

The data intermediaries bundle data and make these available to third parties (data consumers), so that these can develop and offer a product or service for customers on this basis. Another possibility is for the OEM to conclude a contract directly with the data consumer. Data sharing is based on various B2B contracts depending on which form of data provision is chosen (see graphic “Data flow and contractual relationships in ADAXO”).

The objective of this approach is to offer end customers the best-possible service and allow them to choose from various offers and/or suppliers.

III.2. Data access according to FRAND principles

One of the basic premises of ADAXO is fair, reasonable and non-discriminatory data access for third parties. Although access to the data is not free of charge because various cost drivers such as the provision/development of data accesses or operation do exist, pricing must always be fair. Thanks, in particular, to the freely accessible provision of data via various marketplaces, intermediaries and data spaces, the price is determined by the interplay between supply and demand. The data marketplaces therefore not only have a technical data sharing function, but also serve the natural regulation of the market price in the sense of fair pricing. Refusal to provide data to individual parties, i.e., the deliberate discrimination against them, is not permitted.

Future regulatory projects should aim to initiate data markets. Only functioning data markets can ensure pricing according to the FRAND principle.

III.3. Authorization and consent management in ADAXO

An authorizer in ADAXO is typically the vehicle owner, the vehicle holder and/or the vehicle user. The authorizer can vary depending on the data point.

Because it is particularly valuable for innovative business models, a significant portion of the data derived from the vehicle is person-related. These data are always subject to the provisions of the GDPR. Data can only be used on the basis of the consent given by the authorizer in the context of the intended use thereof.

This necessitates the establishment of effective and GDPR-compliant authorization management. The ADAXO concept fully satisfies this requirement:

In accordance with applicable law, data are transferred only for a particular purpose, i.e., for the specific use case.

- From the customer's perspective and from that of data protection law, authorization management should be central, consistent and simple to use, and as such should rest with the manufacturer (OEM) as the central contact for data collection.

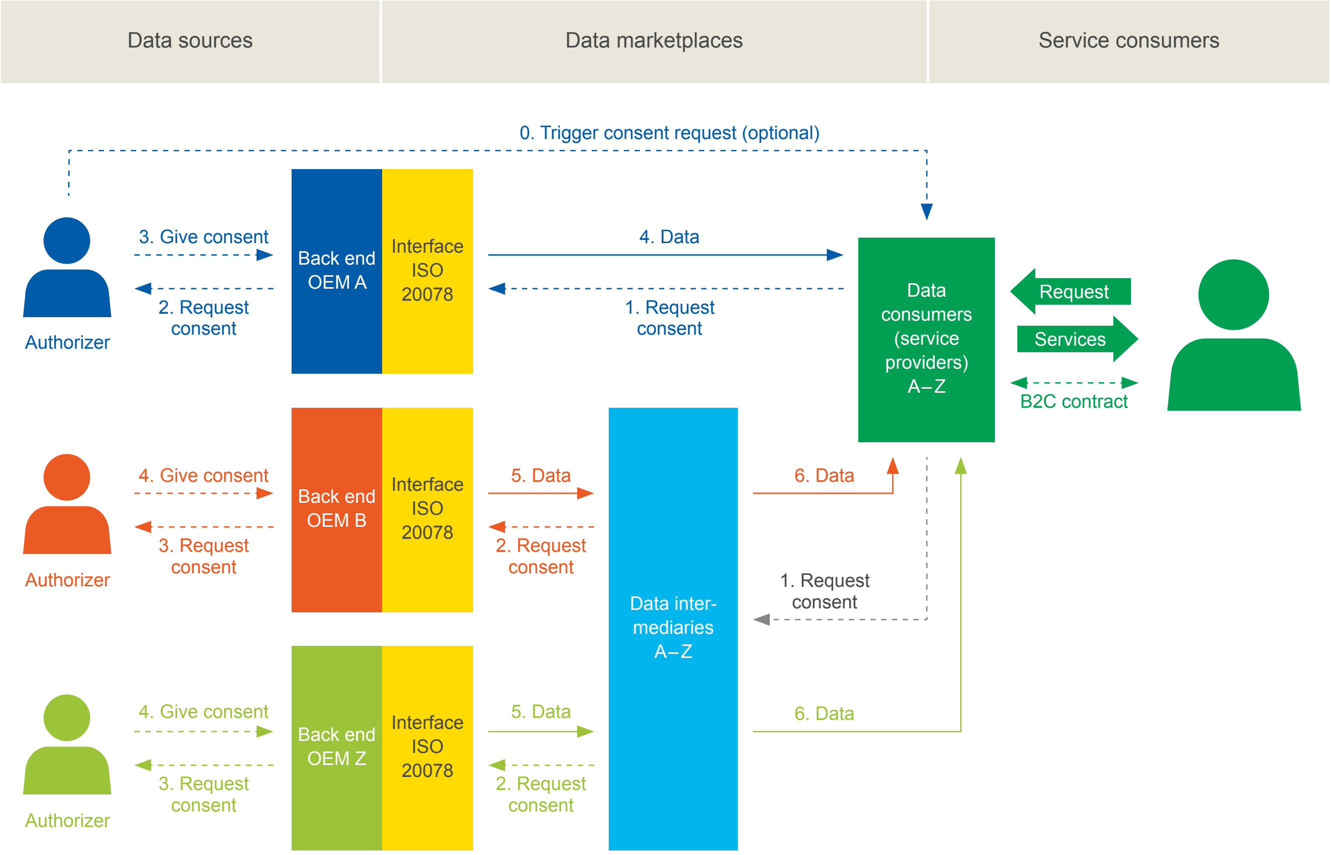
- The customers have sovereignty over the data. They decide, in accordance with the applicable law, which data are transmitted to which recipients. The manufacturers should comply with the customers' wishes.

- The commercial data flow is not monitored by the OEMs, unless this is required for legal, contractual or security reasons.

- Confidentiality clauses ensure that customer data are not analyzed, thus preventing reverse engineering. Authorizations for third-party services can be encrypted so that the business models of third parties do not become known to OEMs.

The manufacturers can make data accessible to OEM-operated and non-OEM-operated data marketplaces that satisfy the relevant prerequisites. The primary data collectors will ensure compliance with the legal requirements by means of an end-to-end authorization management system.

Authorization and consent management in ADAXO



As previously illustrated, data in the ADAXO concept first flow via a cellular interface from the vehicle to the vehicle manufacturer's back-end server. The prerequisite for this is that the owner of the rights to the data consents to this. This is normally the authorizer for the vehicle[7]. Consent is managed by the authorizer initially (one time) creating a so-called owner account online with the vehicle manufacturer. The authorizer can then use this account to manage their data pursuant to the GDPR. The authorizer can, for example, release their data for use by a third party for a specific purpose, revoke this consent, request a copy of the data, etc.

