abida
ASSESSING BIG DATA

Das vernetzte und autonome Fahrzeug

DATENSCHUTZRECHTLICHE HERAUSFORDERUNGEN

GEFÖRDERT VOM

Bundesministerium
für Bildung
und Forschung

01IS15016C

Leibniz Universität Hannover
Institut für Rechtsinformatik

Jonathan Stoklas
Kai Wendt

Die Autoren bedanken sich bei Dipl-Jur. Nelli Schlee für ihre wertvollen Anmerkungen und Ergänzungen.

ABIDA - ASSESSING BIG DATA

PROJEKTLAUFZEIT 01.03.2015-28.02.2019

Westfälische Wilhelms-Universität Münster,
Institut für Informations-, Telekommunikations- und
Medienrecht (ITM), Zivilrechtliche Abteilung

Karlsruher Institut für Technologie,
Institut für Technikfolgenabschätzung
und Systemanalyse (ITAS)

Leibniz Universität Hannover
Institut für Rechtsinformatik
(IRI)

Technische Universität Dortmund,
Wirtschafts- und Sozialwissenschaftliche
Fakultät (WiSo) Techniksoziologie

Ludwig-Maximilians-Universität München,
Forschungsstelle für Information, Organisation
und Management (IOM)

Wissenschaftszentrum
Berlin für Sozialforschung

ABIDA - Assessing Big Data

Über das Gutachten

Das Gutachten wurde im Rahmen des ABIDA-Projekts mit Mitteln des Bundesministeriums für Bildung und Forschung erstellt. Der Inhalt des Gutachtens gibt ausschließlich die Auffassungen der Autoren wieder. Diese decken sich nicht automatisch mit denen des Ministeriums und/oder der einzelnen Projektpartner.

ABIDA lotet gesellschaftliche Chancen und Risiken der Erzeugung, Verknüpfung und Auswertung großer Datenmengen aus und entwirft Handlungsoptionen für Politik, Forschung und Entwicklung.

www.abida.de

Inhaltsverzeichnis

1. EINLEITUNG UND GANG DER UNTERSUCHUNG

Das moderne Kraftfahrzeug benötigt und produziert eine Vielzahl an Daten und durch das Internet wird es mit anderen Entitäten vernetzt. Ziel ist u.a. das Fahrerlebnis zu verbessern und Arbeitsprozesse zu effektivieren. Das Erstellen von Bewegungs-, Nutzungs- oder Kommunikationsprofilen ist u.a. für Marketingzwecke und die Versicherungsbranche von großem Interesse. Das Fahrzeug selbst wird zunehmend autonomer und die im Wagen integrierte Software trifft automatisierte Einzelentscheidungen, etwa bei der Modifikation von Fahrbefehlen aus Sicherheitsgründen oder beim automatisierten Notfallruf.

Diese Entwicklung wirft viele rechtliche Fragen auf. Ein relevantes Problem stellt sich z.B. bezüglich der Zuordnung von Daten bzw. der Berechtigung anfallende Daten zu nutzen. Verschiedene Beteiligte – z.B. Hersteller, Werkstatt, Arbeitgeber, Fuhrparkbetreiber, Softwareanbieter, staatliche Stellen – haben (berechtigte) Interessen an den Daten.

Zudem stellt sich die Frage, welche Rolle das Datenschutzrecht spielt. Sind alle Daten, die durch das Fahrzeug generiert bzw. durch Sensoren aufgenommen werden, personenbezogen? Welchen Einfluss hat dies auf die Frage der Nutzungsberechtigung?

Wer ist eigentlich verantwortliche Stelle? Gibt es eine Mehrheit von Verantwortlichen? Welche Anforderungen sind an die Hersteller der Kraftfahrzeuge aufgrund des nun in der Verordnung gesetzlich festgelegten Privacy by Design-Grundsatzes (Art. 25 DS-GVO) zu stellen? Danach müssen die Verantwortlichen technische und organisatorische Maßnahmen sowie Verfahren einführen, die gewährleisten, dass die Vorschriften der Datenschutz-Grundverordnung (DS-GVO) eingehalten werden. Standardeinstellungen von Verarbeitungsverfahren sollen sicherstellen, dass nur so viele personenbezogene Daten wie nötig verarbeitet werden. Zwar erfolgte die Verabschiedung der DS-GVO bereits 2016, anwendbares Recht wurde sie jedoch erst in diesem Jahr. Und auch, wenn die Automobilindustrie seit Verabschiedung der Verordnung bemüht ist, interne Prozesse DS-GVO konform anzupassen, müssen sich Modelle und Leitfäden für die Praxis erst noch herausbilden. Big Data-Verfahren könnten sich in dieser Hinsicht als höchst voraussetzungsvoll erweisen. Das Prinzip Privacy by Default ist bislang von sämtlichen Anbietern nicht sonderlich beachtet worden. Unter anderem wird man untersuchen müssen, welche Möglichkeiten der Datenverteilung es gibt und wie beispielsweise Prinzipien der Zweckbindung und der Datensparsamkeit im Smart Car-Kontext umzusetzen sind.

Dazu gehört auch, die entsprechenden Einwilligungsmodelle zu gestalten, wobei hier Fragen der Informiertheit und Freiwilligkeit eine Rolle spielen. Inwiefern neue Umsetzungsstrategien (gestufte Einwilligungserklärungen, One-Page-Policy, Ampelsystem, standardisierte Symbole nach Art. 12 Abs. 7 DS-GVO) für das Instrument der informierten Einwilligung genutzt werden können, um diese wieder zunehmend als ein Instrument der informationellen Selbstbestimmung zu erachten, ist zu untersuchen. Zudem stellt sich das Problem, wie die Daten von Mitfahrern oder Gelegenheitsfahrern, welche zu den verantwortlichen Stellen in keinerlei Beziehung stehen, zu handhaben sind? Wie kann Transparenz für die Betroffenen geschaffen werden?

2. BEGRIFF UND FUNKTIONSWEISE

Kraftfahrzeuge für den privaten Personenverkehr generieren schon heute mehrere Gigabyte an Daten pro Stunde[1] und erschaffen damit einen neuen Geschäftszweig der mehrere Milliarden Euro generieren können soll.[2] Die Daten werden auf unterschiedliche Art und Weise gesammelt und können je nach Fahrzeugtyp und technischer Ausstattung variieren.

