xapix

2020

# Best Practices and Guidelines for Data Governance and Standards in Automotive

Whitepaper

xapix.io

# Foreword

Data is one of the most important pillars of digitalization and the driving force for smart innovations in the field of mobility. In 2016, the Federal Ministry of Transport and Digital Infrastructure (BMVI) established the mFUND financial assistance programme. With the mFUND, the BMVI has since been promoting more than 180 projects that use data to develop applications which will improve mobility in our country. Regarding substance, data governance is one of the funding priorities within the mFUND, since without common standards and rules, we will not be able to turn our vision of automated and connected mobility into reality.

The mFUND project Smart API examines the conditions for the introduction of common data standards for the automotive industry. With connected and autonomous vehicles it is all about communication. The exchange of data that is necessary for connectivity goes hand in hand with numerous questions and challenges, for instance, what sort of data will be produced? How and were will these data be stored? How do businesses deal with personal data? To whom do the data "belong"? What do the various stakeholders expect?

The present White Paper addresses these questions and examines challenges and possible solutions for data governance in the automotive industry.

I hope you enjoy reading it.

**Steffen Bilger**
Parliamentary State Secretary at the Federal Ministry of Transport and Digital Infrastructure

# Contents

# The challenges facing the automotive tech space today

Connected cars and autonomous vehicles are all about communication—with each other and with their surroundings.

The exchange of data brings a variety of questions and challenges, currently under particular scrutiny in Europe and the US: What kind of data is produced? Where and how is this data stored? How do companies handle user-related data and automatically generated data? Who owns it? And what are the needs of the different stakeholders involved?

This paper takes a closer look at these challenges, putting forward a broad picture of the vehicle data economy as it stands and looking at the implications for the future.

It will look at data storage and usage concepts; current data standards and standards in communication; governance and the handling of personal data in the European Union and the US, offering insights into a key legal discussion: the ownership of vehicle-generated data. Finally, the interests of different stakeholders will be considered: What is important for all parties involved?

# Vehicle data categories

The German Association of the Automotive Industry/Verband der Automobilindustrie (VDA) defines four data usage categories.[1]

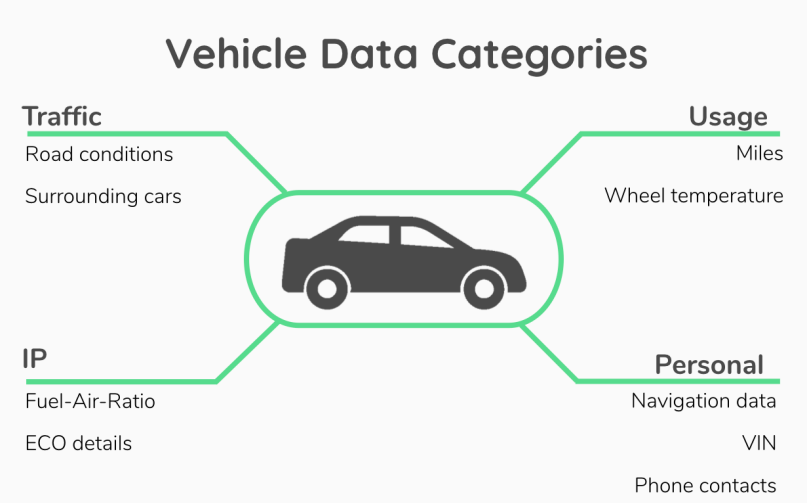


**Figure 1: Vehicle data categories**

**Traffic data:** traffic related data can be released anonymously to public services, such as police and fire brigades, supporting them

[1] In order to meet the needs of the various stakeholders, the vehicle-generated data is divided into four categories of use. It is possible that individual data elements can be found in multiple categories.
Category 1
In category 1, data relevant to traffic safety is made available anonymously. This data is made available to public services so that traffic control centers, fire brigades and police can use them to optimize traffic safety.
Category 2
Category 2 data is anonymized and available across manufacturers. This data forms the foundation for the development of new services, business models and innovations, as well as the optimization of traffic.
Category 3
In order to prevent the theft of intellectual property and patented technologies, anonymous manufacturer-specific data is made available in category 3, which is exclusively available to the respective original parts manufacturer. This supports fair competition and contributes to the further development and improvement of the vehicle and vehicle components.
Category 4
Many services that are tailored to individual needs and increase the comfort of the consumer require personal user data. This is only made available in category 4 with the express permission of the consumer. Data protection is the top priority for the German automotive industry.
https://www.vda.de/en/topics/innovation-and-technology/data-security/data-usage-categories.html
(retrieved on 20.9.2019)

in keeping the public space safe. Early alert systems are able to operate in real time.

