FEDERATION INTERNATIONALE DE L'AUTOMOBILE
REGION I - EUROPE, THE MIDDLE EAST AND AFRICA

What EU legislation says about car data

Legal Memorandum on connected vehicles and data

#mycarmydata

Memo

To: Ms Laurianne Krid

CC:

Matter Nr: 1060415

From: Dr. Marc Störing

Office: Innere Kanalstr. 15 D-50823 Köln

Date: 16 May 2017

Legal Memorandum on Connected Vehicles and Data

Dear Ms Krid

This memorandum discusses the legal situation with regard to data in connected vehicles and the consequences arising there from under European data privacy and liability law aspects. For that purpose, we particularly assess the positions of data protection supervisory authorities as well as literature and current case law but also positions of various European automotive industry associations. Further, we take corresponding provisions of the Regulation (EU) 2016/679 (General Data Protection Directive – **"GDPR"**) into consideration that will become applicable on 25 May 2018 in order to determine if the GDPR allows a different legal estimation. The present legal situation is based on Directive 95/46/EC (**"Data Protection Directive"**) and naturally we take such present law into account as well.

The Fédération Internationale de l'Automobile, 8, Place de la Concorde, 75008 Paris, France (**"FIA"**) is the addressee of this memorandum and may disclose it to third parties at its own discretion. However, this memorandum cannot be relied upon by such third parties.

Preface

Technical progress and digitisation of vehicles contribute to new functionalities providing higher levels of vehicle and traffic safety, economic and environmental efficiency and comfort or info-tainment for drivers and passengers alike. Modern vehicles contain a multitude of electronic components and control units that constantly collect, store, process, transmit and use data (**"process"**) occurring in connection with (connected) vehicles irrespective of the legally relevant question whether such data is generated in the vehicle (**"vehicle generated data"**) or provided (**"customer provided data"**) by vehicle keepers, drivers and passengers (**"customer"**). As modern vehicles get more and more connected they could potentially exchange this data wirelessly with vehicle manufacturers (**"OEM"**), suppliers and third party service providers as well as other stakeholders of the after-market.

However, these developments create new challenges and legal uncertainties for both customers and stakeholders, in particular in regard to questions of data privacy and data access.

Executive Summary

Data in connected vehicles qualifies as personal data to any party that may reference that data with reasonable means to a specific individual. For such a qualification it is neither relevant whether data compromises technical data, nor whether data is vehicle generated or provided by the customer. Even the question of anonymisation depends on whether the controller can employ reasonable means to re-establish such a reference (Sec 2 et. seq.).

The GDPR does not fundamentally change this legal assessment as objectives, legal principles and evaluations of European privacy law will stay basically unchanged even though the GDPR nevertheless strengthens the data subject's sovereignty over his[1] data. In particular, the right to receive and transmit his data to third parties (right to data portability, Art 20 GDPR – Sec 3) will have a significant impact on data from connected vehicles.

Product safety and liability aspects are relevant in the context of handling data from connected vehicles as well, since they serve the interests and integrity of customers. Despite this essential function, fundamental data privacy principles are neither reversed nor restricted by liability obligations. In particular, obligations in the context of product safety and liability do not permit OEMs to permanently and comprehensively collect and evaluate data from connected vehicles (Sec 4). Furthermore, product safety and liability aspects neither exclusively entitle OEMs to process data nor do these considerations in any form prevent third parties from accessing said data.

1. To enhance legibility references to persons are not gender-specific.

In Legal Detail

1. Legal basis formed by Directive 95/46/EC and Regulation (EU) 2016/679

As of 25 May 2018 the GDPR will apply directly in all European Member States and will thereby repeal the Data Protection Directive from 1995. However, despite exceptions, such as the right to data portability in Art 20 GDPR, the GDPR does not fundamentally change core aspects of privacy law. It rather brings procedural and institutional modifications that not only give Europe-an supervisory authorities additional possibilities to enforce data privacy provisions more effectively but will also further harmonize European data privacy law.[2] As a consequence, the GDPR does not initiate a contentual and conceptional revolution of fundamental data privacy principles, assessments and frameworks.

In fact, concept and qualification of personal data remain unchanged and still pose the point of reference for the application of data privacy law and the thereof resulting privacy objectives.[3] The GDPR as well as the Data Protection Directive impose restrictions and obligations on the processing of personal data in Art 5 Para 1 lit a-f GDPR. Those principles enumerated in Art 5 Para 1 lit a-f GDPR basically correspond with Art 6 Para 1 lit a-e Data Protection Directive.[4] They include lawfulness, fairness and transparency of processing; and uphold the principle of purpose limitation, data minimisation and storage limitation. Insofar, the GDPR poses rather an evolution than a revolution.[5]

However, in regard to sanctions the GDPR indeed is a revolution. The influence of data protection supervisory authorities will grow significantly, in particular due to higher sanctions, cf. Art 83 Para 4 and 5 GDPR.[6]

As an overall result for the subject matter of this legal memorandum, the changeover from Directive 95/46/EC to Regulation (EU) 2016/679 as the legal basis for European data privacy law will neither substantially remodel the assessment of data in connected vehicles, nor impose changes in regard to the allocation of obligations and responsibilities.

2. Data in connected vehicles under current and future European privacy law

Present and future European privacy law protects "the fundamental rights and freedoms" of individuals, "and in particular their right to privacy with respect to the processing of personal data". Privacy law strives to enable the individual to control who can process his personal data, for what purposes and to which extend.[7] Therefore, privacy law aims at a protection against data rather than a protection of data.[8] From this starting point, European data privacy law applies – only and to the extent – personal data is being collected, processed or used, Art 3 Para 1 Data Protection Directive (Art 2 Para 1 GDPR). The understanding of what constitutes personal data is therefore the key question in privacy law. Striving for a robust answer on whether data in the context of connected vehicles shall be deemed personal data or not is challenged by legal disputes on two different levels: The question of whether technical data can at the same time qualify as personal data (see Sec 2.1) and the debate on the correct interpretation of the definition of personal data (see Sec 2.2).

2.1 Controversy around personal data and technical data

Vehicle generated data often has a clear technical nature without the intention to make any statement regarding the customer. This fact triggered a dispute on whether such data should exclusively be deemed technical data or whether it could simultaneously qualify as technical data and as personal data as well. Two different approaches can be observed: an approach hereafter called "mutual exclusion theory" (Sec 2.1.1), and in contrast thereto a view hereafter called the "theory of combined qualifications" (Sec 2.1.2).

2. Kühling/Martini, in: EuZW 2016, 448.
3. Albrecht, in: CR 2016, 88, 90 et seq.
4. Plath, in: BDSG/DSGVO, 2nd Ed. 2016, Art. 5 DSGVO rec 1, Schreiber, in: Plath, BDSG/DSGVO, 2nd Ed. 2016, Art. 4 DSGVO rec 4 et seq.
5. Kühling/Martini, in: EuZW 2016, 448, 450.
6. Kühling/Martini, in: EuZW 2016, 448, 452; Faust/Spittka/Wybitul, ZD 2016, 120.
7. Weichert, in: Däubler/Klebe/Wedde/Weichert, BDSG, 5th Ed. 2016, § 1 rec 1 et seq.
8. Consequently, companies cannot rely on data privacy aspects in order to protect their own commercial interests, Weichert, in: Däubler/Klebe/Wedde/Weichert, BDSG, 5th Ed. 2016, § 1 rec 4 et seq.