The owner account also enables the vehicle manufacturer to contact the authorizer directly to obtain the authorizer's consent to the transfer of their data to a third party for a specific purpose, provided that the manufacturer was asked by such a third party to do so. In other words, a service provider contacts the OEM and requests the release of certain data of a

[7] If the owner lends out the vehicle or if personal data of passengers are collected, it is assumed that the owner obtained the oral consent of these persons.

certain customer for a defined purpose. The OEM forwards this request to the owner of the owner account. If the account owner consents, the OEM can forward the respective data to the data consumer making the request.

If the data flows through a data intermediary, authorization management must, of course, also include the intermediary. In this case the data consumer contacts the intermediary with the request that certain data from connected data sources be provided. The intermediary must first forward this request to the respective OEMs. These once again use the owner account to contact the authorizer with the request. If the authorizer consents, the OEM can forward the respective data to the intermediary, who then turns them over to the data consumer.

A special authorization management case is the situation in which an authorizer wants to use a certain service for which access must be granted to the authorizer's personal data. In this case, the authorizer triggers the consent process described above and uses their owner account with the OEM to consent to the forwarding of their data.

III.4. Cybersecurity

Cybersecurity protects the vehicle against unauthorized third-party access. Unauthorized access to the vehicle systems enables the actors to receive information and/or transmit it to vehicles outside the vehicle itself, as well as to establish an interface between multiple vehicles simultaneously without the need of physical access to the vehicle. Countering such attacks requires logical and physical isolation techniques. This is important because the best method for preventing an attacker from gaining remote control of a vehicle or manipulating its performance is to ensure that there are no vulnerabilities or connections via which an unauthorized third party can access vehicle components and send commands to them. As development progresses, various vehicle manufacturers will offer the option of installing software from third-party providers in vehicles, subject to the regulatory requirements, certification aspects and the requirements for software update management systems. The required international standards have been implemented for reasons of cybersecurity and to protect against manipulation of in-vehicle software. For example, UNECE R155 (Cybersecurity Management System, CSMS) applies for the type approval of all new vehicle types effective July 2022. UNECE R156, which governs the establishment and operation of a certified software update management system (SUMS), was also ratified in summer 2020. These UNECE regulations ensure, among other things, the necessary cybersecurity activities before, during and after product development and are always considered in the ADAXO concept.

III.5. Prerequisites for connectivity

Due to the coupling of a multitude of functions, data providers have a fundamental interest in maintaining the basic connectivity of vehicles for as long as possible.

The basic connectivity of the vehicle is therefore maintained for as long as, on the one hand, the technical prerequisites for this are fulfilled and, on the other hand, the authorizer has booked the basic connectivity. Potential technical factors that could lead to a termination of the basic connectivity and typically lie outside the sphere of the data provider and data consumer include such things as the deactivation of older cellular networks (2G and 3G networks), non-fixable security incidents in older systems, or the end-of-life of the technology used.

III.6. Free access to vehicle resources

III.6.1. Non-discriminatory access to vehicle resources

The OEMs offer access to all data and functions that they themselves use to provide their own services. Non-discriminatory access to the data is provided either via intermediaries (possibly masked, e.g., using neutral servers) or directly via the OEM on the basis of B2C or B2B contracts, respectively.

In contrast to purely read access to vehicle data stored in the back end (i.e., without affecting the vehicle itself), there are additional risks to the integrity of the vehicle systems and their operational safety when there is a write (or read and write) connection to the vehicle, such as is required for remote diagnostics. For remote diagnostics, the vehicle manufacturer therefore makes all diagnostic-relevant data and functions available via an abstraction layer so as to preclude particularly risky operations and operating states. The applicable principle here is that authorized third parties receive access to such remote diagnostic services at the same time and to the same extent as the respective manufacturer’s authorized dealerships, workshops and service providers.

To preclude mutual interference, remote diagnostics can only be performed by a single party at any given time.

ISO 20080 (Remote Diagnostic Support) should be amended to include this.

Because remote diagnostics and repairs via write access often also include the deactivation of safeguards (e.g., window pinch guard) and changes to actuators (e.g., trailer hitch extension), the service provider must ensure user expertise and a commitment to proper use.

Interaction with the service consumer via HMI uses available technical solutions, and the information is mirrored in the vehicle's HMI. Existing technical solutions can fulfill these requirements.

III.6.2. Monitoring and enforcement

The monitoring and enforcement of diagnostic mechanisms is supported, if necessary. This can also be via a "structured forum" of the affected parties and possibly with the involvement of the EU Commission. See the recommendation in Section IV.2.

III.6.3. Prevention of unauthorized business monitoring

The commercial data flow is not monitored by the OEMs, unless this is required for legal, contractual or security reasons. Confidentiality clauses ensure that customer data are not analyzed, thus preventing reverse engineering of service offerings.

Read data access use case:

- See Section III.2 for the precise authorization workflow as an extension of ISO 20078.
- The authorizer (OEM's contractual partner for the telematic request) must be clearly identifiable by the OEM and therefore cannot be masked.
- The service provider and the service providers customers can be masked via a data intermediary (e.g., neutral server). This constitutes non-disclosure in the sense above.

Remote diagnostic support use case:

- Remote diagnostic support (RDS) refers to read and write online access to vehicle systems via the OEM back end for the remote diagnostic and maintenance purposes, i.e., access that can have a direct effect on the vehicle's electrical/electronics system and its components, including actuators.
- The position described below is not restricted to tele-diagnostic and maintenance purposes, but rather can be applied to all remote online access (ROA) use cases (including the use of such remote services as remote door unlock).

- A data intermediary (e.g., neutral server) acts as a technical service provider to the service provider that has concluded a B2B master agreement for RDS with the respective OEM in accordance with the framework conditions.

- Liability remains with the service provider; an RDS contract between the service provider and the OEM is concluded in accordance with the B2B master agreement.

- The data intermediary (e.g., neutral server) handles authentication and authorization of the service provider's customers (individual service unit performing the work).

- The authorizer must be clearly identifiable by the OEM and therefore cannot be masked.

- Due to the regulated transfer of liability, the service provider must be clearly identifiable by the OEM and therefore cannot be masked.

- The service provider's customers (individual service unit performing the work) can be masked via an identifiable data intermediary (e.g., neutral server) and identifiable service provider. This constitutes non-disclosure in the sense above for the individual service unit performing the work.

III.6.4. Access authentication

One has to differentiate between read data access to the OEM back end (without affecting vehicle systems) and write access, e.g., remote diagnostic support (RDS) to the vehicle via the OEM back end, since a regulated transfer of liability from the OEM to the service provider must be ensured in the event of direct access to the vehicle.

