Comment

of the German Insurance Association (GDV)

ID-number 6437280268-55

on the

EDPB Guidelines 1/2020 on processing personal data in the context of connected vehicles and mobility related applications

Gesamtverband der Deutschen Versicherungswirtschaft e. V.

German Insurance Association

Wilhelmstraße 43 / 43 G, 10117 Berlin
Postfach 08 02 64, 10002 Berlin
Phone: +49 30 2020-5000
Fax: +49 30 2020-6000

51, rue Montoyer
B - 1000 Brüssel
Tel.: +32 2 28247-30
Fax: +49 30 2020-6140
ID-Nummer 6437280268-55

Contact:
Datenschutz/Grundsatzfragen

E-Mail: **data-protection@gdv.de**

www.gdv.de

Executive summary

Data from connected vehicles allow the insurance industry many opportunities to offer customers high-quality services and generate added value for them. These services include among others:

- Telematics insurance products,
- Roadside and accident assistance,
- Preventative advice and service and
- Claims settlement.

Against this background, the EDPB guidelines 1/2020 should be adjusted and further differentiated in several points. This concerns in particular the following aspects:

- Incomplete portrayal of present situation concerning processing of data from connected vehicles
- No necessity for an additional legal basis under the GDPR if the ePrivacy directive applies
- Overly heavy focus on consent as a legal basis
- No general prohibition of automatic and continuous geolocation
- No excessive requirements for the principle of data minimization and the first layer of the layered approach for information obligations
- Telematics insurance contracts can be information society services
- Incomplete presentation of facts in the case study on pay as you drive (PAYD) insurance policies
- Missing relevant use cases/case studies

Note:

The guidelines regularly refer to usage-based insurance tariffs, where individual driving behaviour is assessed, as pay as you drive (PAYD) insurances. This corresponds with how the term is often understood by the public. In contrast the insurance industry which offers these products has traditionally referred to insurance policies that are based on individual driving behaviour as pay how you drive (PHYD) insurances. The term PAYD insurance has been reserved for insurance products where primarily the individual mileage covered is taken into account. In contrast, the driving behaviour is not used in PAYD insurance policies for calculating the premiums. In order to avoid misunderstandings, the guidelines should be adjusted to refer to insurance policies based on driving behaviour as PHYD insurances.

For reasons of consistency with the draft guidelines this comment will also refer to PHYD insurances as PAYD insurances.

1. Introduction

The digitalization of the society is progressing unstoppably. Machines can communicate with each other and an increasing number of everyday objects are connected to each other. Digital networking offers many possibilities and opportunities for offering new products and services and improving them. This is particularly true for connected motor vehicles.

The insurance industry can use data generated by connected vehicles for performing and optimizing a plethora of services thereby creating significant added value for customers. These services are among others:

- Telematics insurance

  In telematics or usage-based insurances data from connected vehicles are collected through telematics devices, smartphones and/or sensors. Thus, considerate driving behaviour can be rewarded with discounts on the insurance premiums. Especially novice drivers, who statistically possess high claims expectancy, can be rewarded for considerate driving with corresponding discounts.

- Roadside and accident assistance

  In the event of a breakdown or accident the great accuracy of the data obtained from connected vehicles would enable insurance companies to provide quick and effective breakdown and accident assistance.

- Preventative advice and service

  Insurance companies could further improve their services for the customer through the use the vehicle data. For instance, the data could be used to inform the driver about necessary repairs, visits to the service station or more favorable driving routes in case of traffic jams.

- Claims settlement

  Telematics data enable insurance companies to conduct quicker and more precise analyses of accidents which in turn allows for quicker and more precise claims settlement.

Against this background, the German insurance association is of the opinion that the EDPB guidelines 1/2020 require further differentiation and adjustments:

2. Incomplete analysis and portrayal of the current situation concerning processing of data from connected vehicles

The draft guidelines in general do not correctly portray the present situation regarding the processing of personal data from connected vehicles. They especially lack focus on data processing by car manufacturers. Car manufacturers are the primary stakeholders responsible for or involved with most activities concerning personal data from connected vehicles. If their importance is not adequately accommodated, the guidelines may unintentionally have a negative impact on proper and free competition.

In addition, the EDPB should take caution not to restrict the use of personal data from connected vehicles beyond what is required by the GDPR by posing further requirements that are not essential for reaching an adequate data protection level. Otherwise, effective competition with stakeholders who are not explicitly addressed by the guidelines will be distorted.

3. No necessity for an additional legal basis under the GDPR if the ePrivacy directive applies

According to Art. 5 (3) ePrivacy directive, the collection of information from terminal equipment requires the user's consent. This does not apply if access to the information is strictly necessary in order to provide an information society explicitly requested by the user. If this exception is applicable, the processing of personal data from terminal equipment shall still require a legal basis under Art. 6 GDPR (page 5, para. 17-18).

