European Automobile Manufacturers Association

ACEA COMMENTS ON EDPB GUIDELINES 1/2020 ON PROCESSING PERSONAL DATA IN THE CONTEXT OF CONNECTED VEHICLES AND MOBILITY RELATED APPLICATIONS

INTRODUCTION

ACEA welcomes the publication of the EDPB's draft guidelines on processing personal data in the context of connected vehicles and mobility related applications. It is very important for the automobile industry that data protection authorities across the EU, in working to the common goal of supporting the development of trusted connected vehicle services in a Digital Single Market, have a good and common understanding of how data protection rules should apply in the field of connected vehicles and mobility services. This facilitates compliance and ensures a level playing field for all actors.

We consider, however, that it is too early to move to the final version at this time. We recommend first, that the EDPB considers opportunities for industry stakeholder engagement so that the final guidance is achievable and strengthens customer trust in new connected technologies, and second, that these guidelines align with the requirements of the final ePrivacy Regulation.

To ensure legal certainty, we feel it is important that the EDPB guidelines be consistent with the guidance provided earlier by national data protection authorities. In France, the CNIL published a compliance package on connected vehicles and personal data in October 2017. In Germany, the data protection authorities issued a paper jointly with the automotive industry association VDA in January 2016. We are concerned that the content of these national guidelines is insufficiently reflected in, and in some cases conflicts with, the draft EDPB guidelines.

The automotive industry is keen to work with the EDPB to achieve pragmatic and operationally effective guidelines that allow suitable implementation of the privacy safeguards anticipated under the GDPR and related privacy rules. Both in France and in Germany, our sector was consulted in the development of their national guidance, had the opportunity to demonstrate how connected

vehicles work and had the ability to discuss with the authorities specific practical issues vehicle manufacturers face when designing such vehicles and the services that come with them. This consultation showed that connected vehicles differ in many ways from smartphones (see also https://www.cardatafacts.eu/) – differences that we believe should be reflected in the guidance.

Considering that these are the first EDPB sector-specific guidelines and that they will set the framework for assessing our sector's compliance with the GDPR and related privacy rules, we would highly appreciate being given the opportunity to meet with the drafters of the guidelines before the EDPB adopts the final version of the guidelines. On that occasion, we would like to illustrate some of the concerns expressed in this paper and organise a live demonstration of connected vehicles. We believe this would provide insights into the specificities of connected vehicles that would make it possible to enhance the effective implementation of the guidelines.

Finally, we find it unfortunate that the guidelines provide a detailed assessment of data processing in connected vehicles under the ePrivacy Directive at a time when that Directive is about to be replaced with a new ePrivacy Regulation that could differ, possibly significantly, from this Directive. This means that the guidelines, if published in their current form, risk being outdated very soon, creating a disjointed approach, potential confusion and costs in implementing requirements which have not yet been properly codified. We therefore believe it would be preferable to postpone and review the publication of the guidelines until the content of the new ePrivacy Regulation is known with certainty.

MAIN OBSERVATIONS

SCOPE

Connected vehicles

ACEA would welcome consistent definitions by EU regulators, in order to minimise confusion and aid data subjects' understanding of the industry. In particular, we recommend that there is a consistent definition of what constitutes a "connected" vehicle. The guidelines define the connected vehicle in a very broad manner, i.e. as "a vehicle equipped with many electronic control units that are linked together via an in-vehicle network as well as connectivity facilities allowing it to share information with other devices both inside and outside the vehicle" (§20).

In our understanding, connectivity implies that there is a connection between the vehicle and another remote device, and that data are transmitted from one device to another. This is reflected in national guidance including the CNIL's compliance package, which defines connected vehicles as "vehicles that communicate with the outside world (mobile applications, other vehicles,

infrastructure, etc)". It is also consistent with the distinction made by the German data protection authorities between "offline" and "online" vehicles.

The definitions used in both national guidelines help to clarify that the communication that occurs exclusively within an in-vehicle network should be outside the scope of the guidelines. If this were not the case, even vehicles produced in the 20th century that contain at least a few electronic control units (e.g. for anti-lock brakes, motor management or even powered windows) would be connected vehicles. This would defy common sense.

For reasons of consistency and clarity, we therefore suggest that the EDPB guidelines define connected vehicles in the same manner as the CNIL compliance package.

Professional use of vehicles

The guidelines specify that they focus in particular on the personal data processing in relation to the non-professional use of connected vehicles by data subjects (§ 19). The data processing carried out by employers providing company cars to members of their staff is said to be out of scope (§ 31).

We believe it is necessary to make it clear(er) in section 1.3.1 that also data processing in relation to commercial vehicles used for professional purposes (road transport, public transport, etc) is also not covered by these guidelines.