**Usage data:** used for different services and business models, the required data is released anonymously to third parties in order to develop new products. Telematic data can be included, as well as traffic-related data. This category will drive future innovations.

**IP data:** this category contains data sets relevant to intellectual property. This data is available solely to the original equipment manufacturer (OEM) and its contractual partners; its use is in order to further improve the OEM's vehicles and to gain valuable insights on the lifecycles of its products under real conditions. The new dimensions of evaluable data are likely to optimize certain mobility concepts to a new level, also enabling the creation of more brand-specific services.

**Personal data:** in order to offer a service tailored to an individual, it is necessary to gain information on that driver's behaviour, only possible if the individual gives their consent. With privacy more valued than ever, personal data requires special treatment; since the introduction of the General Data Protection Regulation (GDPR), severe penalties for data breaches can be imposed on companies.

These four categories consist mostly of technical data gathered through the telematics system of the connected vehicle and from roadside infrastructure. Communication between connected vehicles and infrastructure leverages the positive effect of data usage on traffic safety; in addition, fuel consumption is expected to decrease through intelligent analysis of operating states and following recommendations for travel speed and in advance-phased traffic lights.

The data offered is different for most OEMs and for different models. Most of the premium segment vehicles are equipped with more sensory technology than the average car and can therefore offer a wider range of data points which, in turn, can be used to offer other, more personalized services. OEMs use different ways of contributing data through their application programme interfaces (APIs). Much of the telematic data differ in data types, saved in different units. This results in many different data sets, which need to be standardized in order to process them effectively.

As seen in the table below, each of these OEMs provides data on tire pressure, but in different formats. Mercedes uses the absolute value of 'kilopascal'; in comparison GM uses 'gauge value'. The difference is the reference point used to calculate the pressure value. In absolute pressure, a perfect vacuum is used as reference; for gauge pressure, it is the surrounding atmospheric pressure. Meanwhile, Porsche provides the tire pressure in bar—i.e. 1 bar equals 10,000 pascal—also offering the value as a float.

Therefore the introduction of certain standards and integration tools is essential.

| | Tire Pressure | Battery/Fuel status | Accele-ration | Speed |
|---|---|---|---|---|
| **Ford** | - | 78 % (number) | - | 100 km/h (number) |
| **Mercedes** | 200 kPa (integer) | 78% (number) | - | 100 km/h (number) |
| **GM** | 200 kPaG (integer) | 78% (number) | - | 100 km/h (number) |
| **PSA** | - | %*** | 63%* | 100 km/h (number) |
| **Porsche** | 2 bar (float) | 0.78 (float) | 0.7 (gforce) | 100 km/h (number) |
| **BMW** | - | 78% (number) | 0-5 stars** | - |

* acceleration pedal activated
** evaluation of driving style
*** documentation doesn't include clear information

## Data storage concepts

Today there are three different concepts determining the handling of vehicle-generated data, two of which are already implemented and working.

The first is called ‘extended vehicle concept’. OEMs transfer any data generated to their own proprietary servers, with access to car data only possible through their external server. Many experts criticize this concept, as it puts the OEM in a position of monopoly —the OEM can decide who should have access to the data. OEMs argue that it is the only way to guarantee the security of personal user data. Currently, there is no regulatory framework to deal with this situation although an ISO standard (ISO standard 20077-1) on this technical concept offers a step towards interoperability.

Whilst from a technical perspective, the second concept, the ‘neutral server’ or ‘shared server’ offers the same solution, the data is not under the exclusive control of the respective OEM. A neutral entity operates the server and grants access to any third party under the same non-discriminatory conditions. This setup gives consumers or fleet owners full control over their data, thereby following the ethos of consumer data-focused regulations such as GDPR and California Consumer Privacy Act (CCPA), while offering the possibility of giving access to multiple makes and models of different OEMs, as long as mutual contractual agreement is reached.