- Read data access:

  – See Section III.2 for the precise authorization workflow as an extension of ISO 20078).

  – The authorizer (OEM's contractual partner for the telematic request) must be clearly identifiable by the OEM and therefore cannot be masked.

  – The service provider and the service providers customers can be masked via a data intermediary (e.g., neutral server). This constitutes non-disclosure as described in Section III.6.3.

- Write data access (e.g., remote diagnostic support, RDS):
  - Remote diagnostic support (RDS), ISO 20080, refers to read and write online access to vehicle systems via the OEM back end for the remote diagnostic and maintenance purposes, i.e., access that can have a direct effect on the vehicle's electrical/electronics system and its components, including actuators.
  - The position described below is not restricted to tele-diagnostic and maintenance purposes, but rather can be applied to all remote online access (ROA) use cases (including the use of remote services like remote door unlock).
  - A data intermediary, e.g., neutral server) can act as a technical service provider to the service provider by concluding a standard master agreement for RDS with each OEM in accordance with the framework conditions.
  - Liability remains with the service provider; an RDS contract between the service provider and the OEM is concluded in accordance with the standard master agreement.
  - If a data intermediary (e.g., neutral server) is used, the data intermediary handles authentication and authorization of the service provider's service consumer (individual service unit performing the work).
  - The authorizer must be clearly identifiable by the OEM and therefore cannot be masked.
  - Due to a regulated transfer of liability, the service provider must be clearly identifiable by the OEM and therefore cannot be masked.
  - The service provider's customers (individual service unit performing the work) can be masked via a data intermediary (e.g., neutral server) and identifiable service provider. This constitutes non-disclosure as described in Section III.6.3.

III.6.5. Liability

One has to differentiate between read data access to the OEM back end (without affecting vehicle systems) and remote diagnostic support (RDS) to the vehicle via the OEM back end, since a regulated transfer of liability from the OEM to the service provider must be ensured in the event of direct access to the vehicle. The liability for RDS remains with the service provider; an RDS contract between the service provider and the OEM is concluded in accordance with the B2B master agreement. With RDS, the service provider must be clearly identifiable by the OEM and therefore cannot be masked due to the regulated transfer of liability.

III.6.6. Identification of the end customer

End customers can be both authorizers and service consumers.

With read access, the service consumers of the service provider can be masked via a data intermediary (e.g., neutral server).

But with RDS, the service provider must be clearly identifiable by the OEM and therefore cannot be masked due to the regulated transfer of liability. The service consumers of the identifiable service provider (individual service unit performing the work) can, however, be masked by the data intermediary (e.g., neutral server).

In both use cases above, the authorizer cannot be masked due to the required telematic contract for basic connectivity.

III.7. Illustration of various data architectures in the vehicle

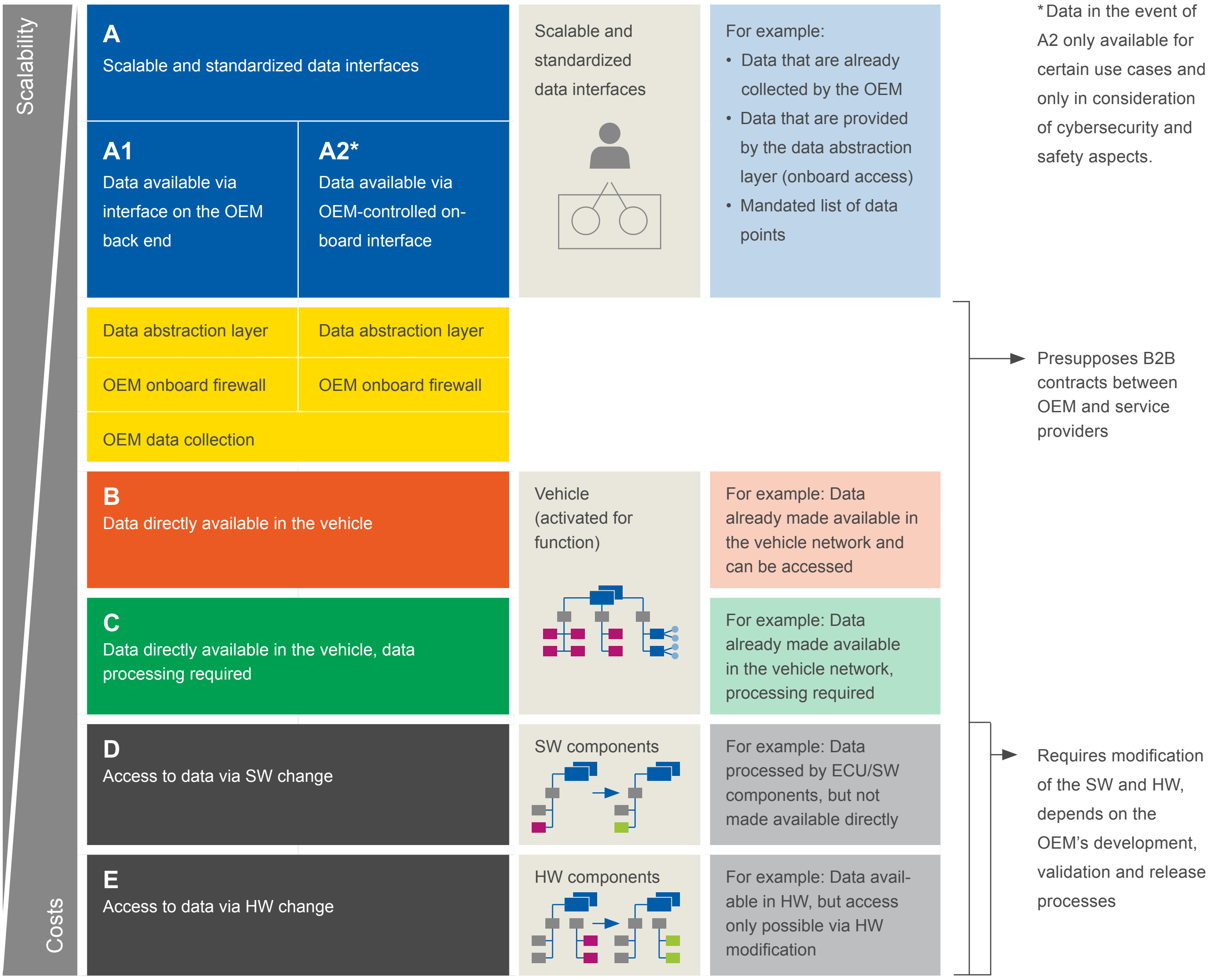
The data architecture in the vehicle differentiates clearly between a public (A) and private (B–E) area comparable to an internet, in which public information is accessible, and an intranet, which is protected with security measures, for example.