Data controller

The guidelines recommend that data be processed as much as possible inside the vehicle and state that if data must leave the vehicle, consideration should be given to anonymise them before being transmitted.

In our view, a "general" recommendation to anonymise data or separate it from the vehicle or from other personal identifiers does not depict the variety of possible services and use cases in the connected vehicle context. A clear differentiation should be made between use cases that do not require processing of personalised data (e.g. "live traffic") and services that do (e.g. services such as remote car status or remote control of auxiliary heating for specific customers that need linking to their other data or to a customer account).

We understand EDPB references to "local" processing are intended to mean where the data stays in-car (i.e. "local" processing should be construed the same as CNIL package references to "scenario 1, in-in"). The applications mentioned in the guidelines include eco-driving, in-vehicle safety-enhancing applications and applications for unlocking, starting and/or activating certain vehicle commands (§70).These applications are considered to fall outside the scope of the GDPR because

the data processing occurs within the vehicle without the transfer of personal data to a data controller or data processor (§71).

While we fully support this assessment, we believe the same should apply to any data processing that occurs purely inside the physical vehicle. This is what the German data protection authorities concluded in their 2016 statement, which says that data is collected by a controller only "as soon as data is transmitted out of the vehicle". The CNIL equally found that "the data collected in the vehicle remain under the user's sole control and are not transmitted to the service provider".

Consequently, GDPR recital 78 we understand would also align with this, where it considers that in this scenario, vehicle manufacturers would only be a producer of the product, and should only be considered controllers when data leaves the vehicle to be processed or used by them, i.e. when it is transmitted electronically or read out, for example to provide journey information to a specific off-board held customer account .

In conclusion, it should be clear that as long as data remains within the vehicle, manufacturers are only the producers of that vehicle and their obligation is to ensure that the vehicle is designed in accordance with the principles of privacy by design and by default. They become controllers or processors only from the moment data leaves the vehicle and is transmitted to them via a network.

On a separate point, we believe that roadside assistance operators could act as data processors on behalf of a vehicle manufacturer, not only as data controllers as suggested in §83.

PERSONAL DATA

The guidelines stipulate that "much of the data that is generated by a connected vehicle relate to a natural person that is identified or identifiable and thus constitute personal data" (§ 28). We believe this statement is too broad and does not accurately reflect the specificities of motor vehicle data.

Much work is put in at privacy by design stage by manufacturers today to ensure that customer data is only processed where it is appropriate and proportionate to do so, in keeping with GDPR requirements.

The vehicle identification number (VIN) is often used to assure vehicle data is linked to the correct vehicle, but it is a misconception that VIN on its own can be considered personal data, beyond a construction that it is pseudonymised data (i.e. other data must be linked to it in addition, before VIN will be capable of reasonably being considered in context to attach to personal data). VIN is not designed to identify any person – it is the automotive industry equivalent of a serial number, in that it identifies *only* a specific vehicle.

According to Regulation 19/2011, VIN means the alphanumeric code assigned to a vehicle by the manufacturer in order to ensure proper identification of every vehicle. It consists of three sections, i.e. the world manufacturer identifier (to identify the manufacturer), the vehicle descriptor section (to indicate the general characteristics of the vehicle) and the vehicle indicator section (to identify a particular vehicle).

For data added to VIN to be considered as personal data, it would have to meet the GDPR test in context of use (i.e. be information that can be demonstrated to *relate* to an identified or identifiable natural person). For example, VIN linked to journey data used to provide journey information to a specific off-board held customer account, would in context be considered personal data. VIN linked only to vehicle part information (used only to research vehicle model performance, or to check the correct part is being ordered for the correct vehicle model), we would consider fails to meet the GDPR test of being able to relate to an identified or identifiable person.

In addition, motor vehicles are specific – and different from other products like smartphones – in that they have multiple users and therefore multiple potential "data subjects". This feature will become even more pronounced with the current trend towards car sharing. It also has practical implications that should be understood and taken into account when assessing to what extent connected vehicle data can be related to a natural person that is identified or identifiable (see section below on "data categories and context of processing").

Data categories and context of processing

The variety of data subjects that exist in the context of connected vehicles affects the degree to which specific types of data can be related to those different data subjects.