2.1. BEGRIFF UND BEGRENZUNG DES UNTERSUCHUNGSGEGENSTANDES

Die verbauten Technologien sind davon abhängig, um welche Art von Fahrzeug es sich handelt. Dabei ist nicht ausgeschlossen, dass sich die Technologien in allen Fahrzeugarten wiederfinden und ergänzen. Vereinfacht können die Fahrzeuge in zwei Arten unterschieden werden: Die lediglich vernetzten Fahrzeuge, ohne Automatisierung von Fahrfunktionen (oder auch „Connected Cars"), und autonome Fahrzeuge.

Ein lediglich vernetztes Fahrzeug zeichnet sich dadurch aus, dass die Fahrfunktionen im Wesentlichen noch durch einen Menschen, den Fahrzeugführer, ausgeführt werden und dieser nur durch unterschiedliche Assistenten (ABS, ACC, s.u.) unterstützt wird. Eine allgemeingültige Definition für das „vernetzte Fahrzeug" gibt es nicht. Die Bezeichnung ist vielmehr zutreffend, wenn das Fahrzeug die Möglichkeit hat, sich mit dem Internet oder anderen Teilnehmern zu verbinden (Vernetzung) und so unterschiedliche weitere Services zur Verfügung zu stellen (Kommunikation).[3] Damit sich das Fahrzeug mit dem Internet verbinden kann, werden weitere Technologien genutzt. Dazu gehört etwa die Verbindung via GSM (*Global System for Mobile Communications*) bzw. UMTS (Universal Mobile Telecommunication System) Modulen, in Verbindung mit einer SIM-Karte, durch eine WLAN Verbindung oder mittels Bluetooth. Während sich das GSM Modul direkt mit dem Internet verbinden kann, benötigen die WLAN- und Bluetooth-Module einen externen Router ins Internet.[4] Dieses könnten öffentliche WLAN Hotspots sein, aber auch das eigene Mobiltelefon mit Internetverbindung. Neben der Internetverbindung verfügen die meisten Fahrzeuge auch über ein GPS-Modul, das zum Betrieb von Navigationssystemen benötigt wird.[5]

Das autonome Fahrzeug bewegt sich unter Zuhilfenahme von unterschiedlichen Technologien wie Sensoren, Radar und optischen Einrichtungen selbstständig fort.[6] Die von den technologischen Einrichtungen erhobenen Daten und Werte werden an einen Algorithmus übermittelt, der die Fahrweise reguliert und über Aktuatoren physisch umsetzt. Damit kann sich das Fahrzeug ohne Einwirkung von natürlichen Personen fortbewegen und ist „*autonom*".[7] Diese Idealvorstellung von einem autonomen Fahrzeug entspricht jedoch nicht den heutigen Gegebenheiten. Vielmehr muss die Beschreibung dieser Art von Fahr-

[1] Rummel, Das vernetzte Auto: Datenverarbeitung in Echtzeit, IoT 2018, https://www.industry-of-things.de/das-vernetzte-auto-datenverarbeitung-in-echtzeit-a-686637/. (zuletzt aufgerufen am 09.07.2018).
[2] *Weichert*, NZV 2017, 507, 507.
[3] *Vogt*, Geschäftsmodelle für das vernetzte Fahrzeug, HNU Working Paper Nr. 30 (2014).
[4] *Johannig/Mildner*, Car IT Kompakt, S. 2 (2015).
[5] Vgl. W*eißer/Färber*, MMR 2015, 506.
[6] *Maurer et al.*, Autonomes Fahren, S. 3 (2015).
[7] *Wagner*, Technik autonomer Fahrzeuge – Eine Einführung in *Oppermann/Stender-Vorwachs*, Autonomes Fahren, S. 14 (2017).

zeugen in mehreren Schritten erfolgen. National wurde am Anfang eine dreistufige Einordnung vorgenommen (Teil-, Hoch- und Vollautomatisiert)[8], während international fünf Stufen sowie eine Vorstufe (Stufe 0) zur Einordnung genutzt werden, welche nun auch hier genutzt wird:[9]

Stufe 0: Keine Automation – Fahrer führt das Fahrzeug dauerhaft ohne eingreifende Fahrzeugsysteme

Stufe 1: Fahrerassistenz – Fahrer führt das Fahrzeug dauerhaft, während Systeme andere Funktionen durchführen

Stufe 2: Teilautomatisiert – Fahrer muss das System dauerhaft überwachen, während das System die Fahrfunktion in spezifischen Anwendungsfällen übernimmt

Stufe 3: Hochautomatisiert – Fahrer muss System nicht mehr dauerhaft überwachen, aber potentiell in der Lage sein, dass Steuer zu übernehmen. System übernimmt die Fahrfunktion in spezifischen Anwendungsfällen und erkennt Systemgrenzen und fordert den Fahrer rechtzeitig auf das Steuer zu übernehmen.

Stufe 4: Vollautomatisiert – In spezifischen Anwendungsfällen ist kein Fahrer mehr erforderlich. Das System kann im spezifischen Anwendungsfall alle Situationen automatisch bewältigen.

Stufe 5: Autonom/Fahrerlos – Es ist durchgehend kein Fahrer mehr erforderlich. Das System übernimmt die Fahraufgabe vollumfänglich bei allen Straßentypen, Geschwindigkeitsbereichen und Umweltbedingungen.

Die Sensoren des autonomen Fahrzeuges werden dabei von den Funktionalitäten des vernetzten Fahrzeuges unterstützt, wodurch der Fahralgorithmus auf weitere Daten zugreifen kann, um eine sichere Fortbewegung zu ermöglichen.

2.2. TECHNISCHE FUNKTIONSWEISE

Um die generierten Daten erfassen zu können und eine Einordnung des Personenbezuges zu ermöglichen, ist es notwendig die einzelnen Funktionalitäten darzustellen und die verarbeiteten Daten in einem vernetzten und automatisierten Fahrzeug (Smart Car) zu identifizieren.

2.2.1. GPS

Das Global Positioning System (GPS) ist ein satellitenbasierendes Ortungssystem, das den Aufenthaltsort bis auf wenige Meter genau bestimmen kann. Um eine Ortung durchzuführen, muss das Objekt von mindestens drei Satelliten erfasst werden können. Die Position wird dann anhand der x- und y-Achse (Längen- und Breitengrad) berechnet. Um auch die Höhe des Objektes zu errechnen, wird mindestens ein dritter Satellit benötigt. Im optimalen Fall wird das Objekt durch mindestens vier Satelliten erfasst. Die Bestimmung erfolgt anhand von Informationen die zwischen dem GPS Empfänger und den Satelliten ausgetauscht werden.[10] Der Satellit schickt dazu seinen Standort, Zeit und Bezeichnung an den Empfänger. Mittels der zeitlichen Differenz zwischen Versendung und Empfang der Nachricht, kann

[8] Vgl. *Wagner*, Technik autonomer Fahrzeuge – Eine Einführung in *Oppermann/Stender-Vorwachs*, Autonomes Fahren, S. 16 (2017).