Area A is for data that are made available to authenticated third parties via scalable and standardized interfaces. The data set in A is expanded continually.

We differentiate here between an ExVe interface, which is available on the OEM back end (A1), and an onboard interface that can only provide data for specific use cases (A2).

Cybersecurity requirements determine to what extent and for which purpose data can be made available. Due to the greater risks of onboard access, the potential extent of the available data will be smaller with A2 than with A1.

Various data architectures in the vehicle



A
Scalable and standardized data interfaces

A1
Data available via interface on the OEM back end

A2*
Data available via OEM-controlled onboard interface

Scalable and standardized data interfaces

For example:

- Data that are already collected by the OEM
- Data that are provided by the data abstraction layer (onboard access)
- Mandated list of data points

*Data in the event of A2 only available for certain use cases and only in consideration of cybersecurity and safety aspects.

Data abstraction layer | Data abstraction layer

OEM onboard firewall | OEM onboard firewall

OEM data collection

Presupposes B2B contracts between OEM and service providers

B
Data directly available in the vehicle

Vehicle (activated for function)

For example: Data already made available in the vehicle network and can be accessed

C
Data directly available in the vehicle, data processing required

For example: Data already made available in the vehicle network, processing required

D
Access to data via SW change

SW components

For example: Data processed by ECU/SW components, but not made available directly

E
Access to data via HW change

HW components

For example: Data available in HW, but access only possible via HW modification

Requires modification of the SW and HW, depends on the OEM’s development, validation and release processes

Detailing Cases B and C: (B) Data directly available as an onboard resource are made available that can be elevated to Level A. (C) These data can be preprocessed to make additional data available. This requires additional resources, however.

Data that can be assigned to B and C and should be made available in A require an additional B2B contract between the OEM and the third party, i.e., this is only possible with the consent of the OEM or on the basis of a legal foundation. On the basis of such an agreement and its technical possibilities, the OEM will provide the third party with additional data from the vehicle via the interface (Case B) or will perform onboard preprocessing (Case C). The third party must provide the specification for such preprocessing in the form of requirements or pseudocode and the OEM performs the integration. The specification must consider data economy, adequate interface width (number of data points) and latency, as well as event-based timeliness and processing frequency.

Detailing Cases D and E: There are also data that cannot be accessed yet (D and E). In the case of D, data collection is only possible with a change to the software components. For example, a date has been computed by an ECU but not yet transmitted. In the case of E, collection is only possible with a change to the hardware components, e.g., if the ECU is not technically connected to the abstraction layer or sensors are not installed.

Use cases that can assigned to D and E therefore require an additional B2B contract between the OEM and the third party, i.e., they are only possible with the consent of the OEM or on the basis of a legal foundation.

The deeper the collection of data goes into the architecture, the more complex (cost and time) the implementation is.

The development of software for vehicle systems and software for data provision are subject to clear guidelines, such as requirements specifications, manufacturer-specific standards and design guidelines, industry-wide security and functional safety guidelines, and regulatory framework conditions. In addition, resource requirements (e.g., RAM and CPUs) are agreed individually.

Validation and approval processes defined and used by the vehicle manufacturer itself must be observed, as safety and security requirements, for example, can only be mastered by considering the entire system (see, in particular, variant diversity, test application and safeguarding processes).

The development and integration of software decoupled from these processes is therefore not feasible.

The vehicle manufacturer is always responsible for the integration, functional safety and security, as well as configuration and resource management. As it stands today, the possible integration of third-party software is only feasible under the additional premise of disclosing the source code.

All data are abstracted prior to their provision to third parties. The aim of this abstraction is to make the purely technical vehicle signals usable and to describe them as independently as possible from manufacturer and vehicle generation (e.g,. vehicle signal specification, VSS). Access to the data provided always occurs above this abstraction layer. The degree of abstraction can vary depending on the E/E architecture generation. The current high integration effort for secure data provision can possibly be reduced in future E/E architecture generations through the use of virtualization and software isolation technologies.

The ADAXO concept also enables the representation of new content, possibly with the help of HW or SW changes in the vehicle. The ADAXO concept supports the functional safety requirements implemented in the vehicle (e.g., ASIL conformity of vehicle functions).

In contrast to purely read access to vehicle data available via the interface, (i.e., without affecting the vehicle itself), there are additional risks to the integrity of the vehicle systems and operational safety when functions are used.

For remote diagnostics (or write access via the onboard APIs), the vehicle manufacturer makes all diagnostic-relevant data and functions available via an abstraction layer so as to preclude particularly risky operations and operating states. The applicable principle here is that authorized third parties receive access to such remote diagnostic services and writing onboard APIs to the same extent and for the agreed purpose as the respective manufacturer's authorized dealerships, workshops and service providers.

Note: The detailed flow of the remote diagnostic use case can be found in Attachment V.2.

The vehicle must be adequately secured for write access, e.g., against rolling away or persons getting trapped in the window. This secured state must be confirmed in the vehicle via the HMI (if the vehicle isn't locked) or by a responsible person via an app (if the vehicle is locked). Corresponding legislation is recommended.

III.7.1. Installation and execution of onboard software

As new architectures are introduced, hypervisor technologies will become available, for example, which will enable hardware abstraction to the extent that the preprocessing of information will also be possible by third parties in the future.

The use of onboard resources harbors additional risks for the integrity of the vehicle systems and operational safety. Whenever possible options or developments are considered, all the companies always give top priority to the safety of all road users and those involved in the repair process.

Validation and approval processes defined and used by the vehicle manufacturer itself must be observed, as safety and security requirements, for example, can only be mastered by considering the entire system (see, in particular, variant diversity, test application and safeguarding processes).

The development of software for vehicle systems and software for data provision are subject to clear guidelines, such as requirements specifications, manufacturer-specific standards and design guidelines, industry-wide security and functional safety guidelines, and regulatory framework conditions. In addition, resource requirements (e.g., RAM and CPUs) are agreed individually.

The development and integration of software decoupled from these processes is therefore not feasible.

The vehicle manufacturer is always responsible for the integration, functional safety and security, as well as configuration and resource management. As it stands today, the possible integration of third-party software is only feasible under the additional premise of disclosing the source code.

Fundamentally, though, only the company responsible for certifying the vehicle can approve software and manage vehicle resources (e.g., bandwidths for data transmission in the vehicle). This must be done in accordance with regulatory requirements (e.g., UNECE R155 on cybersecurity), certification aspects and the requirements for software update management systems (UNECE R156) if software from third parties is installed in the vehicle.