Generally speaking, we identify three buckets of data originating from the vehicle:

- Technical data related to the vehicle as a product (no or very low characterisation of usage by the data subject)
    - Data regarding vehicle components (e.g. serial number, software version)
    - Data related to vehicle quality and maintenance (e.g. diagnostic trouble codes)
- Data related to the data subject (owner, driver, passenger, subscriber, user of the service)
    - Data regarding driving/driver behaviour (e.g. usage statistics)
    - Data directly provided by the data subject (e.g. mobile phone connected, music played)
    - Contractual and financial data (e.g. accounting and invoices, warranty)
- Data related to the environment of the vehicle

- Data related to the external environment (e.g. external temperature, wipers on/off when automatic mode)
- Data of other data subjects close to the vehicle who are "seen" by outward facing cameras or recognised by other sensors (e.g. pedestrians, other drivers or passengers, other license plates)

Please see the table at the end of the document for a more detailed yet non-exhaustive overview of the different type of data processed in the context of connected vehicles.

From our perspective, all this data does not necessarily relate to each data subject. Consequently, it should not be considered personal data in all cases. Whether or not it constitutes personal data will depend on the context of processing.

For example, some data is purely technical data. It is generated (component data, sensor data, actuator data, oil temperature, distance driven), aggregated (average fuel consumption, average speed, odometer reading) or stored in the vehicle (software version, variant coding) but it cannot be related to and is unlikely to have any real privacy impact on any particular data subject. Should vehicle manufacturers process such data, for example for the purpose of vehicle quality or vehicle improvement, this should therefore not be considered processing of personal data.

By contrast, other data such as fuel consumption, speed, acceleration, deceleration and braking during a specific trip can be related to the driving behaviour of a data subject if such data is used, for example, in the context of a pay-how-you-drive insurance service. This should always be assessed in the context of the data processing activities and consider whether the purposes of the processing are intended to impact directly or indirectly the relevant data subjects.

Data subjects

With regard to data processing in connected vehicles, we identify six main types of data subjects:

- The vehicle owner
- The subscriber of a service
- The user of a service
- The driver
- The passenger
- Individuals close to the vehicle who are "seen" by outward facing cameras or recognized by other sensors

While the first three are generally identifiable by the manufacturer, this is very often not the case for the others. As previously highlighted, this is key differences with other products like smartphones, which tend to be inherently for personal use rather than a shared device.

From our perspective, this implies that in cases where the vehicle manufacturer has no reasonable chance of identifying the driver or the passenger, it will not be possible for him to obtain consent from the data subject or to enable the latter to exercise his or her rights.

Possibly with the intention of addressing this issue, the guidelines state that manufacturers should implement inside the vehicle a profile management system to store the preferences of known drivers (§ 88). This obligation – which does not appear as such in the GDPR - could act against data protection ideals in that it forces manufacturers to take measures to make identifiable every data subject who has an interaction with the vehicle. This would not only take away customer choice to ride in a vehicle without registering, but de facto, also make anonymous driving impossible. In order to be used fully, a profile management system would need to force all drivers to identify themselves or to accept privacy settings each time they start the vehicle. This would not be user-friendly, sit very uneasily with the data minimisation principle, and still not be sufficient to obtain the consent of passengers, for example. In our view, it would be counterproductive in terms of privacy protection and in conflict with article 11(1) GDPR if, for the sole purpose of compliance, manufacturers were forced to implement measures to identify data subjects that they could not and would not need to identify otherwise.

We therefore believe that the statement in § 28 should be re-formulated to reflect the reality that not all data subjects related to connected vehicles are always identified or identifiable, at least not for the vehicle manufacturer.

Data subject rights

The guidelines stipulate in various places that data subjects should have the right to stop the processing of data or delete data that were processed. For example, § 88 says that drivers should be enabled to stop the collection of certain types of data, temporarily or permanently, at any moment, except if a specific legislation provides otherwise or if the data are essential to the critical functions of the vehicle. In § 74, the guidelines say that data subjects should be able to delete permanently any personal data before the vehicles are put up for sale.

We believe this is neither practicable nor necessary from a data protection point of view. However, this activity could be managed on a server taking into consideration that the onboard device typically does not support this kind of flexible logic.

In our view, the only data that data subjects should have access to and be able to delete (or otherwise exercise their rights on) from the vehicle are those data that they have provided themselves (mobile phone data, navigation data, infotainment and comfort settings).

Deleting other, more technical, vehicle data seems inappropriate. If data relating to components or

to the health status of the vehicle were deleted (e.g. software version or diagnostic trouble codes) as a result of their inclusion in a wider definition of personal data, this would make it impossible for manufacturers to fulfil their responsibilities in terms of product safety, product liability and warranty. Without such data, repairers could not carry out adequate repair and maintenance works. and authorities could not conduct the periodic technical inspections that EU law prescribes. In some cases, deleting specific data such as the odometer reading may even be illegal.

A contextual perspective, establishing that not all vehicle data should be considered personal data, would help data subjects to better understand the scope of their rights.