[9] Definitionen basieren auf der Übersetzung des VDA, Automatisierung – Von Fahrerassistenzsystemen zum automatisierten Fahren, S. 15 (2015) welche auf dem Standard *SAE International: Levels of Driving Automation for On-Road Vehicles J3016* basiert.

[10] Vgl. *Niehues*, Hochgenaue Positionsbestimmung von Fahrzeugen als Grundlage autonomer Fahrregime im Hochgeschwindigkeitsbereich, S. 33 ff..

die Entfernung zum Satelliten berechnet werden. Zusammen mit den Daten von zwei weiteren Satelliten kann der GPS Empfänger die Position mittels der Entfernungsrechnung von drei Punkten (Trilateration) bestimmen.[11] Dazu kann nicht nur die geografische Position benannt werden, sondern durch weitere Messungen auch die Geschwindigkeit des Objektes und in welche Richtung es sich bewegt.

2.2.2. KARTEN

Neben der GPS Lokalisierung werden Karten zur Navigation eingesetzt. Ergänzend zum GPS kann so die Position des Objektes noch genauer bestimmt werden. Die durch das GPS ermittelte Position kann auf diese Weise einer postalischen Adresse zugeordnet werden. Für autonome Fahrzeuge sind hochauflösende Karten erforderlich, um eine exakte Navigation zu gewährleisten.[12] Dazu müssen sog. Landmarken in den Karten genau eingezeichnet werden. [13] Zudem ist es erforderlich, dass die Karten für das autonome Fahren ständig aktualisiert werden, um aktuelle Gegebenheiten (Baustellen, neue Straßen, Veranstaltungen, etc.) abbilden zu können. Eine konstante Verbindung des Fahrzeuges mit dem Internet ist hierfür Voraussetzung.[14]

2.2.3. NETZWERK

Die Vernetzung mit dem Internet erfolgt mittels Schnittstellen. Diese können als eigene GSM/UMTS Einheit in das Fahrzeug integriert sein oder sich mit externen Sendern über Bluetooth oder WLAN verbinden.[15] Die Kommunikation zwischen Sender und Empfänger verläuft über das entsprechende Mobilfunknetz eines Telekommunikationsanbieters. Dabei wird die IMEI (International Mobile Station Equipment Identity) für das Objekt, hier das vernetzte Fahrzeug, sowie die IMSI (International Mobile Subscriber Identity) für die SIM-Karte übermittelt, damit der TK-Anbieter prüfen kann ob der Sender einen Anspruch auf Zugang zu seinem Netz hat.[16] Außerdem wird die aktuelle IP-Adresse des Fahrzeuges übermittelt, die zur Identifizierung der Anfrage benötigt wird bzw. damit die angeforderten Daten an den richtigen Adressaten zurück gesandt werden können.[17] Die IP-Adresse wird daher nicht nur an den TK-Anbieter übermittelt, sondern auch an den entsprechend adressierten Dienstleister (je nach Funktionalität können das Social-Media-Plattformen sein, Suchmaschinen und andere Online-Services).[18] Seit April 2018 ist die VO (EU) 2015/758 über Anforderungen für die Typgenehmigung zur Einführung des auf dem 112-Notruf basierenden bordeigenen eCall-Systems in Fahrzeugen und zur Änderung der Richtlinie 2007/46/EG (eCall-VO) anwendbar. Danach sind die Hersteller verpflichtet, in allen nach dem 31.3.2018 zugelassenen Fahrzeugen das sog. eCall-System zu verbauen (Art. 4 eCall-VO). Dieses soll im Fall eines Unfalls automatisch Kontakt mit den zuständigen Notrufzentralen (112) aufnehmen.[19] Somit sind fortan alle Fahrzeuge verpflichtend netzwerkfähig.

---

[11] Vgl. *Niehues*, Hochgenaue Positionsbestimmung von Fahrzeugen als Grundlage autonomer Fahrregime im Hochgeschwindigkeitsbereich, S. 23.
[12] Eckstein, Autonomes Fahren: Sensoren und hochgenaue Karten sind das A und O in Elektronik Automotive S. 16 (04/2016).
[13] Vgl. *Jotzo*, Aktive Landmarken zur Positionsbestimmung von autonomen Fahrzeugen, (2003); *Wagner*, Technik autonomer Fahrzeuge – Eine Einführung in *Oppermann/Stender-Vorwachs*, Autonomes Fahren, S. 25 (2017).
[14] *Wagner*, Technik autonomer Fahrzeuge – Eine Einführung in *Oppermann/Stender-Vorwachs*, Autonomes Fahren, S. 26 (2017).
[15] *Johannig/Mildner*, Car IT Kompakt, S. 6 f. (2015).
[16] *Nürnberger*, DuD 2018, 79, 82.
[17] Vgl. auch *Langer*, RAW 2017, 103.
[18] *Weichert*, SVR 2014, 201, 204.
[19] Vgl. ausführlicher dazu Kap. 6.2.2.4.

2.2.4. SENSOREN

In einem modernen Fahrzeug sind mehr als 100 unterschiedliche Sensoren eingebaut.[20] Diese Sensoren verfolgen unterschiedliche Zwecke und liefern Daten die etwas über den Zustand des Fahrzeuges aussagen oder die Umgebung des Fahrzeuges analysieren und auf diese Weise das assistierte und autonome Fahren ermöglichen. Die Sensoren können in Zustandssensoren und Fahrsensoren unterteilt werden.