To this end, guidelines should be prepared in collaboration with the associations to provide a secure basis for the installation of third-party software in vehicles. The structured forum described in Section IV.2 can provide a foundation for this.

III.7.2. Interaction with the driver via HMI (human-machine interface)

The following conditions must be observed when accessing the HMI (incl. display and control elements):

- legal guidelines, driver distraction guidelines analogous to those from the NHTSA, ethical/moral guidelines;
- HMI design guidelines, e.g., type sizes, layout, driver centricity, animations;
- architecture, resources and security guidelines.

Depending on the technologies used (OEM-specific solution or projected mode), this governance role is assumed by the vehicle manufacturer or the party responsible for the platform (e.g., Apple for CarPlay). The technologies also differ with respect to functionality, scalability, and the time and costs required for implementation.

For reasons of functional safety, certain displays/signals may not follow immediately or at all (such as streaming video while driving).

Assessment criteria:

- Scalability for the OEM: Effort for the OEM to test and approve third-party solutions must be manageable.
- Scalability for the third party: Minimal adaptations required for each OEM or solution can be used universally.
- Fulfillment of third-party requirements: functional requirements, e.g., maintenance applications, interaction with the customer.
- Short-term achievability: Technology is already available in the market or can be introduced in the short term.

Technologies assessment

	Projected mode	Notifications	Native app on head unit (OEM app store)
Description	Availability of projected mode in all vehicles / cross OEM	Opening of ConnectedDrive messaging service for third parties	Third-party development of Android apps, inclusion in OEM app store
Functionality	Proprietary applications on the basis of permitted templates	Informational notifications with message content (text) and sender (navigable address and telephone number)	Proprietary applications (Android app)
Technology providers and governance	Apple/Google	OEM	OEM
Cross-brand ecosystem/ scalability from third-party perspective	+++	++	+
Effort OEM/scalability from OEM view	+++	++	–––
Fulfillment of third-party requirements	0	+	+++
Short-term achievability	++	++	–––
Potential for improvement	Extension of permitted functions	Integration into CarData API, possibly return channel	

1. Projected modes
    a. offer good scalability for the OEM and third party. In the case of projected mode, the third party only has to develop once; OEM adaptations are not required. Testing/ qualification is the responsibility of the platform provider (e.g., Google or Apple), for whom this is a core business, unlike for the OEMs.
    b. can be used for end-customer interaction, but not for comprehensive business cases (e.g., remote diagnostics)
    c. are available immediately.
    d. must be extended beyond the currently available domains messaging, infotainment and navigation, i.e. the functional requirements of the third parties have not yet been met. Joint approach to, for example, Apple/Google regarding expanding the functionalities of projected modes. The use of projected modes in the market is growing quickly (particularly in the USA), so it can be assumed that the number of available domains will be expanded.

2. Message centers
   a. offer good scalability for the OEM and third party.
   b. can be used with restrictions for end-customer interaction: text message with limited active content (e.g., geolocation, telephone number), offer return channel for confirmation or similar.
   c. are available immediately.
   d. thus meet the functional requirements of third parties with respect to a large range of use cases, but are limited with respect to interaction possibilities.
   e. standardized formats must be developed.

3. OEM native apps (OEM app store)
   a. offer very limited scalability via OEMs and third parties.
   b. offer extensive end-customer interaction.
   c. are partially available.
   d. thus completely meet the functionalities of the third parties.

Based on the criteria evaluated, an OEM-side offer and the use of technologies 1 and 2 by third parties is recommended (see figure "Technologies assessment"). In addition, third-party offerings must be identifiable as such.
At the moment, Solution 3 does not fulfill the criteria, as it requires extensive development, validation and approval processes (per app and OEM) and thus does not scale.

Various technologies that enable third-party access to the HMI are already available today. However, only two can be used scalably by OEMs and third parties. These can be combined with off-board and onboard APIs as described in Section III.7.1.

III.8. Access via the onboard diagnostic (OBD) interface

All data and functions available to the manufacturer's workshops via the OBD interface are also made available without discrimination to third-party providers. Access details are laid down in the EU Type Approval Regulation 2018/858, Annex X, No. 2.9. If vehicle manufacturers have taken measures, e.g., the introduction of certificate diagnostics, as part of the implementation of UNECE Regulation R155 and R156 (Cybersecurity and SUMS), these will also be made available to independent market participants without discrimination, subject to verification/obtaining the relevant certificates.

The OBD access is retained for repair and error diagnostics. The OBD interface is modified in accordance with the new requirements and per the state of the art. Data are made available as described in Section III.7.

IV Progressive recommendation for action from a holistic concept for the automotive sector

The ADAXO concept enables access to vehicle data in a manner that is more secure, more competitive and fosters innovation.

The objectives and recommendations for action are summarized in this concluding section.

IV.1. Premises and primary objectives

The two elementary objectives of ADAXO are:

- **“We empower customers to create added value for themselves and society using vehicle and mobility data.”**
  The decision about the user of personal vehicle and mobility data lies directly with the customers (authorized parties). They alone decide where the added value from the sharing of their data should be created in order to make their personal mobility and mobility for all safer, more sustainable and more convenient.
  The VDA member companies have focused their concepts on the customers, enabling them to generate added value from their data.
  The recommendations for actions are intended to establish the conditions required in fair collaboration with other market participants.

- **“We support the direction taken by the European data strategy to foster innovations and future-oriented business models.”**
  Vehicle and mobility data are an important lever for fostering innovations and business models that will make Europe competitive for the future. These can be new business models of startups, for example, that arise from the merging of widely diverse and also explicitly cross-sector data sources. However, even established business models, e.g., in the independent maintenance and repair sector, can improve their added value and services through the use of data.
  All of this contributes to making the European economic zone more globally competitive and resilient. The VDA member companies see it as their obligation to also contribute in the data economy to Europe’s future viability. European values and principles, which are formulated in the European data strategy, are the foundation of how we go about this.

The following conditions must be met:

- **Safety first**
  A car is not a smartphone. Access to vehicle data can only occur with uncompromising attention to the safety of the vehicle and its occupants. No innovation and no business model justifies jeopardizing vehicle users or the inappropriate use of their personal data. Absolute compliance with all applicable regulations regarding cybersecurity, data protection and software update management is the framework for ensuring this level of safety.

- **Fairness**
  The VDA member companies agree that added value from data can only be created on the basis of business models that work for all involved. The common objectives can only be reached if all market participants share data.