LEGAL BASIS (E-PRIVACY & GDPR)

ePrivacy

We find it unfortunate that the guidelines provide a detailed assessment of data processing in connected vehicles under the ePrivacy Directive at a time when that Directive is about to be replaced with a new ePrivacy Regulation.

This is all the more so since the content of article 8 of this Regulation could differ significantly from that of article 5(3) of the Directive, which it corresponds to. Indeed, the version of the Council document dated 21 February 2020 states that the storage of or access to data is permitted when it is necessary for providing a service requested by the end-user. This "service" is a much broader concept than the "information society service" contained in article 5(3) of the ePrivacy Directive

Also, recital 21 of the latest Council draft of the ePrivacy Regulation says that consent is not required to the extent that it is necessary to use or access data for the provision of the service requested by the end-user. This would include, for example, pay-as-you-drive (based on mileage only) or pay-how-you-drive (based on mileage and driving style) insurance.

Even more significantly, article 8(1)(g) of the latest Council text permits data storage or access where it is necessary for the purpose of the legitimate interests pursued by a service provider, except when such interest is overridden by the interests or fundamental rights and freedoms of the end-user.

This means that the guidelines, if published in their current form, risk being outdated very soon. We believe it would be preferable to postpone the publication of the guidelines until the content of the new ePrivacy Regulation is known with certainty (i.e. following an agreement between the European Parliament and the Council). We think the quality and accuracy of the guidelines are more important than the speed with which they are adopted.

Diverging national implementations of the ePrivacy Directive make the situation even more

challenging. Germany, for example, has no full implementation. This would mean that the guidelines, which are supposed to apply cross the board, would have to be adapted locally to reflect these different implementations of the Directive. This problem would not exist with the forthcoming ePrivacy Regulation, which will apply directly in all Member States.

On substance, we understand that the EDPB considers vehicles to be "terminal equipment" in the sense of article 5(3) of the ePrivacy Directive. This implies that, as a rule, anyone using a publicly available electronic communications network to store or access data in the vehicle, must obtain the consent of the vehicle owner or user. The only exceptions are when the data are stored or accessed for the sole purpose of carrying out the transmission of a communication over an electronic communications network or when it is strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide that service.

We believe connected vehicle should not be considered "terminal equipment" as defined in article 1 of Directive 2008/63 ("equipment directly or indirectly connected to the interface of a public telecommunications network to send, process or receive information;") in all cases (*please see our detailed analysis of the relationship between the GDPR and article 5(3) of the ePrivacy Directive in Annex 1)*.

It should be identified that many vehicle networks will not be publicly available in the same way that a smartphone will allow any of its users access to the general internet. Connected vehicles include closed networks, with many M2M features not even accessible to users, and designed to include cybersecurity protections (as distinct from open public internet networks).

To the extent that (part of) a vehicle would be considered terminal equipment, we believe it is important that data protection authorities agree that this Directive applies only to data storage or access that occurs from outside the vehicle, i.e. through communications between the vehicle itself and other devices (which can be located inside or outside the vehicle) that provide a connection to a public telecommunications network. This includes communications over a mobile telecommunications network to or from a vehicle manufacturer's server, over Bluetooth to or from the mobile phone of the driver or passenger and the provision of Wifi on board. Importantly, it does not include communications between the electronic control units inside the vehicle through the in-vehicle network(s) of the vehicle itself. Consequently, the consent required by the ePrivacy Directive should apply only in case of such "external" data transfer (access or storage), from those areas of the vehicle that meet the criteria to be considered terminal equipment.

Legal basis

The guidelines strongly suggest that vehicle manufacturers and service providers will require the

consent of the data subject for most, if not all, data processing operations. This is linked, at least partially, to the interplay between the ePrivacy Directive and the GDPR. In particular, the guidelines state that "consent will likely constitute the legal basis both for the storing and gaining access to information already stored and the processing of personal data following aforementioned processing operations" (§ 15).

This gives the impression that a double consent would be needed, one under the ePrivacy Directive and another under the GDPR. However, this is contradicted by some of the use cases that are analysed in the same guidelines. For example, for pay-as-you-drive/pay-how-you-drive insurance services (§ 105), the renting and booking of parking space (§ 120) and tackling auto theft (§ 160), it is said that the performance of the contract can be the legal basis for data processing under the GDPR and therefore by implication no consent would be required or indeed relevant in those cases.

As mentioned above, recital 21 of the Council draft of the ePrivacy Regulation suggests that consent under that Regulation is not required. It says that "in the area of IoT services which rely on connected devices (such as connected thermostats, connected medical devices, smart meters or automated and connected vehicles), the use of the processing and storage capacities of those devices and access to information stored therein should not require consent to the extent that such use or access is necessary for the provision of the service requested by the end-user".