2.1.1 Mutual exclusion theory

Until now, various European automotive industry associations made different attempts to classify data occurring in connected vehicles (exemplary: European Automobile Manufacturers Association – **"ACEA"**; German Association of the Automotive Industry – Verband der Automobilin-dustrie – **"VDA"** and the British Society of Motor Manufacturers and Traders – **"SMMT"**). In particular, VDA[9], ACEA[10] and SMMT[11] so far prominently defended a position according to which data may be generally separated in different categories resulting in an "either / or" distinction between non-personal and personal data. With the exception of data for services requiring user or vehicle identification, data is considered to be merely of technical nature with allegedly no relevance to data privacy law.[12] Further, these associations tried to establish a clear separation between data provided by the customer as personal data and vehicle generated data as non-personal data.[13] Correspondingly they state that "vehicle generated data excludes data imported by vehicle users" and thereby implying an "either/or" relation concerning vehicle generated and customer provided data.[14] Thirdly, these associations took up a position claiming that most of the so defined vehicle generated data consists largely of anonymised data.[15]

2.1.2 Theory of combined qualifications

The opinion of the European Commission,[16] the German government,[17] the German data protection supervisory authorities18[18] and the vast majority of legal scholars differs from the estimations of the European automotive industry associations described above.[19] According to this view, data in connected vehicles, irrespective of its content, does qualify as personal data if it can be linked to one or more individual data subjects such as customers. Any indirect reference to a customer is sufficient for the data to qualify as personal data. Information is indirectly linked if data references foremost to material things but secondarily allows drawing conclusions concerning an individual's personal circumstances.

In other words, although technical data references primary to the vehicle as a material thing, it makes it possible for certain parties to infer facts regarding personal circumstances of the customer.[20] For example, technical information regarding a low oil gauge of a specific vehicle is a reference to a material situation. If this information is linked to an identifiable customer, it directly relates to this customer and makes the deduction possible, that the oil gauge of the specific individual's vehicle is low. In summary, whether data containing technical information does qualify as personal data depends on whether the data can be linked to an individual.

Older statements of the German data protection supervisory authorities could be understood to contradict such an assessment and to classify vehicle generated data as mere technical data.

But a diligent evaluation of these statements show that neither the model information[21] nor the statement of the Bavarian data protection supervisory authority (Bayerisches Landesamt für Datenschutzaufsicht – **"BayLDA"**) correspond with this view and do not support a general categorisation of data in (connected) vehicles. The statements acknowledge that a variety of a vehicle's electronic components contain data storages that either temporarily or permanently store information regarding the state of the vehicle, incidents and defects. This data may in certain constellations, but not in general, classify as mere technical data. Thus, these statements accurately affirm that vehicle generated data, if contained in the vehicle, does not yet mandatorily qualify as personal data in relation to the OEM or third parties.

9. VDA, Data Protection Principles for Connected Vehicles, 3 November 2014, www.vda.de/en/-topics/innovation-and-technology/network/data-protection-principles-for-connected-vehicles.html, last retrieved on 30 March 2017; VDA, in: Position – Access to vehicle and vehicle generated data, 19 September 2016, p. 1, www.vda.de/en/topics/innovation-and-technology/network/access-to-the-vehicle.html, last retrieved on 30 March 2017.
10. ACEA, ACEA Principles of Data Protection in Relation to Connected Vehicles and Services, Septem-ber 2015, p. 4, www.acea.be/publications/article/acea-principles-of-data-protection-in-relation-to--connected-vehicles-and-se, as consulted on 24 March 2017; ACEA, ACEA Strategy Paper on Connec-tivity, April 2016, p. 4, www.acea.be/uploads/publications/ACEA_Strategy_Paper_on_Connectivity.pdf; last retrieved on 30 March 2017.
11. SMMT, Connected and Autonomous Vehicles – Position Paper, February 2017, p. 6 et seq., www.smmt.co.uk/wp-content/uploads/sites/2/SMMT-CAV-position-paper-final.pdf, last retrieved on 30 March 2017.
12. VDA, Data Protection Principles for Connected Vehicles, 3 November 2014, VDA, in: Position – Access to Vehicle and Vehicle Generated Data, 19 September 2016, p. 2 and 6 et seq.; SMMT, Connected and Autonomous Vehicles – Position Paper, February 2017, p. 7, 21 et seq.
13. VDA, Data Protection Principles for Connected Vehicles, 3 November 2014, p 2, annex: chart; ACEA, ACEA Principles of Data Protection in Relation to Connected Vehicles and Services, September 2015, p. 4; ACEA, ACEA Position Paper Access to Vehicle Data for Third Party Services, December 2016, p. 2 et seq.; SMMT, Connected and Autonomous Vehicles – Position Paper, February 2017, p. 21 et seq.
14. SMMT, Connected and Autonomous Vehicles – Position Paper, February 2017, p. 21 et seq.
15. VDA, in: Position – Access to Vehicle and Vehicle Generated Data, 19 September 2016, p. 6 et seq.; SMMT, Connected and Autonomous Vehicles – Position Paper, February 2017, p. 23; ACEA, ACEA Position Paper Access to Vehicle Data for Third Party Services, December 2016, p. 3.
16. Cf. European Commission, A European strategy on Cooperative Intelligent Transport Systems, a mile-stone towards cooperative, connected and automated mobility, COM(2016) 766 final, 30 November 2016, p. 8, ec.europa.eu/energy/sites/ener/files/documents/1_en_act_part1_v5.pdf, last retrieved on 30 March 2017.
17. BT-Drs. 18/1362, 2 May 2014, Question 11 and 12, p. 5.
18. Joint Declaration of the Conference of the Independent Data Protection Authorities of the Federation and the Länder and VDA, of 26 January 2016, https://www.bfdi.bund.de/SharedDocs/¬Publikationen/-Entschliessungssammlung/DSBundLaender/ErklaerungDSKVDAVernetzteKfz.pdf, last retrieved on 30 March 2017; with some restrictions also: VDA and German data protection supervisory authorities, Muster-Information über Datenspeicher im Fahrzeug, 2012 (no longer publicly available); Bayerisches Landesamt für Datenschutzaufsicht, in: Info-Kompakt, Mein Auto – meine Daten?, January 2016; www.lda.bayern.de/media/info_kompakt_fahrzeug.pdf, last retrieved on 30 March 2017.
19. Instead of many: Roßnagel, in DuD 2015, 353, 355; Weichert, in: SVR 2014; 201, 204; Roßnagel, in: SVR 2014, 281, 283 et seq.; Kremer, see www.rdv-online.com/serie/datenschutz-im-vernetzten-auto-teil-3, last retrieved on 30 March 2017; Buchner, in: DuD 2015, 372, 373; Hornung, in: DuD 2015, 359, 364; Weisser/Färber, in: MMR 2015, 506, 508.
20. Weichert, in: SVR 2014; 201, 204.
21. VDA and German data protection supervisory authorities, Muster-Information über Datenspeicher im Fahrzeug, 2012; Bayerisches Landesamt für Datenschutzaufsicht, in: Info-Kompakt, Mein Auto – mei-ne Daten?, January 2016.