IV.2. Recommendation for action to implement a data economy within the automotive industry

With the joint ADAXO concept, the VDA member companies support the objectives of the European Union and thus also explicitly the objectives of the EU data strategy for strengthening Europe's data economy, and also the defined objective of creating a digital single market.[8] The technical framework and implementations required for this – see Section III – make it possible, whilst ensuring compliance with the FRAND conditions and with the extended vehicle concept, to further foster data use and data exchange for third parties seeking data. Furthermore, the systemic integrity of the vehicles and accordingly the imminent safety of all road users can be ensured in accordance with essential safety aspects (incl. cybersecurity) and thus make a relevant contribution in the direction of Vision Zero[9].

Core elements therefore also include the continued participation of market participants in new innovations and business models as well as a harmonizing approach to be strived for within the European Union. In light of this, we recommend ensuring consistent compatibility with horizontal regulations (incl. Data Act and Data Governance Act).

The German automotive industry therefore recommends the following actions:

(1) **Data sovereignty:** Access to data is always provided while preserving the customer's data sovereignty and while ensuring cybersecurity on the basis of the extended vehicle concept and under FRAND conditions.

[8] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52015DC0192&from=EN
[9] https://op.europa.eu/en/publication-detail/-/publication/d7ee4b58-4bc5-11ea-8aa5-01aa75ed71a1

(2) **Authorization management:** The decision-making authority regarding the use of the data ultimately resides with the customer. The transparent and central administration of authorization management at the OEM for the customer also achieves this within the context of cybersecurity and the OEM's overarching responsibility for customer safety.

(3) **Protection of third-party business models:** It is both technically and contractually ensured that commercial tracking of the data or use cases of third parties is precluded. Accordingly, use of the extended vehicle interface for third parties – individual service providers, marketplaces in the meaning of intermediaries – ensures that the monitoring of use cases can be precluded. Monitoring within a dedicated scope is necessary in light of certain legal, contractual and/or security reasons, as well as for the optimization of data transfer and authorization management.

(4) **Transparency about available data:** Transparency about the available data (Category A)[10] of an individual OEM is to be ensured via a viewable data catalog per OEM. The catalog is made available in electronic format via the extended vehicle concept or a corresponding web interface. Further data can be added successively to this catalog due to technical expansions and new vehicle generations. It is also possible to add additional data to Category A on the basis of individual B2B contracts.

(5) **Uniform framework:** Development of a uniform framework for the description of vehicle data with the aim of creating enhanced transparency and understanding on the part of data users. Accordingly, a common terminology in the sense of a meta data description is to be developed together with more than just the OEMs.

(6) **Data set for value-added services:** There is a consensus for the development of a basic, initial and cross-manufacturer data set for cross-manufacturer value-added services. The goal is a non-static data set that will develop and adapt over time.

(7) **Approach:** The premise of an overarching data set and thus also the essential, constant further development of the same is a basic use case and thus a logic based on added value. This use case is to be established by means of a structured forum. It is essential here that any third parties wanting to use the OEM's data as well as the data providers consider and prioritize the concrete data requirements in derivation of relevant use cases, and finally assess them under the premise of general economic viability. Furthermore, it should be emphasized as a basic hypothesis that the current data basis will fundamentally and constantly expand and continue to develop due to new vehicle generations.

The structured forum should be conducted with the involvement of the relevant data users and the individual OEMs. It is also urged that the EU Commission play a leading role, for example as the organizer and moderator, so that the essential neutrality of the forum is maintained.

The German automotive industry is convinced that the ADAXO concept will make a substantial contribution to the implementation of the European data strategy. We will actively promote its implementation and call on all interested parties to help shape it.

[10] See Section III.7

V Attachments

V.1. EU Commission study: TRL remedy measures and initial evaluation

The study commissioned by the European Commission includes the following recommendations for action, which the study concludes are necessary for the establishment of a functioning data market.

1. Availability of data and functions catalog
   Transparency about the availability of data across manufacturers is particularly necessary for the efficient development of independent, third-party services based on vehicle data.

2. Standardization of data and functions
   A standardization of the data and functions for services (reading/writing) is intended to make the purely technical vehicle signals more efficiently usable and to describe them as independently as possible from manufacturer and vehicle generation (e.g., vehicle signal specification, VSS).

3. Minimum functions and minimum data set(s)
   The availability of data and functions across manufacturers is particularly necessary for the development of independent, third-party services based on vehicle data. This should make possible the initial enabling of third-party multi-brand services with the aim of establishing an ecosystem that continues to grow on the basis of supply and demand.

4. Standard contract terms for B2B contracts
   If permissible under antitrust law, uniform contract components would be particularly welcome for the efficient development of independent, third-party services based o n data.

5. Maximum fees for data/function access
   Demanding a maximum price can safeguard the provision of new business models. This demand can also have a prohibitive effect on the data offering, however.

6. Preventing inappropriate business intelligence by resource provider
   The demand for the prevention of data access analysis serves to protect new business models in development by third parties.
   One has to differentiate between read data access to the OEM back end (without affecting vehicle systems) and remote diagnostic support (RDS) to the vehicle via the OEM back end, since a regulated transfer of liability from the OEM to the service provider must be ensured in the event of direct access to the vehicle.

7. Preserving unencrypted OBD access
   All data and functions available to the manufacturer’s workshops via the OBD interface are also made available without discrimination to third-party providers. Access details are laid down in the EU Type Approval Regulation 2018/858, Annex X, No. 2.9.

8. OEM connectivity contract without bundled services
   Data transmission by the vehicle is coupled to a service offer by the OEM, and thus so is the data transmission for third parties. A basic connectivity should make it possible for third parties to offer end customers services on an equal footing.

9. Maximum response times for OEMs
   Data and functions should be available in the same quality (latency and trigger) to all market participants (OEMs and third parties). The process of providing new data and functions should strive for market-typical response times to which customers are accustomed when using digital end products and the services based on them.

10. Access to remotely available data and functions based on fair, reasonable and non-discriminatory (FRAND) principles
    In contrast to purely read access to vehicle data stored in the back end (i.e., without affecting the vehicle itself), there are additional risks to the integrity of the vehicle systems and their operational safety when there is a write (or read and write) connection to the vehicle and to its data and resources – i.e., remote diagnostic and maintenance functions. The applicable principle for access by authorized third parties is that they receive access to such remote diagnostic services and functions at the same time and to the same extent as the respective manufacturer's authorized dealerships, workshops and service providers.

11. Reporting information to Commission to monitor compliance with FRAND principles
    Reports on this subject will be submitted to the EU Commission by the manufacturers, service providers or neutral servers.

12. Separation of duties
    The access approver and data holder are not consolidated in one role. The customer, not the data holder, approves access to the data. One has to differentiate here between read data access to the OEM back end (without affecting vehicle systems) and remote diagnostic support (RDS) to the vehicle via the OEM back end. The process must differentiate between OEM, telematic customer (the OEM's contractual partner for the telematic scope) and service providers.