The wording of the guidelines does not make it sufficiently clear whether, the EDPB holds the view that only the further processing of the data after their collection from the terminal equipment requires a legal basis under Art. 6 GDPR or whether a legal basis under the GDPR shall also be necessary for the act of collecting the information. Within its scope of application, the ePrivacy Directive supersedes the GDPR according to Art. 95 GDPR in conjunction with recital 173. A legal basis under the GDPR cannot be required if the collection of the data falls within the scope of application of the ePrivacy Directive and the latter stipulates that consent is not necessary. The EDPB should specify that a legal basis under Art. 6 GDPR is only necessary for further processing operations after the collection of data from the terminal equipment.

4. Overly heavy focus on consent as a legal basis

The guidelines regularly portray obtaining consent as a necessity, although it is legally often not required:

a) Passengers

On pages 10-11 para. 46-49, the guidelines go into more detail on the requirements for consent: Controllers must take particular care to ensure that in cases, where consent is necessary, they obtain it separately for each participant, e. g. owners and users of vehicles.

It should be noted that consent is not necessarily required for passengers or a driver who is not the owner of the vehicle or the policyholder of the motor insurance. Instead other legal bases can be considered.

It is unclear how the EDPB defines the term "vehicle user". It would be problematic if “vehicle user” also means passengers. In this respect, it can be agreed with the EDPB that in practice it could be difficult to obtain the consent of drivers and passengers (page 11 para. 49). If one were to require the consent of mere passengers, it would always have to be determined which and how many people are present at what time during which ride. Such an approach would considerably and unnecessarily lower the level of data protection. Moreover, a passenger could undermine the consent given by the driver by refusing to give his or her consent.

b) Alternative legal bases for the driver of the vehicle

The guidelines analyze pay as you drive (PAYD) insurances in a case study (pages 21-25 para. 103-127). They rightfully explain that the processing of the policyholder’s personal data from connected vehicles can be based on Art. 6 (1) (b) GDPR.

However, the guidelines do not specify on which legal basis the processing of personal data of a driver who is not also the policyholder (a third party) can be carried out. The guidelines should be supplemented in such a way that the processing of the data of the third party/parties can be based on legitimate interests pursuant to Art. 6 (1) (f) GDPR, provided that the data are attributed to the policyholder and there is no interest in identifying the third party/parties. In this case, the interests of the insurance company and the policyholder in the performance of the telematics insurance contract outweigh any conflicting interests of the third party.

c) Collection of telemetry data

The guidelines state on page 11 para. 52 that telemetry data, which is collected for maintenance purposes may not be disclosed to insurance companies without consent for the purpose of offering behaviour based insurance policies.

While the statement is correct with regard to the specific situation described in para. 52, the EDPB should mention that conversely telemetry data, which is necessary for the performance of a telematics insurance contract or other contractual services can be processed on the grounds of Art. 6 (1) (b) GDPR. Otherwise para. 52 may be misunderstood in a way that the further processing of telemetry data in the context of insurance policies based on driving behaviour always requires consent.

d) Transmission of data to commercial partners

According to page 20 para. 95 the data subject's consent should be systematically obtained before their data are transmitted to commercial partners.

This recommendation is not practical. Moreover it stands in contradiction to page 20 para. 93 of the guidelines, whereas a data controller may transmit personal data to a commercial partner provided that the transmission can be justified by any one of the legal bases stated in Art. 6 GDPR, not just consent.

5. The option to conduct further processing of personal data on the basis of Art. 6 (4) GDPR should not be excluded

The EDPB considers further processing of personal data on the basis of Art. 6 (4) GDPR not possible when data are collected on the basis of consent as required by Art. 5 (3) ePrivacy directive or on the basis of one the exemptions since it would undermine the data protection standard of the ePrivacy directive. (page 11 para. 50).

This line of argument is not correct. Art. 6 (4) GDPR permits the further processing of personal data for a purpose other than that for which they were collected, provided that the further processing is not already covered by consent. The successful compatibility check therefore replaces the alternatively possible consent for further processing. The requirements for effective consent are identical under the ePrivacy directive and under the GDPR. It is therefore not apparent to what extent the level of protection of the ePrivacy directive would be undermined. If consent is already dispen-

sable under Art. 5 (3) of the ePrivacy directive, the level of protection of the directive is not undermined a fortiori by the application of Art. 6 (4) GDPR to the further processing of the data.

6. No general prohibition of automatic and continuous geolocation

According to the EDPB, geolocation data can provide information on habits and sensitive matters of the persons concerned. Among other things, they allow conclusions to be drawn about religious and sexual characteristics. Therefore, they may only be processed to the extent absolutely necessary (page 12 para. 60). For this reason, geolocation should only be activated when the driver starts a function that requires knowledge of the vehicle's location. On the other hand, geolocation should not be activated automatically and continuously every time the vehicle is started (page 13 para. 61).