However, this does not preclude its classification as personal data, in particular if this data is later accessed by these parties. Such a legal classification and its consequences arise if and when a person or body collects processes or uses that data. Moreover, the model information clearly realises that the data may very well qualify as personal data in connection with further information and thereby acknowledges that technical data does not exclude the possibility that it may simultaneously constitute personal data.[22] The cautious approach is due to the fact that this model information was written under the assumption of an "offline vehicle".[23] Therefore, it does not take into consideration that in connected vehicles (or "online vehicle") data collection, processing and use already starts with the transmission of data out of the vehicle to back-end servers of OEMs and other par-ties.[24] Even the VDA has temporarily shared this view in its joint declarations with the German data protection supervisory authorities.[25]

2.1.3 Settling the dispute

Whereas it is necessary in terms of transparency to accurately reflect which data is collected and processed and for what purpose, a general separation of data in personal data and tech-nical data is misleading. Such approach is neither backed by law nor literature and would lead to the consequence that it is necessary for a qualification of data as personal data that the data subject provided the data not only causatively but also consciously. Therefore, only in case the customer is aware that he generates data, such data would qualify as personal data.

Any descriptive categorisation of collected data does not entail any data privacy assessment in regard to questions of admissibility and lawfulness of any data processing. However, that these assessments are not based on solid legal evaluations in terms of data privacy law but are rather political statements can be easily derived from the wording of the papers.

All statements by European associations of the automotive industry have to concede that a "combination of data can lead to data protection relevance"[26] and that their data privacy relevance "depends on the extent to which they can be combined with other data"[27] and may therefore "easily become [personal data], the moment it is tied to a personal identifier, such as but not limited to the VIN" (Vehicle Identification Number (**"VIN"**)[28]. Albeit, the European associations of the automotive industry try to preclude "technical data" generated in the vehicle from a classification as person-al data, they cannot substantiate such separation.

This becomes particularly obvious with the VDA paper stating that this technical data "should be and should remain technical data"".[29] The use of the subjunctive already shows that even in the VDA's estimation this classification of data is neither definitive nor legally justified. Furthermore, in contradiction to that classification as mere "technical data" as opposed to personal data, the VDA pronounces that the OEM as a "data controller may have an overriding legitimate interests in terms of vehicle and product safe-ty"[30] in regard to some of the "technical data". With this contradiction the VDA opposes its own statement, since the need to justify data collection or processing does not arise at all unless the data qualifies as personal data, cf. Art 7 Data Protection Directive (Art 6 Para 1 GDPR). The Article 29 Working Party[31] also rejects such a separation of data as well, when expressly equat-ing "data provided knowingly and actively by the [customer]" with data "generated by his or her activity,"[32] and thereby including data that is "generated by and collected from the activities of users […] by virtue of the use of the service or the device".[33] Both are deemed personal data in accordance with European privacy law.

As a result, data does not automatically lose relevance in terms of privacy just because it is being qualified as technical data. In contrast, data might even primarily contain technical information but can at the same time qualify as personal data.

2.2 Legal Dispute around the abstract definition of personal data

Accepting the fact that technical data by way of principle can simultaneously qualify as personal data leads to the question of when exactly data qualifies as personal data in a given situation. The question which requirements have to be fulfilled to consider a natural person identifiable for a specific controller was subject to heated legal disputes. Finally, the European Court of Justice (**"ECJ"**) specified the criterions determining under which circumstances an individual such as the customer is deemed identifiable and therewith brought long sought clarification.

2.2.1 Relative vs. absolute approach

According to Art 2 lit a Data Protection Directive, data qualifies as personal data if it relates to an identifiable person and such "identifiable person is one who can be identified, directly or indirectly". Almost identically, the GDPR defines "an identifiable natural person" as an individual "who can be identified, directly or indirectly", Art 4 No 1 GDPR. The key issue triggering the legal dispute is the implied reference to an unclear third party: The definition is not about the nature of data but rather about someone's capability to actually identify a person behind the data.[34]

22. Buchner, in: DuD 2015, 372, 373.
23. Otherwise it is not comprehensible why the parties categorically excluded the possibility of compiling movement profiles with the help of vehicle generated data.
24. Bartelt/Eisenmann/Ihle, in: DuD 2017, 211, 214.
25. Joint Declaration of the Conference of the Independent Data Protection Authorities of the Federation and the Länder and VDA, of 26 January 2016.
26. VDA, Chart of Data Categories, in: Data Protection Principles for Connected Vehicles, 3 November 2014.
27. ACEA, ACEA Principles of Data Protection in Relation to Connected Vehicles and Services, Septem-ber 2015, p. 4; SMMT, Connected and Autonomous Vehicles – Position Paper, February 2017, p. 6 et seq., 21; VDA, in: Position – Access to Vehicle and Vehicle Generated Data, 19 September 2016, p. 2 et seq.
28. MMT, Connected and Autonomous Vehicles – Position Paper, February 2017, p. 7.
29. VDA, Chart of Data Categories, in: Data Protection Principles for Connected Vehicles, 3 November 2014.
30. VDA, Chart of Data Categories, in: Data Protection Principles for Connected Vehicles, 3 November 2014.
31. The Article 29 Working Party is composed of representatives from all European data protection authori-ties, the European Data Protection Supervisor as well as the European Commission and its opinions serve as guidelines in regard to interpretation and implementation of data privacy provisions.
32. Article 29 Working Party, in: Guidelines on the right to data portability, WP 242, adopted 13 December 2016, p. 3; Jülicher/Röttgen/v. Schönfeld, in: ZD 2016, 358, 359.
33. Article 29 Working Party, in: Guidelines on the right to data portability, WP 242, adopted 13 December 2016, p. 8.
34. Dammann, in: Simitis, BDSG, 8th Ed. 2014, § 3 rec 20.

But Art 2 lit a Data Protection Directive as well as Art 4 No 1 GDPR are completely open in regard to the question whose capabilities are actually relevant. As a result, two different theories have emerged, both trying to resolve that open question.

The so-called "relative approach" considers only the company actually controlling the data (the data controller) to be legally relevant; therefore, the exact same data might be deemed personal data in the hand of one company[35] but not in regard to other companies that do not control such data.

In contrast, the so-called "absolute approach" considers capabilities of virtually everyone to be relevant; therefore the absolute approach assumes an individual identifiable in relation a company if not only the respective company itself but any third party may identify this individual, even if this requires additional knowledge exclusively assigned to such third party. Hence, the absolute approach regards almost all data for any party as personal data, if only someone can actually identify a person behind that data.[36] Obviously the dispute is relevant to assess the legal nature of data in connected vehicles as both theories very often result in different results.