Zustandssensoren ermitteln Werte die relevant sind für die Wartung und Pflege, aber auch den Betrieb des Fahrzeuges. Dazu gehören Angaben über den Füllstand des Tanks, den Zustand der Reifen und Bremsbelege sowie Sensoren für Airbag, Gurtstraffer, Fahrbahn oder für die Temperatur. Basierend auf diesen Daten kann der Fahrzeugführer/-halter das Fahrzeug reparieren lassen oder seine Fahrweise ausrichten. Gleiches gilt für autonome Fahrzeuge, die das Fahrverhalten ebenfalls den äußeren Gegebenheiten anpassen müssen und möglicherweise auch eigenständig Reparatur- und Wartungsleistungen beauftragen.[21] Im Grundsatz handelt es sich bei diesen Rohdaten somit um reine Sachdaten basierend auf technischen und physischen Zuständen des Fahrzeuges und der unmittelbaren Umgebung.[22]

Fahrassistenzsysteme sowie autonome Fahrzeuge benötigen aber weitere Sensoren, die das Umfeld des Fahrzeuges erfassen und so dem Fahrer oder dem Algorithmus die nötigen Informationen mitteilen, auf Basis derer diese das Fahrverhalten entsprechend anpassen können. Um alle zur Einschätzung der Situation notwendigen Daten vollständig zu erhalten und die Schwachstellen unterschiedlicher Sensoren auszugleichen, werden verschiedene Arten von Sensoren eingesetzt, die inhaltlich ähnliche Informationen erfassen. Ultraschallsensoren errechnen die Distanz anhand der Signallaufzeit. Der Ultraschallsensor kann nur auf kurzer Distanz eingesetzt werden und feste Objekte erkennen. Daher wird diese Art von Sensoren in der Regel für Einparkassistenten genutzt. Eine genauere Spezifizierung des Hindernisses ist nicht möglich. Zur Abstandsmessung von weiter entfernten Objekten werden Radare eingesetzt, die ebenfalls die Distanz mittels der Signallaufzeit bestimmen können sowie den Winkel zum eigenen Fahrzeug. Zusätzlich kann anhand des sog. Dopplereffekts auch berechnet werden, welche Geschwindigkeit das reflektierende Objekt hat. Hiermit werden Adaptive Cruise Control Systeme (z.B. Abstandsregelautomaten) realisiert. Das Objekt selber kann, wie auch bei den Ultraschallsensoren, nicht näher bestimmt werden. Ebenfalls eingesetzt werden Lidar-Systeme, die ähnlich einem Radar funktionieren, aber statt Radarwellen nutzen diese Laserimpulse zur Messung. Die Objekte der Umgebung lassen sich dadurch zentimetergenau vermessen und als exakte „Punktwolke“ darstellen. Dabei werden Laserstrahlen ausgesandt und anhand der Laufzeit wiederum die Distanz ermittelt. So können mehrere unterschiedliche Distanzen in einem 3D-Bild skizziert[23] werden, welches dann durch Algorithmen analysiert wird und auf diese Weise Objekte als Fahrbahn oder als Hindernisse klassifiziert.[24]

---

[20] Vgl. *Fleming*, Sensors? A forecast in IEEE Vehicular Technology Magazine, S. 4 (03/2013).

[21] ADAC Studie, „Welche Daten erzeugt ein modernes Auto?“, Mai 2016, https://www.adac.de/infotestrat/technik-und-zubehoer/fahrerassistenzsysteme/daten_im_auto/default.aspx (zuletzt aufgerufen 18.07.2018).

[22] *Nürnberger*, DuD 2018, 79 ff.

[23] Vgl. Abbildung 3 in *Wagner*, Technik autonomer Fahrzeuge – Eine Einführung in *Oppermann/Stender-Vorwachs*, Autonomes Fahren, S. 22 (2017).

[24] *Niehues*, Hochgenaue Positionsbestimmung von Fahrzeugen als Grundlage autonomer Fahrregime im Hochgeschwindigkeitsbereich, S. 34 ff.

2.2.5. KAMERA

Ergänzend zu den Sensoren, werden Kamerabilder von der Umgebung aufgenommen und ausgewertet. Dazu werden Stereo-Kameras eingesetzt um eine Art räumliches Sehen zu ermöglichen. Zusammen mit den Daten der weiteren Sensoren lässt sich das Umfeld des Fahrzeuges genau interpretieren. Durch den Einsatz von Thermo-Kamers können auch bei Dunkelheit die erforderlichen Bilder aufgenommen werden. Neben der automatisierten Auswertung zur Navigation des autonomen Fahrzeuges, werden Kameras auch zur Beobachtung des Verkehrsgeschehens eingesetzt (z.B. als Dash-Cams). Kameras nehmen in Bildern oder Videos die Umgebung auf und speichern diese in einem internen Speicher, einer externen Speicherkarte oder laden sie in die Cloud. Weiterhin können auch Kameras im Innenraum zur Müdigkeitserkennung eingesetzt werden, die das Verhalten des Fahrers beobachten und seine Gesichtszüge analysieren. Anhand dieser Daten soll ermittelt werden, wann der Fahrer unkonzentriert oder müde wird und diesem dann mitgeteilt werden, dass er eine Pause einlegen sollte.[25] Alternativ lassen sich zur Müdigkeitserkennung auch Sensoren im Lenkrad implementieren.[26] Zusätzlich kann durch die Innenraumkamera das aktuelle Verhalten des Fahrers ermittelt werden und so die voraussichtliche Zeit berechnet werden, die zur Übernahme der Fahrfunktionen im teil- und hochautomatisierten Fahrzeug (Stufe 2 und 3) erforderlich ist.[27]

2.2.6. KOMMUNIKATION

Um die Sicherheit zu erhöhen und ein “vorausschauendes” Fahren der autonomen Fahrzeuge zu ermöglichen, werden verschiedene Kommunikationskanäle genutzt. Die Fahrzeuge kommunizieren mit anderen vernetzten Autos, mit der öffentlichen Verkehrsinfrastruktur in der Umgebung aber auch mit anderen vernetzten Gegenständen.[28]

Bei der Car-2-Car Kommunikation tauschen die Fahrzeuge untereinander Daten und Informationen aus. So können Gefahrenstellen, die einem Fahrzeug aufgefallen sind, an andere Fahrzeuge gemeldet werden, damit diese die Stelle in ihre Berechnungen einbeziehen können und dementsprechend ihre Fahrweise anpassen können. Es können Staus und Verzögerungen weitergegeben oder stärkere Bremsvorgänge, die dahinter fahrende Fahrzeuge betreffen können, gemeldet werden. Außerdem können so die nächsten Fahrmanöver an die umliegenden Verkehrsteilnehmer kommuniziert werden, sodass diese sich darauf vorbereiten und entsprechend reagieren können. Der Verkehrsfluss wird dadurch vorhersehbarer. Die Kommunikation erfolgt dabei über die oben genannten Netzwerke, insbesondere WLAN oder GSM/UMTS.[29] Die Car-2-Infrastructure dagegen kommuniziert mit den Verkehrseinrichtungen (z.B. Ampeln oder Verkehrsschildern) und kann sich so den örtlichen Gegebenheiten anpassen und z.B. schon abbremsen, wenn die Ampel dem Fahrzeug die kommende Rotschaltung mitteilt. Mittels dieser Kommunikationseinrichtungen lassen sich wiederum auch Gefahrenstellen oder andere Informationen übermitteln und so einen erweiterten Empfängerkreis erreichen. Weiterhin können auch andere