Otonomo, Caruso, IBM and others already operate neutral servers although, while neutral from a technical perspective, concentration in a single server can also result in a monopolistic setup. The aim is to offer many different neutral servers in order to create a diverse environment, thus eliminating the possibility of monopoly. However, providing real-time data to a third party will become increasingly important to emerging services and applications and the use of an external server renders this impossible.

Finally, in the third concept, the ‘on-board application platform’, the operating platform is the vehicle itself i.e. data is stored and sent from the car. As the consumer makes the decision as to whether or not to give consent to any third party, this approach guarantees privacy and it would be possible to fully personalize services to an

individual. But the debate around the 'on-board application platform' relates to its security—the different read and write operations associated with the 'on-board application platform' mean that the vehicle could be a potential target to cyber-attacks. The OEMs state that, because of the different architectures that would be needed to operate on a car's system, the platform will not be able to protect consumers' data properly, while IT specialists state that a well-designed open source solution would improve the security of consumers' data, as well as the cyber security of the whole vehicle.

At this point, the 'on-board application platform' is still at an early stage; before such a platform can be implemented it is crucial for all the stakeholders involved to agree on unified standards and guarantee interoperability between different makes, models and services.[2]

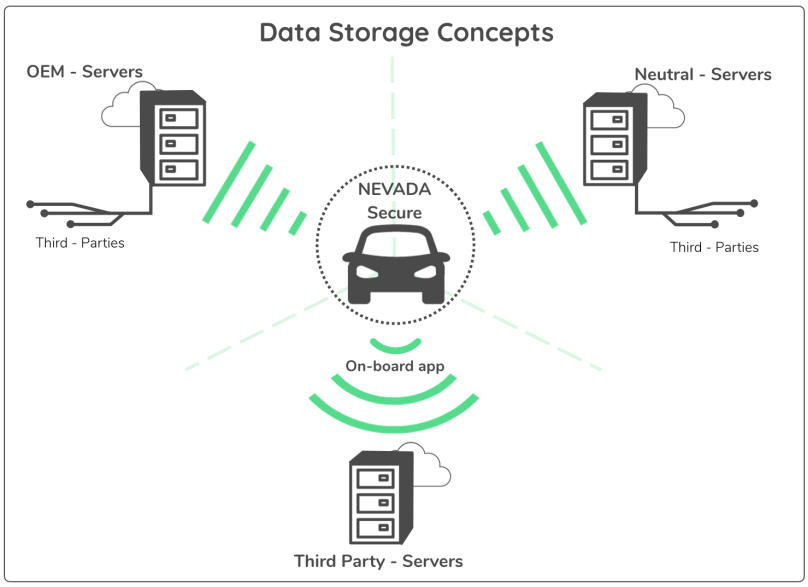


**Figure 2: Data storage concepts**

[2] McCarthy, M., Seidl, M., Mohan, S., Hopkin, J., Stevens, A., Ognissanto, F. Access to In-vehicle Data and Resources: Final Report, May 2017. https://ec.europa.eu/transport/sites/transport/files/2017-05-access-to-in-vehicle-data-and-resources.pdf

## Data standards

As we have seen, there is a need for unified standards across the automotive industry and for the other stakeholders involved, including cities, to make use of the full potential held by connected vehicles. It is important for every participant to rely on provided data sets in order to build seamless mobility solutions for all the different connected devices, vehicle makes and models. (Many different standards exist for different tasks. Rather than considering a complete list of all existing standards, including those relating to technology or communication, this paper focuses on data standards.)

SAE and ISO are developing more unified standards revolving around communications and security. Right now there are several SAE standards (SAE J3005-2, SAE J3138) under development, which will define best practices for cybersecurity. SAE and ISO are also currently collaborating on a cybersecurity standard for road vehicles (ISO/SAE CD 21434). This standard focuses on definition of terminology and processes for cybersecurity.