2.2.1 Clarification by the European Court of Justice in case C-582/14

The European Court of Justice (**"ECJ"**) ruled in October 2016[37] that information not directly identifying a person, will be deemed personal data in the hands of any party (but only in relation to that specific party) that can lawfully obtain sufficient additional data to link the information to a person and therewith identify that person. The Court further states, that for a qualification of data as personal it is not required "that all the information enabling the identification of the data subject must be in the hands of one person". For data to be treated as personal data it is sufficient that the controller can or may employ legal means reasonably available to obtain corresponding additional knowledge from a third person through which the identification of the respective person is possible for the controller.

As a result, the Court ruled in favour of the relative approach but extended the scope of that approach by referring to legal means reasonably available to obtain corresponding additional knowledge.

2.2.3 What this means for connected vehicles

Data coming from connected vehicles is not automatically deemed personal data for everyone.Instead, it needs to be assessed whether or not a specific company actually controlling the data is in a position to identify a person behind that data.

Naturally, a vast variety of constellations is conceivable. In regard to the OEM the majority of legal scholars as well as the European Commission, German data protection supervisory authorities and the German government consider almost all data in connected vehicles as personal data as the OEM can relate this data at least to the vehicle's keeper.[38] OEMs will very often have this possibility either through information in sales contract or via their dealership network. Moreover, official vehicle register provide for the possibility to transfer vehicle and vehicle keeper data to OEMs to support them in case of product recalls or for other legally defined purposes[39]. Therefore, OEMs can typically easily identify at least vehicle keepers with reasonable efforts.[40]

Agreements about remote diagnostics or proactive maintenance will naturally also result in data being collected in such contexts to qualify as personal data. That is due to the fact that the service provider as the customer's contractual partner is aware of its customer's identity and can therefore link pertinent data to such customer – which is the essence of the service. Obviously, this applies not only to OEMs but as well to any other third-party provider offering such services. However, for third-party service providers to access in-vehicle data it is not necessary, either from an actual or legal point of view to conclude contracts with OEMs.

In fact, only by actually avoiding contractual relationships with OEMs third-party service providers may insure that an OEM does not monitor such third parties' contractual relationships. Only by directly concluding contracts with the customer third party service providers can prevent OEMs from identifying the third-party service provider's customers. In contrast thereto, if the respective contract is concluded with the participation of or via OEMs in the key position, the OEM will then always have the possibility to identify the person behind the data. In those cases such in-vehicle data is deemed personal data in regard to the OEM as well.

2.2.4 Relativity of anonymised data

Data can initially qualify as personal data but lose such qualification due to anonymisation. The positions of the European associations of the automotive industry suggest that – even if initially deemed personal data – such data processed by the OEM consists almost exclusively of anonymised data.[41] Data is no longer regarded as personal data pursuant to European privacy law, if it is "rendered anonymous in such a way that the [customer as a] data subject is no longer identifiable", Rec 26 Data Protection Directive (Rec 26 GDPR).

35. Referring to a "company" represents a reasonable simplification here; privacy law actually refers to controllers which could be companies, authorities or even private persons. However, in the given con-text, only companies are relevant. Therefore, this legal memorandum simply refers to company for rea-sons of clarity and readability.
36. Weichert, in: Däubler/Klebe/Wedde/Weichert, BDSG Kompaktkommentar, 5th Ed. 2016, § 3 recital 13.
37. European Court of Justice, Judgment of 19 October 2016, Patrick Breyer v. Bundesrepublik Deutsch-land – C-582/14.
38. Joint Declaration of the Conference of the Independent Data Protection Authorities of the Federation and the Länder and VDA, of 26 January 2016,; with some restrictions also: VDA and German data pro-tection supervisory authorities, Muster-Information über Datenspeicher im Fahrzeug, 2012; Bayerisch-es Landesamt für Datenschutzaufsicht, in: Info-Kompakt, Mein Auto – meine Daten?, January 2016;; instead of many: Roßnagel, in DuD 2015, 353, 355; Weichert, in: SVR 2014; 201, 204; Roßnagel, in: SVR 2014, 281, 283 et seq.; Kremer, see www.rdv-online.com/serie/datenschutz-im-vernetzten-auto-teil-3, last retrieved on 30 March 2017; Buchner, in: DuD 2015, 372, 373; Hornung, in: DuD 2015, 359, 364; Weisser/Färber, in: MMR 2015, 506, 508.
39. For Germany: See Sec 34 Para 1 in conjunction with Sec 35 Para 2 Sentence 1 No 1, Alt 2 and No 1 lit a, Alt 1 StVG.
40. ßnagel, in DuD 2015, 353, 355; Weichert, in: SVR 2014; Roßnagel, in: SVR 2014, 283f.
41. EA, ACEA Position Paper Access to Vehicle Data for Third Party Services, December 2016, p. 3 et seq.; VDA, in: Position – Access to Vehicle and Vehicle Generated Data, 19 September 2016, p. 2 et seq.; SMMT, Connected and Autonomous Vehicles – Position Paper, February 2017, p. 6 et seq.

Therefore, the assessment whether data is rendered anonymous is also subject to the question of identifiably and therefore depends on the knowledge of the controller and the reasonable means he is able to deploy to re-establish the customer's identity.[42] Therefore, in regard to anonymised data the requirements of the ECJ apply as well. In other words, as long as OEMs may reference the data to a unique identifier, the data qualifies as personal data in relation to such OEM.[43] In particular, in cases where the communication between vehicle and vehicle back end is mostly based on unique identifiers, allowing the deliverance of relevant information for the driver in return, data is not anonymised until it is distributed e.g., to traffic data providers.[44] As a result, data may be very well anonymised when distributed to third parties but in relation to the respective OEM the data qualifies as personal data, especially since "it may be relevant for the vehicle manufacturer to identify the registered keeper of the vehicle".[45]

2.3 Addressee of European Privacy Law

Responsible for the processing personal data is the entity who "alone or jointly with others determines the purposes and means of the processing of personal data" (Art 2 lit d Data Protection Directive, Art 4 Para 7 GDPR) and therefore processes personal data on its own behalf ("controller"). Thus, any entity actually accessing or processing data qualifies as a controller irrespective of the underlying legal basis for such data access or processing. Exceptions from this principle are only possible in cases where the entity that accesses and subsequently processes personal data does so on behalf of another entity as the actual controller (so called data processor), cf. Art 2 lit b Data Protection Directive (Art 4 Para 8 GDPR). In these constellations, a contractual structure between the controller and the processor ensures that the allocation of all data privacy obligations remains controller on whose behalf the processor executes the data processing.

As a result, qualification as a controller is a mere legal reflex to an existing factual constellation: The moment, any entity irrespective of whether it is an OEM or a third party service provider accesses or processes data on its own behalf it is deemed a controller and thus has to comply with the obligations and restrictions of European data privacy law.

In other words: The controller as the addressee of data privacy law.[46] Consequently, qualification as controller does neither grant unlimited, exclusive data access nor data ownership or a similar claim to data or even the right to process data at one's own discretion. On the contrary, it sets strict boundaries for such endeavours.