[25] Vgl. u.a. VW, SSP 543: Der Passat 2015, Fahrerassistenzsysteme Selbststudienprogramm, S 37.
[26] *Donath*, Müde und Unaufmerksam: Volvo schaut dem Fahrer in die Augen, veröffentlicht auf golem.de am 18.03.2018 (https://www.golem.de/news/muede-und-unaufmerksam-volvo-schaut-dem-fahrer-in-die-augen-1403-105199.html, zuletzt aufgerufen am 15.08.2018)
[27] TeslaMAG, Tesla Model 3 verfügt über eine auf den Innenraum gerichtete Kamera im Rückspiegel, veröffentlicht am 02.08.2017 (https://teslamag.de/news/tesla-model3-innenraum-kamera-rueckspiegel-15557, zuletzt aufgerufen am 15.08.2018).
[28] S. Darstellung bei *Wendt*, ZD-Aktuell 2018, 06034.
[29] Vgl. Di Vincenzo, C2X-Kommunikation: Auswirkungen der Vernetzung von Fahrzeugen auf die Architektur und Kommunikationsanforderungen, Kap. 2.1.2 (2014).

vernetzte Geräte mit den Fahrzeugen kommunizieren (Car-2-X).[30] So können Fahrradfahrer und Fußgänger anhand ihrer Mobiltelefone besser erkannt werden, deren Position, Fahrtrichtung und Geschwindigkeit bestimmt werden oder wiederrum Informationen transportieren.[31]

Insbesondere die Funktion von Informations-Repeatern ist wichtig, um die notwendigen Informationen an alle möglicherweise betroffenen Fahrzeuge zu verteilen. Die integrierten Kommunikationssysteme der Fahrzeuge haben in der Regel nur einen begrenzten Sendebereich um direkt miteinander kommunizieren können, daher sind Repeater notwendig.[32]

2.2.7. SONSTIGE FUNKTIONALITÄTEN

In einem zentralen Rechensystem im Fahrzeug werden die gesammelten Daten zusammengeführt und ausgewertet. Ein spezieller Algorithmus bewertet die Ergebnisse und zieht daraus die entsprechenden Schlüsse. Die Ergebnisse werden dann an die Aktuatoren weitergeleitet und physisch umgesetzt. Alle Daten und Messergebnisse sowie die tatsächlich ausgeführten Fahrbewegungen sollen zudem in einem Unfalldatenspeicher gespeichert und nach 30 Sekunden wieder gelöscht werden, sofern kein Unfall registriert wurde. Dieses soll die Aufklärung von Unfallgeschehen im Nachhinein erleichtern.

Neben den sicherheitsrelevanten Aspekten der unterschiedlichen Funktionalitäten, sollen diese auch zu einem erhöhten Komfort beitragen. Daher werden dem Fahrer sowie den anderen Nutzern (Bei- und Mitfahrer) neben Service- und Reparaturleistungen auch sog. Infotainment Lösungen zur Verfügung gestellt. Dabei handelt es sich um eine Sammlung von unterschiedlichen Angeboten aus den Bereichen Radio, Multimedia, Navigation und weiteren Konnektivitätsfunktionen. Der Nutzer kann seine unterschiedlichen Accounts und Plattformen mit dem Fahrzeug verknüpfen und auf diese Weise von unterwegs auf die Funktionen zugreifen. Die Infotainment Systeme sind dabei in der Regel voll in die Funktionalitäten des Fahrzeuges integriert, sodass ein ständiger Datenaustausch besteht, um die entsprechenden Services zur Verfügung zu stellen.

3. PERSONENBEZOGENE DATEN IM SMART CAR KONTEXT

3.1. EINFÜHRUNG

Das datenschutzrechtliche Regime ist nur eröffnet, sofern es sich bei den verarbeiteten Daten um personenbezogene Daten handelt. Personenbezogen sind Daten gem. Art. 4 Nr. 1 DS-GVO, wenn es sich um Informationen handelt, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Daten sind identifizierbar, sobald es sich um Informationen handelt, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen einer natürlichen Person zugeordnet werden können.

[30] Vgl. Weichert, SVR 2016, 361, 362.
[31] Johannig/Milder, Car IT kompakt, S. 15 ff. (2015).
[32] Vgl. *Graf*, „Car 2 Car/Car 2 X“ Kommunikation - Kommunikation zwischen Fahrzeugen und deren Umgebung (04.09.2009).

Nicht in den Anwendungsbereich des Datenschutzes fallen somit anonyme Daten, bei denen kein Personenbezug hergestellt werden kann.[33] Ebenso nicht vom Datenschutzrecht erfasst sind Daten, bei denen identifizierende Merkmale nachträglich entfernt wurden, um eine Zuordnung zu einer natürlichen Person auszuschließen.[34] Anonymisiert sind Daten nach Erwägungsgrund 26, sofern die Informationen, sich nicht auf eine identifizierte oder identifizierbare natürliche Person beziehen, oder die personenbezogene Daten, in einer Weise anonymisiert worden sind, dass die betroffene Person nicht oder nicht mehr identifiziert werden kann.

3.2. KRITERIEN FÜR DIE IDENTIFIZIERBARKEIT VON PERSONEN

Eine direkte Identifizierbarkeit ist dabei gegeben, wenn es sich bei dem Datum um individuelle Angaben, wie z.B. den Namen des Betroffenen, handelt. Weitere Beispiele sind das Geburtsdatum, die Adresse oder eine Fotografie des Gesichts bzw. anderen biometrischen Merkmalen, sofern es sich um eine individuelle Kennung handelt, die mit dem Namen unmittelbar in Verbindung steht.[35]