The technical committee ISO/TC 204 is defining standards for "Intelligent Transportation Systems" (ITS). ITS includes all different means of mobility, the ISO committee therefore develops standards which are linked to communication and control systems in the field of urban and rural surface transportation, including intermodal and multimodal aspects thereof, traveller information, traffic management, public transport, commercial transport, emergency services and commercial services.

The working group ISO/TC 22/SC 31 is in charge of data communications for vehicle applications. Their scope also includes data formats and standardized data content. Within the ISO 20078-2019 they have defined extended vehicle web services for already existing infrastructure. These web services work in an interoperable manner to ensure that third parties can use the existing infrastructure of vehicles just like the OEM.

W3C released its "Vehicle Information System Specification" in early 2018. It defines a WebSocket based API which enables client applications to get, set, subscribe and unsubscribe to vehicle

signals and data attributes. Aiming to enable consistent application development to all participating OEMs.

Mobility Open Blockchain Initiatives (MOBI) is a non-profit, smart mobility consortium that aims to improve the smart mobility sector by using the blockchain. Its members are OEMs, suppliers, NGOs and startups. Recently, MOBI released the first vehicle identity standard (VID) on blockchain. Ultimately, this identity standard will be able to identify a vehicle and its owner, as well as to share data, and transact with its environment and other vehicles, without intermediaries.

While the presentation of data on the same subject differs across some OEMs, some data sets are already presented in the same format.

| | **Mileage** | **Vehicle speed** | **Location** |
|---|---|---|---|
| **Ford** | Km (Integer) | km/h (Integer) | Latitude/Longitude (Degrees) |
| **Mercedes** | Km (Integer) | km/h (Integer) | Latitude/Longitude (Degrees) |
| **GM** | Km (Integer) | km/h (Integer) | Latitude/Longitude (Degrees) |
| **PSA** | Km (Integer) | km/h (Integer) | Latitude/Longitude (Degrees) |
| **Porsche** | Km (Integer) | km/h (Integer) | Latitude/Longitude (Degrees) |
| **BMW** | Km (Integer) | km/h (Integer) | Latitude/Longitude (Degrees) |

## Handling personal data

The GDPR is a consumer data-focused regulation, with the individual placed at the center of protection against data misuse by companies. The definition of  personal data in Article 4 of GDPR states that: "'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person."

The consent of the individual is needed to be able to process personal data.

Article 7 delivers conditions for consent. The 'controller'[3] must be able to demonstrate that consent was given; the declaration of consent must be easy to understand, with a clear description of what kind of data will be used for a specific case. The user must be able to withdraw consent at any given time and, if consent is withdrawn, data must be deleted without delay. Other conditions determine that data must be deleted e.g. the data is no longer necessary in relation to the purpose for which it was collected, it was unlawfully processed, etc. See Article 17 for more information.

Furthermore the individual holds a right to data portability (Article 20) and is able to receive and transmit personal data which was "provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance (...)". The transmission should be automated, if technically feasible.

[3] (7) 'controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union of Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law. Article 4, GDPR

While processing personal data, 'controller' and 'processor'[4] are obliged to ensure a certain level of security. Article 32 clarifies these conditions. The pseudonymization and encryption of personal data is the most crucial part.

'Pseudonymization' is the processing of personal data in such a way that it can no longer be attributed to a specific data subject without the use of additional information. As the scope of different data sets is broad, use cases define which data must be pseudonymized. Data which relates to an individual person must always be anonymized, e.g. VIN, name, license plate, most-visited places, etc.

There are certain conditions in which no consumer consent is required to process data:

**The processing is necessary to carry out a contract**
Vehicle servicing providers may need to process in-vehicle personal data about a vehicle owner (e.g. information about the way and distance that the vehicle owner has driven the vehicle) in the course of carrying out maintenance on the vehicle.

**The processing is necessary to protect the vital interests of the data subject**
Emergency services need to access in-vehicle data about the subject at the scene of an accident.

**The processing is necessary to carry out a public function**
A law enforcement agency is mandated to collect and analyze information about the way in which a vehicle has been driven.