This statement is phrased too generally. For example, it would prevent accident reporting/the provision of assistance services. These require knowledge of the location of an accident or breakdown. In this case, however, the driver may no longer be in the state to activate the geolocation. The data subjects actually expect that the promised accident and roadside assistance services are performed without requiring further action on their part.

Telematics insurance policies also provide for an automated correction of reported data: If the driver (properly) adheres to an outdated speed limit due to a cancellation/increase of a speed limit not found on public maps, a correct evaluation of his driving behaviour can be made for this location from the geolocation data of the telematics insurance collective. However, this requires active geolocation.

Moreover, it is certainly correct that geolocation data may allow conclusions to be drawn about sensitive information. However, numerous mechanisms are available to prevent these dangers. First of all, it should be pointed out that insurance companies do not draw such conclusions in the context of telematics contracts because the information obtained from them has no value in the context of the insurance contract. Secondly, the drawing of such conclusions is itself a processing operation which cannot be covered by the contractual purpose of a telematics contract. The drawing of the conclusions would thus be in breach of data protection regulation and subject to a fine. The insurers also take measures to prevent this through technical and organizational measures and safeguards – for example, by storing the personal data exclusively at a service provider who produces a score and transmits only that score (using a pseudonym) to

the insurer. The insurer himself therefore has no access to the behaviour-related data while the service provider has no knowledge of the identity of the policyholder.

7. Local processing of personal data inside the connected vehicle

The EDPB is in favor of always processing personal data locally inside the connected vehicle as far as possible (pages 14-15 para. 70-72). Exclusively local processing inside the vehicle, which is carried out by the driver himself, does not fall within the scope of the GDPR according to Art. 2 (2) GDPR (page 15 para. 71). However, according to guidelines the GDPR does apply to controllers or processors who provide the means of data processing for personal or household activities. If they act in their role as controllers/processors, they must develop applications in compliance with the principle of privacy by design and default (page 15 para. 73).

This section should be rephrased. It is potentially misleading, insofar as it declares that controllers, who merely provide the tools and applications for private data processing, fall within the scope of the GDPR. Controllership always refers to a specific data processing. There is no such processing if an application or tool is merely made available to someone else.

Furthermore, the section gives the impression that producers of hardware/software have obligations according to the GDPR. In contrast, recital 78 merely states that they should be encouraged to adhere to the principle of Privacy by Design and Default when developing products and services. An enforceable obligation does not exist, so that controllers with actual obligations cannot rely on support from producers for fulfilling their duties.

It should be noted that purely local processing of data inside the connected vehicle would currently not be possible for third-party service providers, as vehicle manufacturers currently refuse and prevent this option. For local processing to work the vehicle manufacturers would have to be required by law to provide the appropriate access for third-party service providers. Furthermore, as of yet it is doubtful if data processing systems inside of connected vehicles possess the necessary computing power to perform local processing of such scale.

8. No excessive requirements for the principle of data minimization

With respect to telematics insurance, the EDPB believes that a "hybrid" form of local data processing should be used. The data is to be processed into a score either inside the vehicle or by the telematics service provider.

The score alone should then be transmitted to the insurer at predefined intervals (e.g. monthly) in order to comply with the principle of data minimization (page 16 para. 75).

It must be possible to transmit the score to the insurance company at shorter intervals, as long as these intervals are contractually agreed upon with the policyholder. The driver/policyholder is often given the opportunity to see how he/she has driven after each ride. This service is often expected by the customer and has a positive effect on the road safety aspect, which is inherent in telematics insurance contracts. In case only longer intervals between the transmissions of the score values were allowed, the insurance customers would be deprived of the spontaneous evaluation experience.

Moreover, the possible measures and arrangements for safeguarding the principle of data minimization are formulated too narrowly. It is already unclear whom the EDPB considers a telematics service provider. It is currently not apparent, if the term refers to the vehicle manufacturers or the providers of the electronic communications services through which the data are transmitted. It might also be possible that the EDPB assumes that the telematics infrastructure is provided by an independent third party. Unless the guidelines clarify who is considered a telematics service provider, companies might not be able to properly conduct “hybrid processing” as envisioned by the EDPB. Regardless, it should also be possible for the raw data to be transferred to a processor commissioned by the insurer. The processor could process the data into a score and transfer the score alone to the insurer. This would also be an effective way to ensure data minimization.

9. Too much information required on the first layer of the layered approach for information obligations

When fulfilling their information obligations, controllers can choose a layered approach. On the first layer, in addition to the identity of the controller, the purposes of the processing and the data subject's rights, all other information on the processing that could have the most impact on the data subject or surprise him/her should be provided (page 18 para. 84).