Indirekt identifizierbar ist eine Person, wenn die Information nicht unmittelbar die Person identifiziert, aber das Datum mit der Person verknüpft ist, also eine Unterscheidung von anderen Personen möglich ist.[36] Prägend ist hierbei, dass die Person nur unter Einbeziehung weiterer Informationen tatsächlich identifiziert werden kann. Der Begriff der „Identifizierbarkeit“ kann dabei unterschiedlich ausgelegt werden. In der DS-GVO gibt der Erwägungsgrund 26 Hinweise zur Auslegung des Begriffes der Identifizierbarkeit. Dort heißt es in Satz 3, das zur Feststellung, ob eine Person identifizierbar ist, alle Mittel berücksichtigt werden sollen, die nach allgemeinem Ermessen wahrscheinlich genutzt werden. Dazu können auch Mittel wie die Aussonderung gehören. Sie müssen generell nach allen objektiven Faktoren bemessen werden, zu denen die Kosten der Identifizierung, der erforderliche Zeitaufwand und die zum Zeitpunkt der Identifizierung zur Verarbeitung verfügbare Technologie und die absehbaren technologischen Entwicklungen gehören. Ob das Wissen Dritter in die Beurteilung der Identifizierbarkeit als objektiver Ansatz einbezogen werden soll, bleibt auch unter der DS-GVO offen. Der objektive Ansatz (oder auch absolute Ansatz) bei der Betrachtung des Personenbezuges führt dazu, dass es nicht erforderlich ist, dass der Verantwortliche selber die Person identifizieren kann. Entscheidend ist hiernach vielmehr, ob irgendjemand die Daten einer Person zuordnen kann. Es reicht mithin die abstrakte Möglichkeit einer Identifizierbarkeit, um die Daten zu personenbezogenen Daten werden zu lassen. Datenverarbeitende Stellen, die tatsächlich nicht in der Lage sind, die Person anhand der Daten zu identifizieren, müssten hier somit trotzdem das Datenschutzrecht beachten. Zumindest ist es nach allgemeiner Ansicht wohl nicht unwahrscheinlich, dass auch das Wissen von Dritten in die Beurteilung einbezogen wird. Dieser Ansatz ist jedoch sehr weit und lässt die tatsächlichen Möglichkeiten der Identifizierung außer Acht.[37]

Daher wird auch ein relativer Ansatz vertreten, der die Möglichkeiten des Verantwortlichen in die Beurteilung mit einbezieht. Der relative Personenbezug beschränkt sich bei der Identifizierbarkeit auf die

[33] EuArbR/*Franzen*, DS-GVO Art. 4 Rn. 4.
[34] BeckOK DatenschutzR/*Schild*, DS-GVO Art. 4 Rn. 15.
[35] BeckOK DatenschutzR/*Schild,* DS-GVO Art. 4 Rn. 16.
[36] EuArbR/*Franzen*, DS-GVO Art. 4 Rn. 2-6, BeckOK DatenschutzR/Schild DS-GVO Art. 4 Rn. 17.
[37] Vgl. Paal/Pauly/*Ernst*, DS-GVO Art. 4 Rn. 8-13.

Kenntnisse und Möglichkeiten des Verantwortlichen.[38] Die notwendigen Informationen zur Identifizierung der Person müssen nicht unmittelbar bei dem Verantwortlichen vorhanden sein, sondern es ist ausreichend, dass es nach allgemeinem Ermessen wahrscheinlich ist die Informationen zu erhalten, also mit einem vertretbaren bzw. verhältnismäßigen Aufwand.[39] Im EuGH Urteil zu dynamischen IP-Adressen[40] wurde bei der Auslegung des in der DS-RL genutzten Begriffes „vernünftigerweise" angenommen, dass sich die Informationsbeschaffung auf gesetzlich erlaubte Mittel stützen und praktisch auch durchführbar sein müsse.[41] Danach wäre eine Person identifizierbar, wenn eine Stelle, die eine Kennung oder Kennnummer verarbeitet und die rechtliche Möglichkeiten hat um die notwendigen Zusatzinformation zur Identifizierung der Person zu erhalten, da sie somit in der Lage wäre, die Person bestimmen zu lassen. Ob dieses für die DS-GVO auch in diesem Maße gilt, ist fraglich. Zumindest lässt die Änderung des Wortlautes von „vernünftigerweise" zu „nach allgemeinem Ermessen wahrscheinlich" den Schluss zu, dass hier auch weniger vernünftige Aspekte, somit auch illegale Mittel wie dem Hacken von anderen Systemen oder der illegale Ankauf von Daten bei sog. Datenhändlern, als Risikoabschätzung in die Bewertung mit einbezogen werden müssen.[42]

Offen bleibt auch beim relativen Ansatz, inwiefern die Zusatzinformationen der datenverarbeitenden Stelle zugerechnet werden können. Gerade bei Datensätzen, die einen Doppelbezug aufweisen können, ist es schwierig eine trennscharfe Unterscheidung zu formulieren. Sachdaten z.B. sind in der Regel nicht personenbezogen, da sie sich auf „Gegenstände" oder „Prozesse der Außenwelt" beziehen, unter bestimmten Umständen aber auch einen indirekten Bezug zu einer Person aufweisen können.[43] Daher müssen zur Bestimmung der Identifizierbarkeit weitere Punkte in der Beurteilung berücksichtigt werden. Vermittelnd könnte daher darauf abgestellt werden, dass die verarbeiteten Sachdaten, die „zufällig"[44] auch in Beziehung zu einer Person stehen könnten, nur dem Datenschutzrecht unterliegen und somit Personenbezug aufweisen, wenn der Verarbeitungsvorgang den Bezug auch vorsieht. Impliziert das Sachdatum, aufgrund der Art und Weise des Datums, diesen Bezug zu einer Person, wird von einem personenbezogenen Datum auszugehen sein.[45] Werden reine Sachdaten zu einem personenbeziehbaren Datum verknüpft, sind die Daten ebenfalls als personenbeziehbar zu bewerten. Das gilt auch für Sachdaten, die zwar zur Verarbeitung nicht mit personenbezogenen Daten verknüpft werden, aber dieses für den Verantwortlichen möglich wäre, da er bereits im Besitz der erforderlichen weiteren Daten ist.[46] Damit ist ein weiterer Verarbeitungsschritt in Form der Erhebung nicht erforderlich und die Daten können jederzeit verknüpft werden, unabhängig von der Intention des Verantwortlichen.

[38] Auernhammer/*Eßer*, DS-GVO Art. 4 Rn. 15.
[39] Vgl. Erwägungsgrund 26 S. 3. Unter der DS-RL war statt von einem „allgemeinem Ermessen wahrscheinlich" von „vernünftigerweise" die Rede.
[40] EuGH, Urteil vom 19.10.2016 – C-582/14 „Breyer".
[41] EuGH, ZD 2017, 24 Rn. 46.
[42] *Kügel*, ZD 2017, 455, 459.
[43] Vgl. *Forgó/Krügel*, MMR 2010, 17, 20 in Bezug auf Geodaten.
[44] So *Krügel*,ZD 2017, 455, 457.
[45] Vgl. *Krügel*, ZD 2017, 455, 457 f., am Beispiel des Flurstückes und dem Hinweis, dass ähnliches für ein Kfz.-Kennzeichen oder die IP-Adresse gilt.
[46] *Krügel*, ZD 2017, 455, 459.