However, the view that the controller holds a position of power is a rather common misconception in regard to the meaning of being a controller. In part, this misconception is due to the fairly misleading wording of the English version of the Data Protection Directive and the GDPR. Both, the Data Protection Directive as well as the GDPR employ the word "controller", which in the linguistic usage does indeed imply an element of control. In this regard the English version deviates significantly from other language versions. For example, in Art 2 lit d of the German version of the Data Protection Directive "controller" translates as the "responsible body for the data processing" ("für die Verarbeitung Verantwortlicher") and in Art 4 Para 7 of the GDPR as the "responsible body" ("Verantwortlicher").[47] In these language versions the element of responsibility, which is the core aspect of being a controller, is emphasised and clearly discernible.

2.4 Conclusion

Data from connected vehicles might qualify as personal data even if it describes technical aspects. The ECJ has clarified in October 2016 that data is to be considered as personal data for any company having access to the data and being able to link such data to an individual. Data might be anonymised but as long as reference to an individual still exists, such data is deemed personal data rather than anonymised data. In particular, transferring data from one specific connected vehicle to a company logically results in personal data, not in anonymised data as the technically required link to one specific vehicle also represents a link to an individual vehicle keeper or even another customer.

As a result, data from connected vehicles is virtually always deemed personal data at least in regard to those companies that directly retrieve the data from respective vehicles – most likely OEMs but also third parties providing services to individual connected vehicles, such as remote diagnostics. In those constellations privacy law applies.

Addressee of European privacy law is the controller. Being a controller does not grant a position of power but rather ascribes obligations and restrictions with any entity that actually accesses or processes personal data. In regard to connected vehicles not only OEMs but also third party providers may qualify as controllers, simply by accessing or processing personal data as such.

42. Plath/Schreiber, in: Plath, BDSG/DSGVO, 2nd Ed. 2016, § 3 rec 57 et. Seq.
43. Gola/Klug/Körffer, in: Gola/Schomerus, Bundesdatenschutzgesetz, 12th Ed. 2015, § 3 Sec 43 et seq.
44. Rieß/Greß, in: DuD 2015, 391, 393 et seq.
45. SMMT, Connected and Autonomous Vehicles – Position Paper, February 2017, p. 24.
46. Schild, in Wolff/Brink, Beck'scher Online.Kommentar Datenschutzrecht, 19th Ed. 2017, § 3 rec 110.
47. See also as an example: French version "responsable du traitement" , Spanish version: "responsable del tratamiento" and "responsable" and Portuguese version: "responsável pelo tratamento"

3. Mitigating "lock-in" effects

The monopolisation of customer data can create lock-in effects that may hinder customers to freely dispose over their data and often impedes fair competition, as well as economic and technical developments. The GDPR aims at mitigating these effects by introducing the right to data portability in Art 20 GDPR. It grants the data subject the "right to receive the personal data concerning him or her, which he or she has provided to a controller" in order to store the respective data for his own purposes, or to transfer such "data to another controller", Art 20 Para 1 GDPR.

In regard to connected vehicles this right is relevant as it creates new means for third parties to receive data from connected vehicles. Art 20 Para 1 and 2 GDPR allows for personal data to be transferred to them upon the data subject's request and thus offers third parties to receive personal data independently from the OEM's discretion.

3.1 Objectives of the right to data portability

A right with a clear antitrust intention seems rather surprising in the context of privacy law. And indeed, the Data Protection Directive does not provide for a similar mechanism but only for a right to information in Art 12 of the Data Protection Directive. That older right, however, only aims at enabling the data subject "to verify in particular the accuracy of the data and the lawfulness of the processing" (Rec 41 Data Protection Directive). The GDPR now surpassed this by far. Similar to the Data Protection Directive (cf. Art 1 Para 2 Data Protection Directive) the GDPR's main objectives is to ensure "the free flow of personal data throughout the Union" (Rec 170 GDPR, see also Rec 13 GDPR). But in contrast to the Data Protection Directive, the GDPR transposes this objective stringently by introducing the right to data portability.

The European legislator expressly created the right to data portability foremost based on competitive consideration.[48] The legislator pursues to minimise "lock-in"-effects by enabling the sharing of data between different controllers.[49] Especially the right to directly transmit data from one controller to another controller in Art 20 Para 2 GDPR shall foster competition[50] by allowing the customer to receive a data set which he or another controller can import and further process at his own discretion.[51] Therefore, Art 20 GDPR provides the customer with more possibilities to control the processing of his personal data and thereby grants him an extensive right of disposition.[52]

These objectives can be further derived from Art 20 Para 1 GDPR, as the customer shall have the right to data portability "without hindrance from the controller" meaning he should not be discouraged by expenses or expenditure in order to enable him to change service providers more easily.[53] Therefore, the customer shall have the right to receive his data in a "structured, commonly used and machine-readable format" and with certain exceptions free of charge[54]. This right does not obligate data controllers "to adopt or maintain processing systems which are technically compatible", Rec 68 GDPR[55] but pursues to produce interoperable systems.[56] As a result, Art 20 GDPR shall prevent controllers to build or utilise technical obstacles to impede data portability from one controller to another.[57]

3.2 Data provided by the data subject

Art 20 GDPR applies if the data requested concerns the data subject, the data was provided by him and was processed by automatic means on the basis of either consent or performance of a contract, Art 20 Para 1 GDPR. As this right has no predecessor in European privacy law, the individual elements and requirements are still not conclusively clarified. In particular, it is yet unclear which data is considered to be "provided" by the customer pursuant to Art 20 GDPR, since use cases and case law have not yet been developed. Two different interpretations are currently to be observed.

3.2.1 Narrow interpretation

Some voices in literature interpret the scope of data that they deem as provided by the custom-er rather narrowly, restricting it to contractual master data. According to their interpretation, in the context of a contractual relationship between customers and controllers, data provided by the customer includes only data the customer has given to the controller for the performance of such contract (e.g., name, address, credit card or debit card information, etc.). Additional data resulting from the performance of the contract itself, e.g., order details, is not deemed provided by the customer but is rather allocated to the controller. Such data is reckoned by these voices as data arising from the contractual relationship which excludes the provision by the customer.[58] These voices consider data entered or generated by the customer in order to use technical features outside the scope of Art 20 GDPR.