13. Onboard application platform
    Enables access to data, functions and resources in the vehicle as well as the interfaces to the customer within the framework of the technical conditions. Additional interfaces must be provided in the vehicle for this. This means that access is provided down to levels that are relevant to safety and vehicle approval.
    The development of software for vehicle systems and software for data provision are subject to clear guidelines, such as requirements specifications, manufacturer-specific standards and design guidelines, industry-wide security and functional safety guidelines, and regulatory framework conditions. The vehicle manufacturer is always responsible for the integration, functional safety and security, as well as configuration and resource management. The OEM must therefore ensure at all times that data collection and data use are free of repercussions. This is only possible through the controlled use of data collection and functions. Controlled areas of use must be defined with the vehicle manufacturer for this purpose.

14. Specific consent management and identity validation procedures for ExVe

The foundation for data collection and use is the explicit consent of the customer for a specific purpose. With respect to identity validation, one has to differentiate between read data access to the OEM back end (without affecting vehicle systems) and remote diagnostic support (RDS) to the vehicle via the OEM back end, since a regulated transfer of liability from the OEM to the service provider must be ensured in the event of direct access to the vehicle.

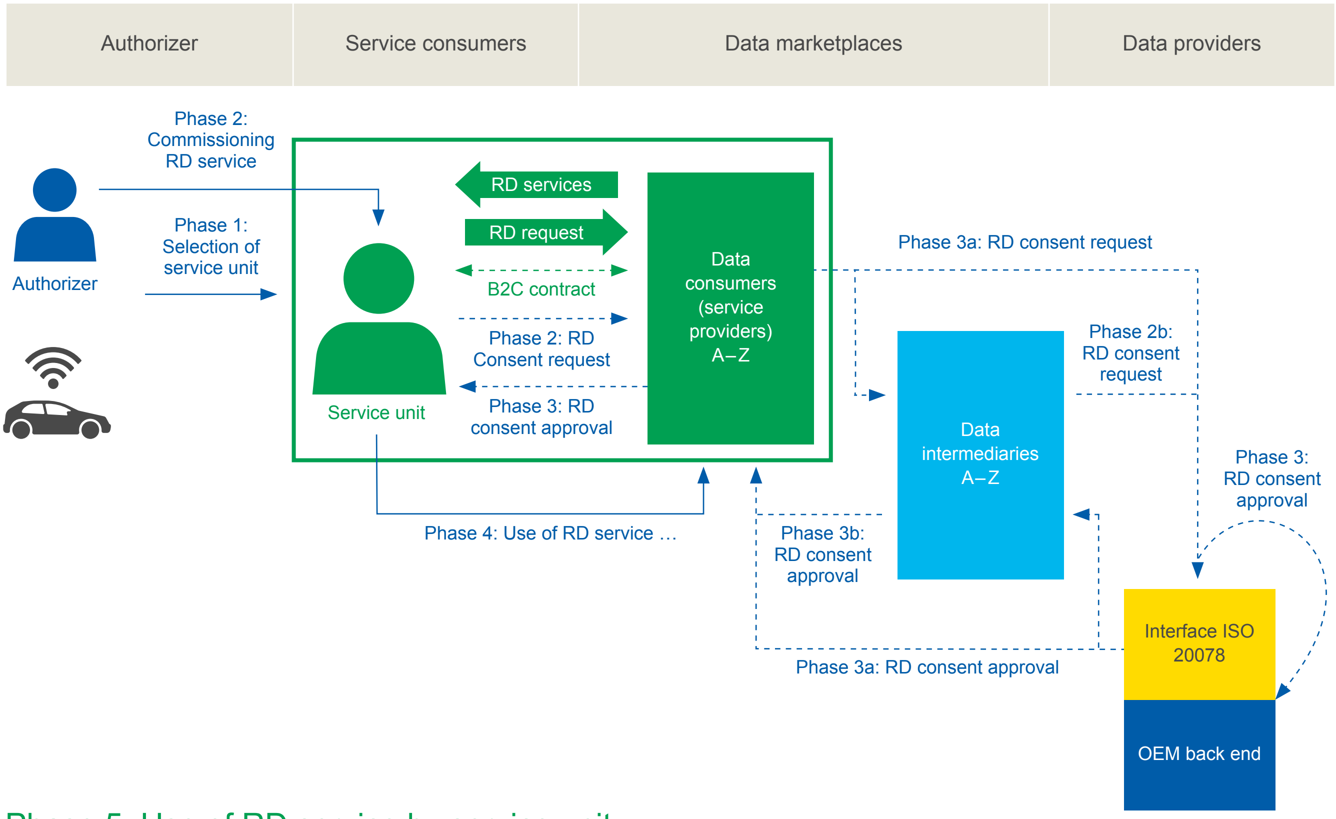
V.2. Detailing remote diagnostic processes