3.3. PERSONENBEZOGENE DATEN IN DEN FUNKTIONALITÄTEN

Die Darstellung der Funktionalitäten lässt bereits erahnen, dass im vernetzten und autonomen Fahrzeug eine Vielzahl von Daten generiert wird. Fraglich ist, ob alle diese Daten ein personenbezogenes Datum darstellen.

- Fahrzeugdaten

Jedes Fahrzeug hat eine sogenannte Fahrzeugidentifikationsnummer (FIN, international: VIN – Vehicle Information Number) die individuell für das entsprechende Fahrzeug ausgegeben wird. Dabei handelt es sich um eine 17-stellige Nummer, die sich aus einem Code für den Hersteller, einer Zahlenkombination für das Modell und meist einer fortlaufenden Nummer besteht. Die genaue Zusammensetzung wird durch die ISO Norm 3779:2009 geregelt. Die Nummer ist am Fahrgestell des jeweiligen Fahrzeuges zu finden sowie in der dazugehörigen Zulassungsbescheinigung, und teilweise auch in dem Kaufvertrag.

Zusätzlich hat jedes Fahrzeug ein individuelles Kennzeichen und ist somit unwiederbringlich mit dem Halter verknüpft. Das Kennzeichen setzt sich aus dem Ort der Zulassung sowie zwei Buchstaben und bis zu vier Ziffern zusammen sowie dem Länderkennzeichen und der EU-Flagge. Das Kennzeichen ist direkt am Fahrzeug angebracht sowie in der Zulassungsbescheinigung vermerkt.

Grundsätzlich lassen sich aus beiden Datensätzen noch keine unmittelbaren Schlüsse auf die Person ziehen. Lediglich beim Kennzeichen wäre eine Halterabfrage möglich. Zudem ließe sich eine Identifizierbarkeit ggf. mittels Initialen und dem möglichen Geburtsdatum auf dem Kennzeichen konstruieren, welche jedoch für einen außenstehenden Betrachter auch nicht zwingend erkennbar sind. Der Unterschied des Kennzeichens zur FIN besteht darin, dass die FIN primär zur Identifikation des Fahrzeuges gedacht ist und originär somit ein reines Sachdatum ohne einen weiteren Personenbezug darstellt, während der Sinn und Zweck eines Kennzeichens darin besteht, das Fahrzeug aber auch den Halter des Fahrzeuges identifizieren zu können (sog. Sachdatum mit Doppelbezug).

Der Halter eines Fahrzeuges ist gesetzlich verpflichtet seine persönlichen Angaben dem Kraftfahrtbundesamt (KBA) mitzuteilen.[47] Ohne diese Angaben kann kein Kennzeichen erteilt werden und somit das Fahrzeug nicht zugelassen werden. Das Kennzeichen ist daher immer zu einer konkreten Person verlinkt.[48] Die Daten werden in den Systemen der Fahrzeugzulassungsbehörden sowie dem Verkehrszentralregister des Kraftfahrtbundesamtes gespeichert. Das Kennzeichen ist dort mit den Halterangaben (u.a. Name, Adresse und Geburtsdatum/-ort[49]) verknüpft.[50] Gespeichert werden neben den Halterdaten auch Angaben zum zugelassenen Fahrzeug, dazu gehören Informationen zum Modell und zur Motorisierung sowie auch die FIN. Eine Herausgabe der Daten bei Rechtsansprüchen ist grundsätzlich vorgesehen.[51]

[47] Vgl. §§ 31 – 39 StVG.
[48] Im Regelfall stellt der Halter eine natürliche Person dar. Jedoch können Fahrzeuge auch auf juristische Personen zugelassen werden. Diese sind nicht durch das Datenschutzrecht geschützt (Art. 1 Abs. 2 DS-GVO). Im vorliegenden Gutachten wird angenommen, dass der Halter eine natürliche Person ist und nur bei ausdrücklicher Erwähnung auch die juristischen Personen einbezogen.
[49] U.a. § 6 FZV.
[50] Vgl. auch *Weichert*, NZV 2017, 507, 509.
[51] U.a. § 39 StVG.

Dem Kennzeichen kommt somit eine Doppelfunktion zu und ist außerdem als eine zusammengesetzte Urkunde zu qualifizieren. Hierdurch kann ein Außenstehender in erster Linie erkennen, ob das Fahrzeug zugelassen ist und dementsprechend auch der Pflichtversicherung unterliegt. Über das Kennzeichen soll aber auch die Person identifiziert werden können. Das Kennzeichen identifiziert den Halter zwar nicht unmittelbar, ist aber unmittelbar zum Halter verknüpft und auch dazu bestimmt diesen zu identifizieren. Die erforderlichen Daten können bei unterschiedlichen Stellen abgefragt werden. Des Weiteren liegen beim Verkäufer des Fahrzeuges sowie dem Hersteller die Daten des Käufers vor und ebenfalls das Kennzeichen, sodass auch hier eine Zuordnung möglich und durch den hier Verantwortlichen wohl auch gewollt ist. Außenstehende Dritte können damit auf unterschiedlichen Wegen, ohne größeren Aufwand und mit unterschiedlichen legalen Mitteln eine Identifizierung des Halters herbeiführen. Verkäufer und Hersteller können innerhalb ihrer Organisationsstrukturen einen direkten Bezug zum Halter herstellen. Damit handelt es sich bei einem Kennzeichen um eine Kennnummer im Sinne des Art. 4 Nr. 1 DS-GVO die einem Namen zugeordnet werden kann und dementsprechend um ein personenbezogenes Datum.

Die FIN hingegen soll insbesondere Marke, Modell und die spezielle Serie des Fahrzeuges identifizieren. Das Datum ist nur direkt mit dem Fahrzeug verknüpft und in der Regel an der Karosserie des Fahrzeuges zu finden.

Die erforderlichen persönlichen Angaben für das Kennzeichen sind beim KBA somit mit der FIN verknüpft. Anhand der FIN kann somit bei einer Abfrage der Halter des Fahrzeuges identifiziert werden. Weiterhin sind die Daten in aller Regel, als Teil des Kaufvertrages, bei dem Verkäufer des Fahrzeuges vorhanden und ebenfalls mit den Käuferdaten verknüpft. Der Käufer ist gewöhnlich, muss aber nicht zwingend, der Halter des Fahrzeuges sein. Bei dem Vertragspartner handelt es sich oftmals um einen Zwischenhändler und nicht dem Fahrzeughersteller selbst. Dennoch werden diese Daten regelmäßig auch an den Hersteller übermittelt, da dieser die Backend-Infrastruktur zur Verfügung stellt um die „Connected Services“ anbieten zu können.[52]

Außerdem werden die Daten an die zwingend vorgeschriebene Haftpflichtversicherung übermittelt. Dort sind Kennzeichen und FIN mit den Angaben des Versicherungsnehmers verknüpft, welcher der Eigentümer oder Halter sein kann, aber auch ein sonst unbeteiligter Dritter.