GDPR applies to all companies processing the personal data of subjects residing in the EU, regardless of the company's location. This applies to a controller or processor not established in the EU, where the activities relate to offering goods or services to EU citizens (irrespective of whether payment is required). Non-EU

[4] (8) 'processor' means a natural of legal person, public authority, agency or other body which processes personal data on behalf of the controller.
(2) 'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction; Article 4, GDPR

businesses processing the data of EU citizens are obliged to appoint a representative in the EU.

Severe penalties can be imposed on non-compliant companies, ranging from up to 10 million euros or two per cent of their annual revenue (whichever is the greatest) on relatively small infringements and up to 20 million euros or four per cent of their annual income for higher-level infringements.

## US data-privacy laws in comparison to GDPR

The CCPA will come into effect on January 1st 2020 with other state laws following suit. Naturally there are differences and similarities between the application of US data-privacy laws and GDPR laws.

The GDPR applies to all kinds of businesses, national bodies and institutions as well as to non-profit organizations; effectively, no-one is exempted. The CCPA applies only to profit-oriented businesses and their service providers and defines thresholds on this matter. Requirements include: the entity does business in California, exceeds $25 million annual revenue and processes the personal information of more than 50,000 individuals for commercial purposes.

There is also a difference in territorial scope. The GDPR also applies to entities outside the EU, if they do business within the EU, whereas the CCPA only applies to organizations that are either based in California or use personal data of citizens for doing business in California, while not being based in California.

The legal basis for processing personal data is very different between GDPR and CCPA. According to EU law, some 'a priori' criteria must be met in order to process personal data (see Article 6), whereas in the CCPA only 'a posteriori' measures must be met, e.g. a mechanism to delete or prevent the sale of personal information.

While both regulations offer a right to object to further processing and selling of personal data, this right to objection differs widely. In GDPR the withdrawal of consent forbids any further processing of personal data, even for non-commercial measures although, if the processor can demonstrate compelling legitimate grounds for processing personal data, this can continue. CCPA's right to object is absolute and strictly forbids any further selling of an individual's data, although that does not mean that the private data cannot be used for other purposes.

Both regulations include a section dealing with monetary penalties, if a company is non-compliant. The major difference is that, in the

EU, administrative fines can be issued directly by a data protection authority, whereas only a civil court can issue a penalty in California.

The criteria for triggering a data breach in the CCPA is an “unauthorized access or acquisition” of sensitive personal data such as a social security number or credit card number. The GDPR has a broader definition: “breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data.” Personal data is also defined as any data which can be directly or indirectly associated with an individual. But only those data breaches which pose a risk of harm to rights and freedoms must be reported; this concept is not included in the CCPA data-breach laws. In GDPR, breaches must not be reported if there were “appropriate technical and organizational measures” in place, such as encryption.

The US model is stricter: Here, breaches which contain encrypted data in storage or transit must be reported.

A breach must be reported within 72 hours according to GDPR; the report can also be provided in phases. Reporting in the US must be between five and 30 days. If a breach poses a risk to the rights and freedoms of an individual in the EU, the company must notify its lead data protection agency (DPA) as well as the individual if the risk is high. The report must specify the nature of compromised data, the number of subjects affected, the name of the data protection officer (DPO), likely consequences for the data subject and measures taken to reduce the risk to the individual. Third party data processors are also obliged to report breaches to their clients “without undue delay after they become aware.” In the US, affected individuals must be notified, as well as state attorneys and federal agencies.

GDPR requires companies to document the facts that led to the data breach and remedial action taken to prevent a recurrence. The US model does not require companies to do so, although many companies will voluntarily.

Another difference between the GDPR and CCPA concerns the ‘right of deletion’, where an individual holds the right to know what information a company holds about them and to ask for it to be deleted. The GDPR strongly supports the protection of personal

data over business interest, where the CCPA's tendency is to favor the role of data as a commercial asset.

The CCPA applies only in California, with other US states likely to publish their own regulations—Nevada passed its own data security law in May 2019.