We believe § 15 should be re-worded since it gives readers the false impression that double consent would be required in most cases. In reality, it would seem no consent is needed in some cases.

The combination of legal bases under the ePrivacy legislation and the GDPR as described in the guidelines sometimes appears unnecessarily complex and impracticable. One example is the pay-as-you-drive/pay-how-you-drive use case, where consent is required for gaining access to the data and where the data can subsequently be processed on the basis of the insurance contract (§ 105).

In our view, combining consent and contract is bound to cause problems. If, for example, the driver would revoke his or her consent, the data processing could no longer take place even when the contract is still in force, in this case with the vehicle owner. It should be noted, however, that this problem should not occur when the new ePrivacy Regulation enters into force since, as mentioned above, the Council draft makes it possible to store or gain access to data when this is necessary to provide a service explicitly requested by the user. As a result, no consent would be required for gaining access to data to be used for a pay-as-you-drive or pay-how-you-drive service, contrary to what the guidelines say. This leads us once more to the conclusion that it is premature to publish the definitive version of the guidelines without knowing the final content of the ePrivacy Regulation.

Separately, when it comes to insurance, the guidelines say that the insurance company should not gain access to the raw behavioural data but only to the aggregate score that is the result of the processing performed by the telematics service provider. In our view, this fails to recognise that

each insurer may have its own (probably IP protected) algorithm for this purpose and that storage of all these algorithms in the vehicle is simply not possible and is also not desired by insurance companies who do not want to reveal them to all manufacturers.

The guidelines in our view do not sufficiently reflect the reality that vehicle manufacturers process data for a variety of purposes, sometimes as providers of services and sometimes as manufacturers of a product for which they have legal responsibilities even after having put in on the market (product safety, product liability, warranty). The CNIL's compliance package included an example where vehicle manufacturers could process vehicle data for the purposes of model optimisation and product improvement either by anonymising the data or, where that is not possible, on the basis of their legitimate interest (scenario 2, "in-out"). We would consider it useful if this example were included in the guidelines as well.

Another example is cybersecurity. Data protection law itself as well as upcoming sector-specific regulations require vehicle manufacturers and other involved parties to provide adequate cybersecurity and to implement a cybersecurity management system. This includes systems and measures for monitoring cybersecurity, for example for detecting intrusion or other tampering attempts and protecting customer accounts, as well as incident response and related processes, for example to provide software updates or inform customers about security issues. All this will require additional data processing, potentially involving personal data. The guidelines should therefore clearly state that the processing of personal data that is necessary to provide and uphold adequate cybersecurity protection and incident response capabilities is considered legitimate.

Especially in the connected vehicle context, it is also important to keep in mind that vehicle manufacturers are subject not only to legal requirements, but also to technical standards and other design requirements, like considering aspects of driver distraction. Requiring permanent or excessive user interaction, for example by showing extensive information messages for data protection purposes or renewing consent every time the vehicle is started or a data processing feature is activated may cause severe driver distraction or render functionalities practically impossible. We feel that the guidelines should therefore aim to better balance data protection aspects with these and other requirements vehicle manufacturers are subject to.

On the whole, we feel the guidelines over-emphasise consent as a legal basis for data processing while somewhat neglecting other legal bases such as performance of the contract and legitimate interest. All these legal bases have equal standing in the GDPR. We feel this should be reflected in a more balanced way in the guidelines.

DATA REQUIRING SPECIAL ATTENTION

Offence related data

The guidelines provide an unusually broad interpretation of offence-related data. They state that "instantaneous speed is, not on its own, offence-related data since it does not, by itself, reveal an offence given that speed restrictions vary by location. However, such data could nevertheless become offence-related data because of the purpose for which it is collected (e.g. for the purposes of investigating and prosecuting criminal offence), in which case the safeguards set out in art. 10 GDPR would apply" (§ 64).

We fully support this analysis and agree that the purpose of the data processing is key to determining whether the data processing falls under article 10 GDPR. This is also in line with the conclusions of the CNIL's 2018 compliance package and considers the contexts in which this data could be compliantly processed – both on-board and off-board, to support appropriate activities such as scientific research. (CNIL package, page 26, considering "in-out" scenarios). Furthermore, the exact geographic position alone will not suffice to determine whether data processing reveals offences since many more factors such as time and weather conditions (fog, for example) need to be taken into account.