Remote diagnostic (RD) – Customer journey

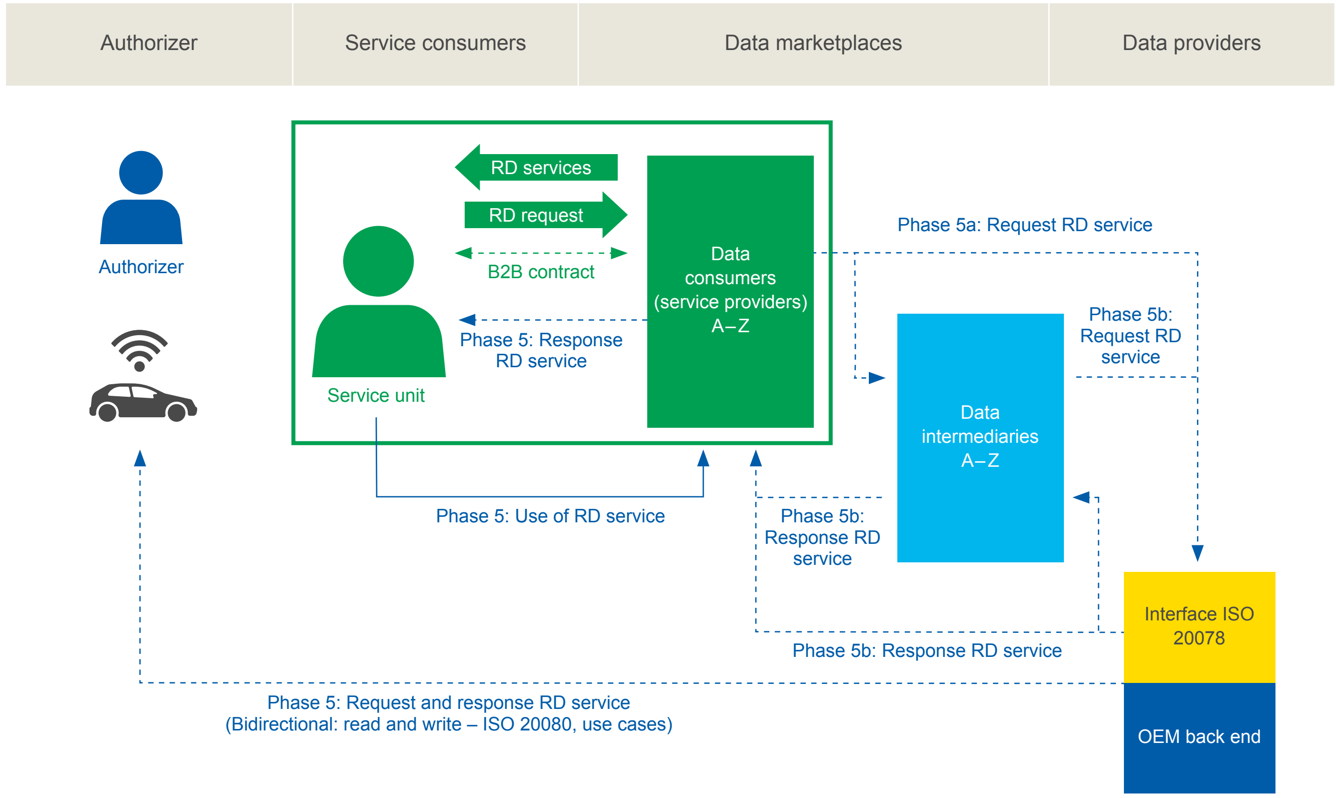
Activity stages:	Phase 1***: Selection of RD service **Authorizer**	Phase 2: Ordering of RD service **Authorizer**	Phase 3: Consent **Authorizer**	Phase 4: Use of RD service by **service unit**
Action:	**Authorizer** chooses RD service of a **service unit*** via an RD **service provider****	**Authorizer** commissions the service unit* to perform RD via RD **service provider****	**Authorizer** gives RD **service provider**** (poss. **intermediary)** consent, to request data bidirectionally via **OEM** (read and write)	**Service unit*** uses the RD service provided by the RD **service provider****
Touchpoint:		• RD service provider web interface • (Poss. Intermediary web interface)	• RD service provider web interface • (Poss. Intermediary web interface) • OEM web interface via OAuth	• RD service provider web interface
Actor:	• Authorizer	• Authorizer • Service unit • RD service provider (poss. commissions intermediary)	• Authorizer • RD service provider (poss. commissions intermediary) • OEM	• Service unit • RD service provider (poss. commissions intermediary) • OEM
Environment:		• Access to RD service provider interface	• Access to OEM interface	• Access to RD service provider interface • Access to the vehicle
Description:	• Authorizer decides that the commissioned service unit* can consume the RD service of an RD service provider** • RD service provider** is a qualified service provider for diagnostics (RMI) • Authorizer accepts read and write access to the vehicle by the RD service provider** (poss. intermediary)	• Authorizer commissions the service unit* with the performance of the RD via the RD server of the RD service provider** and triggers the consent process • Authorizer is informed that the service unit* is performing a diagnostic session via the RD service provider**	• Authorizer consents that the RD service provider** may provide the RD service for the service unit** (poss. via intermediary)	• Authorizer uses the RD service via the service unit* through the RD service provider**

* Individual service unit performing the work = service consumer.
** Remote diagnostic service provider = data consumer.
*** Presuming: Authorizer is already registered with the OEM and the vehicle is linked to a user account.

Remote diagnostic consent process (Phase 1 – 4)


Authorizer
Service consumers
Data marketplaces
Data providers
Phase 2: Commissioning RD service
Phase 1: Selection of service unit
Authorizer
RD services
RD request
B2C contract
Phase 2: RD Consent request
Phase 3: RD consent approval
Service unit
Data consumers (service providers) A – Z
Phase 3a: RD consent request
Phase 2b: RD consent request
Data intermediaries A – Z
Phase 3: RD consent approval
Phase 4: Use of RD service …
Phase 3b: RD consent approval
Interface ISO 20078
Phase 3a: RD consent approval
OEM back end

Phase 5: Use of RD service by service unit


Authorizer
Service consumers
Data marketplaces
Data providers
Authorizer
RD services
RD request
B2B contract
Phase 5: Response RD service
Service unit
Data consumers (service providers) A – Z
Phase 5a: Request RD service
Phase 5b: Request RD service
Data intermediaries A – Z
Phase 5: Use of RD service
Phase 5b: Response RD service
Interface ISO 20078
Phase 5b: Response RD service
Phase 5: Request and response RD service (Bidirectional: read and write – ISO 20080, use cases)
OEM back end

V.3. Glossary

Abbreviation	Meaning
ADAXO	Automotive Data Access – Extended & Open
API	Application Programming Interface
ASIL	Automotive Safety Integrity Level
B2B	Business to Business
B2C	Business to Customer
B2G	Business to Government
CPU	Central Processing Unit
CSMS	Cybersecurity Management System
DA	Data Act
DGA	Data Governance Act
DMA	Digital Markets Act
DSA	Digital Services Act
GDPR	General Data Protection Regulation
ECU	Electronic Control Unit
ExVe	Extended Vehicle
FRAND	Fair, Reasonable and Non-Discriminatory
HMI	Human Machine Interface
HW	Hardware
NHTSA	National Highway Traffic Safety Administration
OBD	On-board Diagnostic
OEM	Original Equipment Manufacturer
RAM	Random-Access Memory

Abbreviation	Meaning
RDS	Remote Diagnostic Support
ROA	Remote Online Access
SUMS	Software Update Management System
SW	Software
TRL	The TRL group of companies based in Crowthorne House, UK, is part of the Transport Research Foundation (TRF).
UNECE	United Nations Economic Commissions for Europe
V2V	Vehicle-to-Vehicle Communication
VO	Regulation
VSS	Vehicle Signal Specification

Contact Persons

Dr. Joachim Damasky
Managing Director
joachim.damasky@vda.de

Matthias Krähling
Head of Department Automotive Technologies and Ecosystems
matthias.kraehling@vda.de

Dr. Joachim Göthel
Senior Consultant
joachim.goethel@vda.de

Angela Pasch
Senior Consultant
angela.pasch@vda.de

Publisher German Association of the Automotive Industry
Behrenstraße 35, 10117 Berlin
www.vda.de/en

Copyright German Association of the Automotive Industry

Reprinting and all other forms of duplication are only permitted with indication of the source.

Version Version 1.0, December 2021

@VDA_online
Verband der Automobilindustrie