48. Jülicher/Röttgen/v. Schönfeld, in: ZD 2016, 358, 360; Kamlah, in: Plath, BDSG/DSGVO, 2nd Ed. 2016, Art. 20, rec. 1; Schantz, in: NJW 2016, 1841, 1845, Cf. Holzweber, in: NZKart 2016, 104, 111.
49. Article 29 Working Party, in: Annex to WP 242 – Frequently Asked Questions, ec.europa.eu/-information_society/newsroom/image/document/2016-51/wp242_annex_en_40854.pdf, as consulted on 15 March 2017; Paal, in: Paal/Pauly, Datenschutz-Grundverordnung, 1th Ed. 2017, Art 20 rec 6; Dix, in: Simitis, BDSG, 8th Ed. 2014, § 34 recital 105; Krauß/Robrahn/von Pape/Zelle, in: DuD 2017, 217, 219; Jülicher/Röttgen/v. Schönfeld, in: ZD 2016, 358, 360; Schätzle, in: PinG 2016, 71, 74 et. seq.
50. Article 29 Working Party, in: Guidelines on the right to data portability, WP 242, adopted 13 December 2016, p. 3.
51. Härting, in: PinG 2015, 71, 72.
52. Kamlah, in: Plath, BDSG/DSGVO, 2nd Ed. 2016, Art. 20, rec. 4.
53. Cf. Gierschmann, in: ZD 2016, 51, 54.
54. Article 29 Working Party, in: Guidelines on the right to data portability, WP 242, adopted 13 December 2016, p. 12 et seq.
55. Paal, in: Paal/Pauly, Datenschutz-Grundverordnung, 1th Ed. 2017, Art 20 rec 5; Härting, in: Daten-schutz-Grundverordnung, 1th Ed. 2016, Rn. 731.
56. Article 29 Working Party, in: Guidelines on the right to data portability, WP 242, adopted 13 December 2016, p. 14.
57. Kamlah, in: Plath, BDSG/DSGVO, 2nd Ed. 2016, Art. 20, rec. 9, cf. Jülicher/Röttgen/v. Schönfeld, in: ZD 2016, 358, 360.
58. Wytibul, in: EU-DSGVO im Unternehmen, 1st Ed. 2016, rec 183; Kamlah, in: Plath, BDSG/DSGVO, 2nd Ed. 2016, Art 20 rec 6.

They deem such cases as not relevant in terms of the right to data portability, as they consider these cases as inconsequential in regard to antitrust objectives.[59] In regard to such data it can be reasonably expected from the customer to enter such data anew when using different applications or services, therefore, the right to data portability should not be applicable.[60]

3.2.2 Extensive interpretation

Other scholars, as well as the Article 29 Working Group, interpret the prerequisites of Art 20 GDPR rather broadly in order to prevent an overly limitation of the applicable scope of this right[61]. The perquisites stating that the data has to be provided by the customer should not be misused to undermine privacy rights.[62] In accordance with this approach "personal data concerning the customer" does not only include personal data as such but pseudonymous data and under certain circumstances even data that might not only concern the customer himself but other individuals as well.[63] Further, the condition of Art 20 Para 1 GDPR stating that data has to be "provided" by the customer does not restrict the amount of data covered by this provision. In contrast, the right to data portability "covers data provided knowingly and actively by the data subject as well as the general data generated by his or her activity.[64] That encloses data that is "generated by and collected from the activities of users […] by virtue of the use of the service or the device" is subject to Art 20 GDPR,[65] including data generated by the data subject's use of the vehicle.

3.2.3 Settling the dispute

The legal dispute around the interpretation of what is considered to be "provided" by the customer is relevant for data from connected vehicles. According to the narrow interpretation al-most all data in connected vehicles would be excluded from the right to data portability, all the more, when considering that the respective voices also exclude data that was entered by the data subject in applications as well as data generated by the data subject when making and adjusting settings. In contrast, the extensive interpretation leads to coherence between the legal concept of personal data and the applicability of the right to data portability.

We consider the extensive interpretation to be correct. A broad understanding of the right to data portability is essential to give this right its full and intended effect: the minimisation of "lock-in"-effects and the strengthening of the customer's disposition over his data.

Restricting the scope of this right to contractual master data renders this right almost void; such contractual master data will regularly pose only a negligible fraction of the relevant data.

Moreover, the view that only data should be included which the customer cannot be expected to enter anew is not comprehensible as this would apply all the more to contractual master data. Considering that it will be often far easier and less time consuming for the consumer to provide his contact data anew than e.g., entering settings and adjustments such an argumentation does not lead to acceptable results. That such a limitation of data was not intended by the European legislator can be easily derived from the fact that the right to data portability was originally designed for social networks. Only later, the European legislator realised the relevance of the effects such a right will have for other sectors and decided to expand the scope of application to all industries that process personal data.[66] Personal data in social networks consists largely of data that exceeds contractual master data. A broad interpretation is further backed up by Art 4 Para 2 GDPR which stipulates that every form of processing may constitute a provision of data.[67] Moreover, a broad interpretation of Art 20 Para 1 unduly endangers business and trade secrets. Those are sufficiently guarded when allowing the controller to erase or extract such information prior to the actual data transfer (see Sec 3.3).

3.3 Limitations

Art 20 GDPR includes only data concerning the data subject, thereby not only excluding anonymous data but also data that is completely unrelated to the data subject. Further limitations result from Art 20 Para 4 GDPR: Data in connected vehicles will often not only relate to the vehicle keeper but to other drivers and passengers of the vehicle as well. This gives rise to the question whether such data is included in the right to data portability especially since, Art 20 Para 4 GDPR stipulates that this right "shall not adversely affect the rights and freedoms of others". Rights and freedoms of others may be affected in case the data does concern other individual as well. Rec 63 GDPR further addresses "trade secrets or intellectual property and in particular […] copyright protecting the software" as third party rights that have to be considered.

59. Kamlah, in: Plath, BDSG/DSGVO, 2nd Ed. 2016, Art 20 rec 7; Gierschmann, in: ZD 2016, 51, 54.
60. Kamlah, in: Plath, BDSG/DSGVO, 2nd Ed. 2016, Art 20 rec 7; Gierschmann, in: ZD 2016, 51, 54.
61. Article 29 Working Party, in: Guidelines on the right to data portability, WP 242, adopted 13 December 2016, p. 3, 8 et seq.; Jülicher/Röttgen/v. Schönfeld, in: ZD 2016, 358, 359.
62. Article 29 Working Party, in: Guidelines on the right to data portability, WP 242, adopted 13 December 2016, p. 3, 7 et seq.
63. Article 29 Working Party, in: Guidelines on the right to data portability, WP 242, adopted 13 December 2016, p.6 et seq.
64. Article 29 Working Party, in: Guidelines on the right to data portability, WP 242, adopted 13 December 2016, p. 3; Jülicher/Röttgen/v. Schönfeld, in: ZD 2016, 358, 359.
65. Article 29 Working Party, in: Guidelines on the right to data portability, WP 242, adopted 13 December 2016, p. 8.
66. Jülicher/Röttgen/v. Schönfeld, in: ZD 2016, 358, 361.
67. This is even more obvious in the German version of the GDPR: "'Verarbeitung' [ist jeder] mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang […]wie das Erheben, das Erfassen, die Organi-sation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereit-stellung."