From our point of view, the instantaneous speed of a vehicle combined with precise geolocation data cannot be considered a criminal office/road code infraction in itself and therefore should not fall within article 10 GDPR. From a legal point of view, the instantaneous speed of a vehicle combined with precise geolocation data can be considered to fall within the scope of that article only if and when a formal act is issued by a competent public authority affirming and stating that this data have determined the legal existence of a criminal offence or a road code infraction. Even though speed and geolocation could infer traffic violations, the processing performed by vehicle manufacturers is not aimed at public authorities' sanctions. This happens in the same way as the EDPB guidelines 3/2019 on processing of personal data through video devices say that "video footage showing a data subject wearing glasses or using a wheelchair are not per se considered to be special categories of personal data."

We also do not understand why the guidelines go on to say that "except for some exceptions, external processing of data revealing criminal offences or other infractions is forbidden" (§ 65). This does not seem coherent. If, as § 64 seems to suggest, the context of the processing determines whether instantaneous speed constitutes offence-related data, it would appear unnecessary and unreasonable to prohibit vehicle manufacturers who process instantaneous speed data for other purposes, for example for traffic information services, from processing such data outside the vehicle, so long as the purposes for processing by those vehicle manufacturers is not aimed at/linked to the determination that a criminal offence/infraction may or not have been committed.

Geolocation data

The guidelines state that geolocation should be activated "only when the user launches a functionality that requires the vehicle's location to be known, and not by default and continuously when the car is started" (§ 61).

We find this impracticable in certain cases.

For example, if a vehicle user subscribes to a "find parked car" service, the guidelines seem to suggest that the vehicle may only send out the location when the customer opens the app and searches for the parking position of his vehicle. This requirement would render the service impossible as the time the request is made will be after the car has last parked, thus preventing last parked data to be stored and available for use. Similarly, vehicle owners who have signed a contract to receive real time traffic information, would probably expect this information to be available from the moment they start the vehicle, for every service they have signed up to that requires the use of location data. Obliging them every time to activate this feature would not seem very user-friendly and would lead to potentially negative outcomes: driver distraction and/or consent fatigue. The same applies for drivers who have a pay-how-you-drive insurance contract, for which the processing of geolocation data may constitute an essential element or for some C-ITS services that require the vehicle to check continuously whether there are traffic hazards along the route.

These examples demonstrate that the wording of the guidelines is too narrow on this point. We think the geolocation should be activated on request of the user for all contracted services at the outset or when the user launches a functionality that requires the vehicle's location to be known.

Biometric data

The guidelines state that "when considering the use of biometric data, guaranteeing the data subject's full control over his or her data involves (…) storing and comparing the biometric template in encrypted form only on a local basis, with biometric data not being processed by an external reading/comparison terminal" (§ 62).

We find this overly restrictive and potentially impossible to operate to. We believe this type of requirement would make the development of new services such as shared mobility and robotaxis without drivers unnecessarily difficult, if not impossible, since biometric data may be used in these cases to identify the passengers who ordered the ride.

VEHICLE DESIGN REQUIREMENTS

The guidelines contain several provisions that have a direct impact on the design of motor vehicles. For example, they suggest that manufacturers should partition the vehicle's vital functions from those always relying on telecommunication capacities such as infotainment (§ 91). They also recommend the development of a secure in-car application platform, physically divided from safety relevant car functions so that access to car data does not depend on unnecessary external cloud capabilities (§ 73).

While accepting all good advice and respecting the principles of privacy by design and by default, we do not believe that it is the role of data protection authorities to recommend specific technical design solutions to vehicle manufacturers. We are not aware of any such requirements for producers of other devices belonging to the Internet of Things. We feel this goes beyond the remit of the GDPR which makes data controllers accountable for putting in place adequate security requirements that take into account the state of the art.

Table: Illustrative overview of data categories regarding connected vehicles

This table is neither exhaustive nor definitive. The context of processing always needs to be considered.

Note: "sensitive" data as described in EDPB Guidelines 1/2020 §2.1, indirect identifiers

Family	Category	Sub-category	Data (example, not exhaustive)	Data subjects
DATA RELATED TO VEHICLE **no or very low characterisation of the usage by the data subject**	**Data regarding vehicle components**	**Identification**	Vehicle identification number (VIN), BIN, registration number	To be determined, depends on the data linked to such ID data
			Type, model year, components identification number, technical specifications	None