The layered approach is counteracted by the fact that too much information is to be provided at the first level already. It is not clear why the rights of the data subject must be described at this level. It should suffice to inform the data subjects about the existence of their rights in the GDPR and to refer to the second layer for further information. Similarly, the requirement to provide any additional information on the processing which

has the most impact on the data subject goes too far. Such information would be overly bureaucratic and have barely any value if all data processing in the particular case is simple and contains nearly no risks.

The EDPB should also clarify that standardized icons (compare page 19 para. 88) are adequate to provide the necessary information for the first layer.

10. No interruption of data collection contrary to contractual agreements

The guidelines provide that drivers should have the possibility at any time to interrupt the collection of certain data temporarily or permanently, unless the data processing is required by law or for critical functions of the vehicle (page 19 para. 88).

This would effectively render the performance of telematics insurance impossible. Telematics insurance policies are designed precisely to analyse risks arising from driving behaviour. If the driver could briefly interrupt the collection of data at any time to go for a risky spin, it would prevent a fair premium from being calculated at the expense of the group of insured persons. For this reason, an exception to the right to interrupt the collection of data must be recognized for cases of contractually agreed data transmissions. At the very least, it must be ensured that the insurance company is made aware of rides without data collection so that it may take them into account in the risk assessment.

11. Incomplete presentation of facts in the case study on pay as you drive (PAYD) insurance policies

In a case study, “pay as you drive” (PAYD) insurance policies are discussed in more detail (pages 21-25 para. 103-127). According to the EDPB, the insurer requires drivers to install telematics devices in their vehicles. The EDPB further remarks that PAYD insurance policies must always be optional. The customer must be able to subscribe to insurance policies that are not based on driving behaviour (pages 21-22 para. 103-104).

The facts presented are not wholly correct. Usage-based car insurance does not always require additional devices to be installed in the vehicle. Alternatively, they can be enabled via smartphone applications, by devices that do not require installation (plug-in or adhesive box solution) or, in the future, by collecting data directly from the vehicle without integrating additional devices.

The EDPB should furthermore clarify that it is sufficient if alternative, non-usage-based insurance policies are available on the market. It cannot be demanded that every insurer provides an insurance policy that is not based on driving behaviour. This would be an intolerable invasion on entrepreneurial freedom and would lead to distortions of competition.

12. Telematics insurance contracts can be information society services

The guidelines state that the performance of a telematics insurance contract does not constitute or relate to an information society service which the user/driver has explicitly requested within the meaning of Art. 5 (3) ePrivacy directive (page 22 para. 105).

It is not understandable why telematics insurance or other insurance services, such as accident assistance or claims settlement, should in general not be considered information society services. “Information society services” are defined in Art. 1 (1) (b) of Directive (EU) 2015/1535 as any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services. At the very least telematics insurance policies, which are concluded by the policyholder via means of electronic communication, would have to fall under this definition. All parts of the contract can be performed electronically and both the conclusion of the contract and the service are provided at the individual request of the policyholder. The EDPB does not give any explanation on why it assumes the opposite.

13. Knowledge of personal data is necessary for telematics service providers

As an alternative to purely local data processing inside the connected vehicle, the EDPB suggests that the telematics service provider should process the data for the insurer into a score and only forward that score to the insurer. Accordingly, the telematics service provider would have the raw data on driving behaviour, but no information on the name, the VIN or other data of the policyholder. The insurer would have these data, but no access to the raw data on driving behaviour (page 22 para. 108).

Such a separation between the data on driving behaviour at a service provider and the contractual data at the insurer is already often implemented in practice. However, there are other ways of achieving a high level of data protection for telematics insurance policies. If such a separation of data shall be pursued, the EDPB would have to specify in its comments that the telematics service provider must have knowledge of at least one identifier. If the guidelines are to be understood as meaning that he may

not have any personal data at all, the insurance contract could not be performed. If the telematics service provider does not have any information about the policyholder, he could only send the score to the insurer. Without an identifier, the insurer would not know for which policyholder and insurance contract the score is intended.

14. Missing relevant case studies

The guidelines examine several examples of processing in the context of connected vehicles. The scenarios are supposed likely to be encountered. While that may be true for PAYD/PHYD insurance products with regard to current developments in vehicle insurance, the practical importance of the other case studies with respect to challenges arising from data protection seems comparatively low, however.

The list of case studies is missing examples from the core business of car manufacturers. Car manufacturers offer many services concerning connected vehicles which pose a plethora of data protection questions. Among the economically relevant use cases is the processing of GPS location and speed data for creating maps, the prediction of traffic density and traffic jam warnings. Practically all car manufacturers make use of connected vehicle data to offer such services.

Berlin, 19 March 2020