However, these limitations do not render the right to data portability futile by giving companies, such as OEMs justification to deny any such portability request in general, by invoking on the fact that almost all data in connected vehicles may relate to various individuals or by citing trade secrets, intellectual property or copyright objections. Even data provided by other individuals may be transferred to the respective customer or another controller as long as the data is used for the same purposes as the original purposes or the receiving controller secures the third party's consent.[68] Further, potential business risks cannot "serve as the basis for refusal to answer portability requests", as controllers may e.g., extract such information, cf. Rec 63 GDPR.[69]

3.4 Conclusion

The right to data portability will have a significant impact on data from connected vehicles. Fol-lowing a clear antitrust intention, the right focusses on mitigating lock-in effects and will allow customer to port vast amounts of data in the given context. The applicability is broad for two reasons: As discussed in Sec 2 above, the vast majority of data coming from connected vehicles is deemed personal data and therefore falls into the scope of privacy law in general. Furthermore as discussed in Sec 3.2 above, the scope of the right to data portability is broad again and in particular comprises also data only rather indirectly generated by the customer, simply by his or her activity. The right to data portability will mitigate "lock-in" effects and enable consumers to arrange the transfer of their personal data from one controller to another. The right to data portability does not constitute a direct right for third parties to retrieve in-vehicle data - simply because the right is attributed solely to the data subject in Art 20 Para 1 GDPR. However, third parties will have access to vehicle generated data (within the limitations set out in 3.3 of this memorandum) at the discretion of the costumer.

4. OEM liability vs. individual rights

OEMs strive to justify comprehensive and continuous processing on the basis of liability provisions obliging manufacturers to monitor their products to prevent damages or injuries of their customers. It is already controversially discussed whether statutory obligations or due diligence standards developed through case law can justify such comprehensive and continuous data processing (see Sec 4.2). Further, any such data processing has to be in compliance with European data privacy law as it retains a decisive role when balancing necessary data processing arising out of liability obligations and the customer's data privacy rights. According to Art 7 Data Protection Directive (Art 6 Para 1 GDPR), any processing of personal data is subject to the ban with permit reservation. Thus, any processing of personal data is only lawful if and to the extent that the data subject has consented in the respective processing of his personal data or one of the justifications stipulated in Art 7 Data Protection Act (Art 6 Para 1 GDPR) applies.

However, even if applicable any such possible legal justification would allow OEMs handling data solely for the purpose of complying with liability obligations but would not allow OEMs to use data for other purposes. In other words, even if liability aspects result in a right for OEMs to use data, such right would not automatically allow any commercial exploitation or other usage of the data. Furthermore, OEMs liability obligations cannot serve to establish an exclusive right to data access and data processing of in-vehicle data as these obligations do not allow for OEMs to categorically deny third parties access to such data in general.

4.1 Possible justifications

Unless the customer has given his consent in the processing of his personal data, OEMs can only base their data processing on statutory justifications. According to Art 7 lit b Data Protection Directive (Art 6 Para 1 lit b GDPR) OEMs may process personal data to the extent that it is necessary for the performance of a contract. In most cases monitoring of the vehicle and its components does not take place in the course of contract performance since a contractual relationship between OEM and the customer does not necessarily exist. Even in case such a contractual relationship vis-à-vis the OEM (e.g. sales contract) exists, monitoring will not deemed to be a part of this contract, since product monitoring obligations qualify as public safety obligation and exist in addition to contractual and statutory protection duties.[70]

Therefore, it has to be assessed if and to what extent such comprehensive and continuous data processing can be based on another provision of the Data Protection Directive. Such a provision might be Art 7 lit f Data Protection Directive (Art 6 Para 1 lit f GDPR). According to this provision, data processing is lawful as long as it is necessary for the purposes of the legitimate interests pursued by the controller. Product monitoring obligations and the therefore necessary data processing pose legitimate interests of the OEMs as they serve to minimize and prevent possible hazards entailed in vehicles or its components. Further, OEMs have a legitimate inter-est to avoid liability risks arising from damages caused by their vehicles.

68. Article 29 Working Party, in: Guidelines on the right to data portability, WP 242, adopted 13 December 2016, p. 9 et seq.
69. Article 29 Working Party, in: Guidelines on the right to data portability, WP 242, adopted 13 December 2016, p. 10.
70. Piltz/Reusch, in: BB 2017, 841, 843.

In addition, OEMs fulfil their public safety obligations by concluding these product monitoring and thus such data processing takes place in order to comply with a legal obligation to which the OEM is subject to (in particular Art 5 Para 1 Sub 3 lit b Product Safety Directive – see Sec 4.2).[71] However, such data processing is only lawful, as long as it is necessary for the specified purposes. The European Product Liability Directive.

Liability pursuant to the European Directive 85/374/EEC ("Product Liability Directive") arises only in case the product actually exhibits defects and these defects have caused a specific damage, Art 1 Product Liability Directive. Thus, the scope of the Product Liability Directive is restricted to the application in case of an actual occurrence of damage or injury.[72] Decisive factor for the requirements regarding applicable safety expectations as well as the due diligence standards is the date the product was made available on the market, Art 7 lit e, Rec 10 Product Liability Directive. Therefore, the Product Liability Directive does neither create any after-market obligations to monitor the product nor does it pose a legal justification for comprehensive and continuous collection and processing of data in connected vehicles.

4.2 The European Product Safety Directive

Whether a different assessment can be based on the Directive 2001/95/EC ("Product Safety Directive") is subject to controversies. This directive does specify public obligations for manufacturers that take effect both before ("ex ante obligations") and after the product was made available on the market ("after-market obligations").

Some scholars have taken the view that product monitoring obligations oblige OEMs to constantly process data in connected vehicles. As connected vehicles offer the possibility to comprehensively monitor vehicle data in real time, OEMs are obliged to utilize this potential. In other words, technological progress offering more opportunities entails and extends monitoring obligations for OEMs.[73]

This view does not take into consideration that such an argumentation does allow OEMs and other manufacturers to determine the extent of their product monitoring obligations and thereby allows them to exploit those obligations in order to undermine fundamental data privacy principles. However, the only decisive factor in regard to the lawfulness of data processing can be whether such data processing is required by the relevant provisions regulating product monitoring obligations. In particular, Art 5 Para 1 Sub 3 lit b Product Safety Directive stipulates primary ex ante obligations for producers that may, in certain circumstances, expand to after-market obligations.

The producer shall "choose to take appropriate action including, if necessary to avoid […] risks [for consumers], withdrawal from the market, adequately and effectively warning consumers or recall from consumers". The measures producers have to take to comply with this provision can be defined by the producers themselves as long as they adequately take the characteristics of the specific product into account and may effectively prevent consumers from a possible damage.[74] Despite the wide ranges of individual actions that may be deployed at the producers own discretion, this does not grant him the right to extensively compile customer data. This becomes clear, when interpreting Art 5 Para 1 Sub 3 lit b Product Safety Directive, that primarily addresses ex ante obligations in conjunction with Art 5 Para 1 Sub 4 lit b Product Safety Directive that focuses on after-market obligations (see below in the next paragraph). Primary ex-ante obligations cannot entitle producers to more extensive measures on the after-market as those provisions that specifically address after-market obligations.