		Vehicle configuration	Type of engine, type of gearbox, parts of the vehicle, hardware and software versions, Electronic Control Unit (ECU) parameters, options	None
		Network & Communication	IP address, IMEI, MAC address of vehicle, IP gateway, WIFI Id, WIFI password, Bluetooth name of vehicle…	To be determined, depends on the data linked to such network a com data
	Data related to vehicle quality and maintenance	**Vehicle status**	Engine temperature, oil pressure, brakes, ESP, steering, average fuel consumption, CO^2, Nox, current charge of the battery, temperature of the battery, airbags, total mileage	None (aggregated data of all drivers so impossible to link them to any individual)
		Default & diagnostic services	Default codes, logs, maintenance issues	None
DATA RELATED TO THE DATA SUBJECTS (owner, driver, passenger, subscriber, service user)	**Data regarding driving/driver behaviour**	**Dynamic**	Speed, mileage (journey), acceleration, gear, engine RPM, instantaneous and average fuel consumption (journey), battery charge and consumption (journey), automatic	Vehicle driver

			braking, Lane Departure Warning, AD Blue level, ADAS	
		Geolocation	Latitude, longitude, altitude, compass, navigation route…	Vehicle driver (and/or identified passenger, if any)
		Vehicle settings & controls	Privacy settings, Number of buckled seat belts, air conditioning, doors open/close, Lights on/off, wipers on/off (manual)	Vehicle driver (and/or identified passenger, if any)
	Data directly provided by the data subject (mobile phone, music, etc.)	**Navigation & Infotainment**	Phone and address book, phone calls history, music, radio preferences, navigation destination & history, pictures, movies, mirroring (e.g. Apple Car Play, Android Auto)	Service user (who is the vehicle driver and/or identified passenger, if any)
		Personal attributes	Video, images, voice as well as biometry captured inside the vehicle	Vehicle driver (and/or identified passenger, if any)
		Network & Communication	MAC address of personal devices, Bluetooth device name of personal devices	Service user (who is the vehicle driver and/or identified passenger, if any)
	Contractual and financial	**Accounting and invoicing**	Order and leasing invoices, sales and	Vehicle owner or subscriber (lease

	data	**documents**	after sales invoices, services invoices	or services)
		Services subscription (connected or any other services such as maintenance)	Description of the services, subscription contractual duration	Subscriber
		Warranty	Description of the warranty coverage (duration, scope, etc.)	Vehicle owner
DATA RELATED TO ENVIRONMENT OR TO OTHER DATA SUBJECTS (outside of the vehicle)	**Data regarding external environment of the car**		External temperature, wipers on/off (automatic mode), lights on/off (automatic mode), images and videos captured from outside	None
	Data of other data subjects		Video and images captured from outside	Any data subjects in the close surrounding of the vehicle who are identifiable

ANNEX 1:

DETAILED ANALYSIS RELATIONSHIP GDPR - ART 5(3) E-PRIVACY-DIRECTIVE

With regard to connected vehicles we see a larger discrepancy between the ePrivacy Directive and the GDPR which in our view would need to be further detailed in the guideline. These discrepancies lie mainly within the scope of the ePrivacy Directive, in the terminology, which the Directive and the GDPR use, and in the question of what is to be understood as "terminal equipment".

Whilst Article 6 General Data Protection Regulation aims at protecting personal data of "data subjects" and at ensuring free movement of data within the Union, Art 5 (3) ePrivacy Directive 2002/58/EC as amended by Directive 2009/136/EC aims on protecting the rights of "subscribers" and "users" with regard to data stored in their terminal equipment. Thus, these legal instruments have different areas of application and aim to protect different objectives. They should, in our opinion, not be intermingled especially given that Art 5 (3) ePrivacy directive 2002/58/EC as amended by directive 2009/136/EC has not been transposed uniformly into the national law of all EU-member states.

We would like to show you in the following examples in which areas we expect challenges:

- Art 3 ePrivacy Directive ("services concerned") states that the (whole) ePrivacy Directive is only applicable to "*publicly available electronic communications services in public communications networks in the Community, including public communications networks supporting data collection and identification devices.*" The wording of Art 3 ePrivacy Directive does not appear to cover car manufacturers as they do not provide a service in a public communication network. Generally, the communication from a vehicle is machine-to-machine communication with the manufacturer's IT backend and does not allow "public communication". Therefore, the interpretation of Art 29 Working Party and now EDPB of Art 5 (3) ePrivacy Directive as a general provision runs counter the wording of Art 3 ePrivacy Directive. We suggest to follow the interpretation of the German data protection supervisory authorities from March 2019 as no general provision (translated from German): „*The provision in Art. 5(3) ePrivacy Directive addresses not only to providers of publicly available electronic communications services, but also to providers of "information society services". These correspond to the services that are referred to as telemedia services in Germany and are regulated by the TMG.*" (Orientierungshilfe der Aufsichtsbehörden für Anbieter von Telemedien (2019), Page 3). This German interpretation

from March 2019 comes to the same result as the Austrian lawmaker of the year 2011 in Art. 96(3) Austrian Telecommunications Act 2003 (BGBl. I Nr. 102/2011; BGBl. I Nr. 78/2018): Art 5(3) ePrivacy Directive is no general provision, it should only be applicable to "publicly available electronic communications services" (Art 2 lit c Framework directive 2002/21/EC) and "providers of information society services" (Art 2 lit a E-Commerce directive 2000/31/EC).