With so many approaches to data protection, vigilance will be required in order to remain compliant in processing personal data; any enterprise needs to be clear about where and how it gathers and processes personal information, keeping a critical eye on its data governance.[5] [6] [7] [8]

**GDPR vs. CCPA**

| | GDPR | CCPA |
|---|---|---|
| **Right to object further processing & selling of personal data** | Withdrawal of consent **forbids further processing** of personal data (unless there are compelling reasons to process data) | Absolute - **strictly forbids** further selling of individual's data; private data may be used for other purposes |
| **Monetary penalties** | Administrative fines can be issued directly by **data protection authorities** | Only **civil court** can issue penalties |
| **Data breach criteria** | "**Breach of security** leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data" | "Unauthorized access or acquisition" of **sensitive personal data** (e.g. SSN, credit card info) |
| **Right to data portability** | **Has limitations** - if a consumer wants access to personal info or wants to transfer info to another entity, the entity must only transfer info provided by consumer | Merged with the right to access; **no limitations** – if a consumer wants access to personal info or wants to transfer info to another entity, the first entity must disclose all info regarding the consumer |
| **Exemptions for right of deletion** | Only made for **public interests** (e.g. to exercise the right of freedom of expression and info) | Made for companies to **provide goods and services** to the consumer; also for public interests |

**Figure 3: GDPR vs. CCPA**

[5] Data breach notification: 10 ways GDPR differs from the US privacy model, pwc United States, December 2016. https://www.pwc.com/us/en/services/consulting/cybersecurity/library/broader-perspectives/gdpr-differences.html (retrieved on 20.9.2019)

[6] Data Guidance/Future of Privacy Forum: Comparing privacy laws: GDPR v. CCPA. https://fpf.org/wp-content/uploads/2018/11/GDPR_CCPA_Comparison-Guide.pdf

[7] Meyer, D., In the Wake of GDPR, Will the U.S. Embrace Data Privacy? Fortune. November 29, 2018 https://fortune.com/2018/11/29/federal-data-privacy-law/ (retrieved on 20.9.2019)

[8] Coos, A., EU vs US: How Do Their Data Privacy Regulations Square Off?
Endpoint Protector Blog, January 17, 2018 https://www.endpointprotector.com/blog/eu-vs-us-how-do-their-data-protection-regulations-square-off/ (retrieved 27.09.2019)

## Whitelisted countries

Whitelisted countries hold a data protection regulation which is adequate to the GDPR. Companies can easily transfer data between an EU member state and a whitelisted country (outside of the EU); no other safeguards are deemed necessary because the protection of transferred data is given. Article 45 of Regulation (EU) 2016/679 enables the European Commission to decide whether a non-EU country offers the same scope of protection.

For a country to be whitelisted, there must first be a proposal from the European Commission. The European Data Protection Board then has to check the national laws and give its opinion; representatives of other EU countries need to give their approval. Finally, the European Commission needs to adopt the decision.

The following countries have so far been recognized as adequate in protection: Andorra, Argentina, Canada (commercial organizations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland, Uruguay and the United States of America (limited to the Privacy Shield framework).[9] [10]

Adequacy talks are ongoing with South Korea.

[9] https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

[10] https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/rules-international-data-transfers_en

## Data protection in China

When talking about data protection, it is essential to look at one of the biggest economies in the world: China. The Chinese market and its companies are gradually becoming more important, particularly in the field of AI and e-commerce. Their champions Baidu, Alibaba and Tencent, to name just a few, are dependent on different extensive data sets, including personal data and, as a result, they have to comply with Chinese data protection laws, as does every company trying to compete in the Chinese market.

The Chinese data protection standards, Data Security Management Approach, are, to an extent, modeled on GDPR but have some basic distinctions; a single standard is not analogous to GDPR. More than 240 national standards related to cybersecurity have been developed by the China National Information Security Standards Technical Committee, as well as the Cyber Security Law, which came into effect in 2017.