Relevant after-market obligations are - in accordance with Art 5 Para 1 Sub 4 lit b Product Safety Directive – "the carrying out of sample testing of marketed products, investigating and, if necessary, keeping a register of complaints and keeping distributors, informed of such monitoring." Those obligations shall ensure that producers can realistically assess risks and potential hazards of products the producer has already placed on the market.[75] Art 5 Para 1 Sub 4 lit b Product Safety Directive requires the manufacturer to conduct random samples to recognise potential risks and changes in the product due to external factors. The required quantity and intensity of such samples depends on the degree of risk associated with the specific product as well as the manufacturer's opportunities to avert the risk.[76] Additionally, manufacturers such as OEMs have to check and assess complaints and maintain a complaint management. This obligation is limited to the collection and assessment of complaints and the assessment of information that was disclosed to the manufacturer without his initiative (e.g., press releases or articles about similar products, test reports[77] and monitoring of similar products produced by competitors[78]) but does not entail further activities to compile additional information about the product.[79]

These sections do, however, neither oblige nor allow OEMs permanent monitoring of all or at least certain vehicles. Even authors that consider constant and excessive evaluation of real time data or other vehicle data in connected vehicles to be a necessary part of the OEM's product monitoring obligations in order to avert possible dangers and risk have to concede that these obligations do not overrule privacy aspects.[80]

71. Piltz/Reusch, in: BB 2017, 841, 844.
72. Cf. for German law: Wagner, in: Münchener Kommentar zum Bürgerlichen Gesetzbuch, Band 6, 7th Ed. 2017, Einl. ProdHaftG, rec 9.
73. Piltz/Reusch, in: BB 2017, 841, 843 and 844; Bodungen/Hoffmann, in: NVwZ 2016, 503, 506; cf. Dros-te, in: CCZ 2015, 105 et seq.
74. Kapoor, in: Klindt, Produktsicherheitsgesetz, 2nd Ed. 2015, § 6 rec 53.
75. Kapoor, in: Klindt, Produktsicherheitsgesetz, 2nd Ed. 2015, § 6 rec 56.
76. Veltins, in: Hauschka/Moosmayer/Lösler, Corporate Compliance, 3rd Ed., § 23 rec 15.
77. Förster, in: Bamberger/Roth, Beck'scher Online-Kommentar, 41th Ed. 2016, § 823 rec 723; Wagner, in: Münchener Kommentar zum Bürgerlichen Gesetzbuch, Band 6, 7th Ed. 2017, § 823 rec 839.
78. BGH, Urt. v. 17. Okt 1989 - VI ZR 258/88 – NJW 1990, 906, 908; BGH, Urt. v. 17 March 1981 – VI ZR 286/78 – NJW 1981, 1606, 1608.
79. Kapoor, in: Klindt, Produktsicherheitsgesetz, 2nd Ed. 2015, § 6 rec 64.
80. Droste, in: CCZ 2015, 105, 110.

On the contrary, they acquiesce that the customer's consent is necessary to process this data as product monitoring obligations are not sufficient to justify such data processing.[81] Hence, they ultimately admit that such comprehensive and continuous data processing does not fall into the scope of statutory monitoring obligations in the first place as this would render the customer's consent unnecessary.

However, even if said comprehensive data processing would be required to comply with this provisions, this would not prohibit OEMs from granting access to vehicle generated data for third parties. This assessment is not undermined by the fact that the relevant provision of Art 5 Product Safety Directive only applies to consumer products (cf. Art 2 lit a Product Safety Directive). Not only the vehicle itself does constitute a consumer product but also most of its individual components. Those components are "likely, under reasonably foreseeable conditions, to be used by consumers" as they are crucial parts of the vehicle, Art 2 lit a Product Safety Directive. Even though, the consumer is less likely to come in direct physical contact with these components (e.g., sensors), they nevertheless qualify as consumer products under this alternative, as these components have an essential function within the vehicle.[82] The directive's objective is to balance typical hazardous situations the consumers might get exposed to, thus it certainly includes potential dangers of malfunctions caused by individual components. Most of these products are further "made available [...] in the course of a commercial activity", since third party suppliers do not exclusively supply individual OEMs but rather distribute their products to repair shops. Hence, these products may be purchased in factory outlets by employees or other customers or are available through other distribution channels, such as the internet.[83]

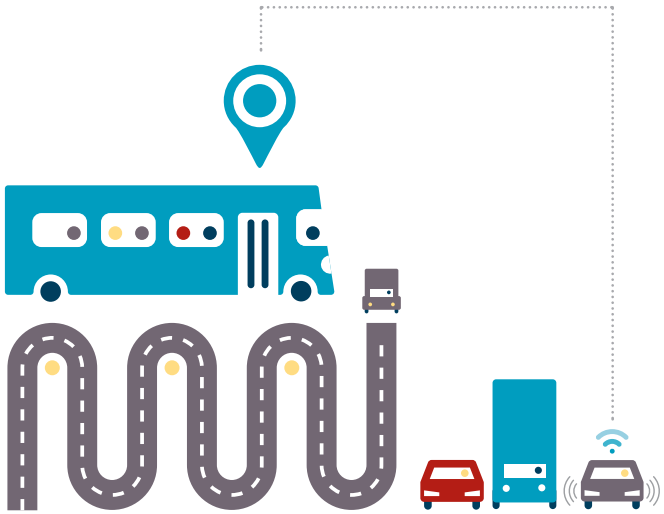
4.3 General data privacy principles in regard to monitoring obligations

In addition to the mandatory restrictions of data processing based on the statutory justifications, other fundamental data privacy principles apply as well, in particular, the principles of data reduction and data economy as a specification of the principle of necessity, and the principle of purpose limitation. The controller is only permitted to process data "necessary" for the intended purpose, cf. Art 7 lit b, c and f and Art 6 Para 1 lit c Data Protection Directive (Art 5 Para 1 lit c; cf. Art 6 Para 1 lit b, c and f GDPR). Thus, extensive monitoring that was neither required by law nor by due diligence standards developed by case law, would not be deemed mandatory under data privacy law and would therefore be unlawful.

Moreover, any personal data processed to comply with respective monitoring obligations is subject to the principle of purpose limitation, Art 6 Para 1 lit b General Data Protection Regulation (Art 5 Para 1 lit b as well as Art 6 Para 4 GDPR). Personal data processed to comply with monitoring obligations can only be processed for these purposes. In case controllers, such as OEMs plan to process such data for another purpose they may only do so within strict legal boundaries. Such changes in the purpose of processing have to be either based on the data subjects consent or have to be compatible with the original purpose the data was collected for, cf. Art 6 Para 1 lit b Data Protection Directive (Art 6 Para 4 GDPR). Thus, any data processed in order to fulfil monitoring obligations can only be used by the controller for these purposes unless either a statutory justification or the data subject's consent exists.

Best regards

Dr. Marc Störing
Rechtsanwalt/Partner



81. Droste, in: CCZ 2015, 105, 110.
82. Cf. for motion sensors in automatic (swing) doors: Klindt/Schucht, in: Klindt, Produktsicherheitsgesetz, 2nd Ed. 2015, Sec 2 rec 192.
83. Cf. Klindt/Schucht, in: Produktsicherheitsgesetz, 2nd Ed. 2015, § 2 rec 199 et seq.

MORE INFO:

www.mycarmydata.eu

FEDERATION INTERNATIONALE DE L'AUTOMOBILE
REGION I - EUROPE, THE MIDDLE EAST AND AFRICA