- The aim of the ePrivacy Directive 2002/58/EC (version directive 2009/136/EC) is to ensure the protection of terminal equipment information. This legal protection of terminal equipment information ends at that point, after the terminal equipment information is retrieved in accordance with Art 5(3) ePrivacy directive (version directive 2009/136/EC).
- The assumption that a connected car as a whole should be "terminal equipment" under European telecommunication law is in our point of view not entirely judicially explored. The term "terminal equipment" did not change since 1988 (ex Art 1 Directive 88/301/EEC) and is still used in the Directive 2008/63/EC. According to Art 1(1) Directive 2008/63/EC, "terminal equipment" is:

  a) *equipment directly or indirectly connected to the interface of a public telecommunications network for the transmission, processing or reception of messages; in the case of both direct and indirect connections, the connection may be made by wire, optical fibre or electromagnetically; in the case of an indirect connection, a device is connected between the terminal equipment and the interface of the public network;*

  b) *Satellite earth station equipment with its facilities;*

  A "terminal equipment" in the sense of European telecommunications law must therefore fulfill at least these two requirements in order to fall under the definition:

  i. It must be connected directly or indirectly to the interface of a public telecommunications network (Art 2 lit d Framework Directive 2002/21/EC).

  ii. It must be a device for sending, processing or receiving "messages". The term "message" is legally defined in Art 2 lit d ePrivacy Directive 2002/58/EG as "*any information exchanged or transmitted between a finite number of parties by means of a publicly available electronic communications service. This does not include information which is transmitted to the public as part of a broadcasting service over an electronic communications network, provided that the information cannot be associated with the identifiable subscriber or user receiving it*;".

  Consequently, in the case of a connected vehicle, only those components can be considered as 'terminal equipment' which are directly or indirectly connected to an interface of a public telecommunications network (Art 2 lit d Framework Directive 2002/21/EC) and which contain 'messages' (Art 2 lit d ePrivacy Directive). It must therefore be checked whether these two

conditions are met before a technical device can even be legally designated as a "terminal equipment" in the sense of Art 1 (1) Directive 2008/63/EC in conjunction with Art 5 (3) ePrivacy Directive 2002/58/EC. In the context of a connected vehicle this will not apply for all components but only to a few.

- We make the observation, that the EDPB's approach of applying article 5 (3) leads to further inconsistencies when it comes to the European telecommunications law terms "subscriber" and "user" and the GDPR term "data subject". In our opinion that is not a correct interpretation of European telecommunication law. A view on the legal definitions of European telecommunications law and of the GDPR shows this

  i. "subscriber" (Art. 2 lit. k Framework Directive 2002/21/EC): "*any natural person or legal entity who or which is party to a contract with the provider of publicly available electronic communications services for the supply of such services;*".

  ii. "user" (Art. 2 lit a ePrivacy Directive 2002/58/EC): *"any natural person using a publicly available electronic communications service, for private or business purposes, without necessarily having subscribed to this service;".*

  iii. *"data subject"* (Article 4 (1) GDPR): *"identified or identifiable natural person"*

  A blanket mixing of GDPR and Art 5 (3) ePrivacy Directive should be avoided in the guidelines, as they do not use the same terminology. Notwithstanding that, we are of the opinion that consent is not the only way to legitimate the data flow; this interpretation might cut off rights of the data subjects. Especially, because Art 5 (3) ePrivacy Directive 2002/58/EC states that the consent of a "subscriber" is enough ("*subscriber **or** user concerned has given his or her consent*"). But "subscribers" can also be legal persons who have the contract "*with the provider of publicly available electronic communications services for the supply of such services*" (Art. 2 lit. k Framework Directive 2002/21/EC). In the case of car manufacturers, where the manufacturer holds the contract with the telecommunications provider for the SIM card in the vehicle and is thus the subscriber, user consent might therefore not be required.

  That would clearly conflict with the GDPR which would require, that the consent is given by the data subject as natural person. This example alone shows that intermixing of "subscribers", "users" and "data subjects" together in one data protection guideline would lead to further challenges and inconsistencies. A more precise legal and technical examination of European telecommunications law is necessary in our opinion.

  That is why we recommend waiting for the e-Privacy Regulation to become into force and for the time being to reduce the EDPB guidelines 1/2020 to the application of the GDPR in alignment with the papers of the German and the French Data Protection authorities about this topic.