Critical data, such as personal data, must be stored within Chinese borders. In the Chinese standard, personal information has a broader definition than in the GDPR; it includes data that could harm mental and physical health if abused, as well as other individuals, property or reputation. If a company seeks to gather personal data, the purpose has to be disclosed to the individual in detail. There are higher requirements for security testing—because of potential national security risks—not only in one standard, but overall. [11] [12] [13] [14]

[11] https://www.csis.org/analysis/new-china-data-privacy-standard-looks-more-far-reaching-gdpr

[12] https://www.chinalawblog.com/2018/05/china-data-protection-regulations-cdpr.html

[13] http://www.cac.gov.cn/2019-05/28/c_1124546022.htm

[14] https://assets.kpmg/content/dam/kpmg/cn/pdf/en/2017/02/overview-of-cybersecurity-law.pdf

## Ownership of data

Clearly personal data belongs to the individual while data which is considered intellectual property belongs to the OEM. But how about automatically generated data, which is neither personal nor protected as intellectual property? Does this data belong to the owner of the car or does it belong to the OEM that provided the facility to aggregate this data?

Currently, there is no legal framework or law which deals with this question and the problem is handled through contracts between consumer and OEM, most usually via general terms and conditions. Nevertheless, all in-vehicle data is transmitted directly to the OEM servers. Exceptions are personal data and data that is needed for repair and maintenance, as this can be accessed via on-board diagnostics (OBD) interface. As soon as personal data is anonymized, individual rights to this data expire and the OEM gains full control of this valuable information. Apart from the mandatory consent of the OEM to access in-vehicle data, no third party is able to communicate with the driver of a connected vehicle via the Human-Machine-Interface (HMI). As things stand, the connected vehicle is a closed system and the respective OEM is effectively the actual—though not legal—owner of all non-personal data.

The current official tendency is to favor the vehicle holder as the owner of vehicle-generated data. Germany is considering the creation of a law relating to the hierarchy of ownership of mobility data. The general idea is to implement licenses for data usage in order to support fair competition in the market, as well as full control for the individual over personal vehicle data. Measures will be implemented in copyright regulation at a European level, as the Ministry of Transport and Digital Infrastructure of Germany/ Bundesministerium für Verkehr und digitale Infrastruktur sets out.[15]

[15] For a detailed analysis see: Wolfgang Kerber, Data Governance in Connected Cars: The Problem of Access to In-Vehicle Data, 9 (2018) JIPITEC 310 para 1.

# Interests of different stakeholders

### Consumers

Consumers buy, lease or rent cars after which they are locked into the specific hardware and software architecture of the vehicle. Naturally a potential buyer expects a degree of choice in terms of alternatives in companies, services and products from which to choose and it is beneficial to provide third parties with data on which to base product development in order for them to be able to make a broad offer to the consumer.

The willingness to make a purchase—or to switch brands—on the basis of connected services continues to increase. The Chinese are most likely to switch brands and pay for connected services (nearly 60 per cent in 2015); in Germany only 20 per cent are willing to do so. Consumer surveys show that most people are aware of the value of their data and the way third parties can utilize this information and, while the majority are concerned about data security and privacy, consumers are most likely to grant access to their personal data for mobility services. A broad scope of different services is of interest for consumers, with the ability to personalize services potentially of interest across different consumer groups.[16]

### Original Equipment Manufacturers (OEMs)

The vehicle manufacturers, or OEMs, are responsible for the safety of their product. It is mandatory to avoid any potential risk across all product elements so, unlike most other connected devices, vehicles are rigorously tested in relation to security and safety. All the different functionalities of a connected car hold a specific risk for the OEM. Safety is particularly critical for uploading functions—such as updating an app—as these hold the potential for dealing with a range of safety hazards. On the other hand, OEMs need to offer the best service to their customers in terms of connectivity or, as recent studies have shown, they will lose customers.

As a result, OEMs are interested in a safe infrastructure for uploading and downloading data to their vehicles, while offering a broad and solid service to their clients without giving away too

[16] Source: McKinsey&Company: Monetizing Car Data, New service business opportunities to create new customer benefits.

many valuable insights on vehicle-generated data. The VDA has developed an interface called: “NEVADA share & secure” (Neutral Extended Vehicle for Advanced Data Access), a standardized concept, which allows only secure connections to the backend servers. The transmission of vehicle-generated data occurs simultaneously, meaning that aggregated data is available to all third parties at the same time. Other means of communication between vehicle and any device are not affected, including the OBD-II interface. The communication between vehicle and backend server is handled by each OEM with their own software which, the VDA states, is important for diversity, fair competition and security.

On the other hand, an open source solution would be as—or even more—secure as the provided software, because all the stakeholders involved as well as the developer community would be able to engage with improving the code and fixing problems.

### Other stakeholders

Stakeholders are mostly interested in the accessibility of vehicle-generated data and, as a result, have a strong interest in how data is stored and made available to the public. Currently, OEMs and neutral server providers are the only sources for such data, meaning that they can determine price and decide on what kind of data points will be provided. Some experts argue that OEMs can monitor the data access of independent service providers and therefore gather crucial insights to data usage, giving them an advantage on promoting their own services to the individual vehicle owner. An ideal development for stakeholders would be the separation of OEM from generated data, leaving the opportunity to create a free-flowing market for data. This could happen with the implementation of an “on-board application platform” though, with no sufficient standards in communication technology and security measures, this is rather unlikely in the next few years.

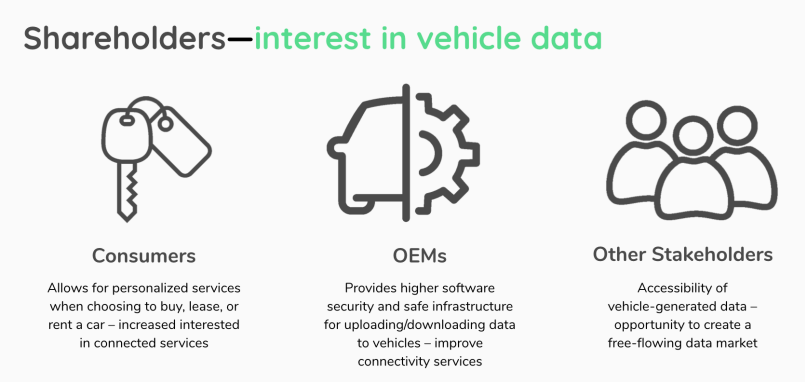


**Figure 4: Vehicle data shareholders**

# Conclusion

Of the many questions to be tackled in relation to the connected vehicle, currently the most important ones are:

In which manner should data be provided: via external servers or from the vehicle itself?
Who owns the automatically generated data: the one who aggregates them or the one who offers the sensory equipment to facilitate them?

People are more aware than ever of their digital footprint and how it influences their lives. As things stand right now, we should see a shift towards the consumer, because of privacy focused regulation entering into force in most countries around the world. Through the connected vehicle, the automotive economy has a symbiotic relationship with its participants; these participants have a genuine interest in fostering the data economy and expanding it.

We have travelled a good way towards implementing standards that will enable interoperability between different systems. The last mile on data integration is yet to be completed, but there are some sophisticated actors working out the final technical problems. By implementing standards on APIs and data formats, it will soon be possible to scale innovation in mobility services and simplify the access requirements for all stakeholders to a minimum.

The benefits are clear, but the way we approach them is not yet clearly defined.

## Xapix and the future of sharing data

At Xapix, we work on these integration tools and standards within the mFUND project. In the future it will be possible to share normalized data easily through the cloud to all stakeholders.

One key area our team focuses on is data integration. Xapix helps mobility companies to combine information from a variety of different sources, some as simple as an excel sheet or as complex as streaming data from multiple sources. Xapix helps to bridge the gap between different sources, systems and formats. Our projects with leaders in the automotive space—including Daimler Fleetboard, BMW and Goodyear—as well as our groundbreaking product development, has made Xapix an authority in that space. We have learned that common, shared data standards can be a key enabler and facilitator for the connected vehicle and digital mobility systems, as these standards can make it easier to access, connect and distribute data for the key players in the automotive space.

We are proud that our work with mFUND contributes to a growing knowledge base around connected vehicle data standards. There is a huge need to facilitate partner collaboration in the automotive and mobility space and, at Xapix, we are proud to be at the forefront of this movement.

Learn more about our product at www.xapix.io or reach out to us to discuss your questions and ideas: hello@xapix.io. We appreciate your feedback and look forward to hearing from you!

Xapix, Inc.
44 Tehama St
San Francisco, CA 94105
United States

Xapix Software GmbH
Ritterstr. 24-26
10969 Berlin
Germany

www.xapix.io
@xapix_io