Die FIN ist somit bestimmungsgemäß nicht direkt mit einer natürlichen Person verknüpft und stellt lediglich ein Sachdatum dar. Primär identifiziert das Datum ein konkretes Fahrzeug. Erst über die Verknüpfung mit weiteren Daten ist eine Identifizierung von Personen möglich. Aufgrund der gesetzlichen Vorschriften ist die FIN jedoch unweigerlich mit personenbezogenen Daten verknüpft und stellt somit ebenfalls ein Sachdatum mit Doppelbezug dar. Zudem bestehen wiederrum gegenüber den speichernden Behörden unterschiedliche Rechtsansprüche, nach denen Dritte die Herausgabe der Angaben verlangen können, z.B. um Haftungsansprüche nach Unfällen geltend zu machen oder anderweitige Straftaten zu verfolgen. In der Praxis wird die Identifizierung durch private Dritte jedoch regelmäßig über das Kennzeichen erfolgen, da dieses leichter zugänglich ist. Neben öffentlichen Stellen sind aber auch nicht-öffentliche Stellen in der Lage die FIN mit personenbezogenen Daten zu verknüpfen. Dieses wird in der Regel der Verkäufer vor Ort sein, der die Daten zumindest im schriftlichen Vertrag miteinander verknüpft. Außerdem wird die FIN zusammen mit den Käuferdaten regelmäßig an den Hersteller und Betreiber der Netzinfrastruktur übermittelt, sodass auch dieser anhand der FIN den Bezug zu einer natürlichen Person herstellen kann. Wird die FIN isoliert oder mit anderen reinen Sachdaten verarbeitet und

[52] Ausführlich zu diesen Konstellationen s. Kap. 6.2.1.1.

hat der Verantwortliche auch nicht die Intention den Halter oder Nutzer zu identifizieren, liegt kein personenbezogenes Datum vor. Sobald der Verantwortliche faktisch jedoch in der Lage ist, den Halter ohne große Anstrengungen zu identifizieren, da die personenbezogenen Daten bereits beim Verantwortlichen vorhanden sind, wird ein Personenbezug anzunehmen sein, der nur entfällt, wenn effektive technische und organisatorische Maßnahmen getroffen wurden um eine Verknüpfung der Daten auch tatsächlich zu verhindern. Die Anbieter von vernetzten und autonomen Fahrzeugen wollen im Regelfall die anfallenden Daten eines Fahrzeuges neben Auswertung zur Qualitätssicherung und Produktsicherung auch nutzen um dem Halter oder Fahrer auf diesen zugeschnittene Angebote zu machen.[53] Den Herstellern sind die Daten, sowohl FIN als auch die Käufer- und Halterdaten, bekannt und eine Identifizierung somit möglich und auch gewollt. In diesem Zusammenhang handelt es sich somit in der Regel bei der FIN um personenbezogene Daten.

- Sensordaten

Sensoren erheben wie bereits oben ausgeführt, unterschiedliche Arten von Daten. Die Daten über den Zustand des Fahrzeuges (Zustandsdaten) bestehen aus Angaben über die jeweilige gemessene Variable: Tankfüllstand, Bremsen- oder Reifenabnutzung, Luft- und Fahrbahntemperatur sowie die weiteren notwendigen Daten die zur Einschätzung des Zustandes aber auch des Fahrverhaltens erforderlich sind. Die Angaben erfolgen in der jeweils gültigen Maßeinheit (Grad, Liter, Bar, etc.). Ähnliche Datensätze erheben die Fahrsensoren. Diese versuchen ein Abbild der Umgebung zu schaffen und das Auto so sicher durch den Verkehr zu leiten. Das Radar und die Ultraschallsensoren messen die Entfernung zu festen Objekten. Das Lidar erstellt ein Abbild von der Umwelt in Form von Punktwolken, welche im Rohzustand von den Algorithmen ausgewertet werden.

Obwohl das Lidar ein Abbild von der Umwelt erstellt, somit auch von Menschen in der Umgebung, sind diese Daten für die menschliche Wahrnehmung nicht erkennbar. Ein Algorithmus ist allerdings auch nicht in der Lage basierend allein auf dieser Datenlage die abgebildeten Personen zu identifizieren. Auch die anderen Datensätze können keine personenbezogenen Daten darstellen, da es rein technische Daten und somit Sachdaten sind, die in ihrem Rohzustand keinen Bezug zu einer natürlichen Person herstellen.

Sobald diese Daten jedoch nicht mehr isoliert verarbeitet werden, sondern in Bezug zu Datensätzen stehen anhand derer eine natürliche Person bestimmbar ist, können auch diese Sachdaten rechtlich ein personenbezogenes Datum darstellen. Die Daten werden zwar in einem sachlichen Zusammenhang verarbeitet, der Zustand des Fahrzeuges oder der Umgebung wird analysiert, aber der Zustand lässt einen Rückschluss auf das Fahrverhalten einer natürlichen Person zu, welche durch die Verknüpfung der Sachdaten mit der FIN oder anderen Daten auch direkt identifiziert werden kann.[54] Somit stellen Sensordaten die zumindest in Zusammenhang mit der FIN stehen, Sachdaten mit Doppelbezug dar die beim vernetzten und autonomen Fahren einen Personenbezug zulassen.

- Standortdaten

Anhand des GPS Signales werden die Koordinaten des Fahrzeuges bis auf wenige Meter genau ermittelt. Angereichert mit zusätzlichen Informationen können die Koordinaten, z.B. anhand Kartenmaterials,

[53] Vgl. u.a. McKinsey, Monetizing Car Data, S. 22 ff.
[54] Vgl. *Krügel*, ZD 2017, 455, 459.

auch einer Adresse zugeordnet werden. Diese Adresse wiederrum kann durch mögliche (öffentlich zugängliche) Quellen wieder einer konkreten Person zugeordnet werden. Zusätzlich kann durch die regelmäßigen Messvorgänge die Geschwindigkeit und Richtung der Fortbewegung gemessen werden. Somit birgt diese Art von Daten ein großes Potential um das Verhalten und die Interessen von natürlichen Personen nachzuvollziehen. Artikel 4 Nr. 1 DS-GVO nennt bei der Identifizierbarkeit von Personen explizit Standortdaten als personenbezogenes Datum, und auch die Art. 29 Datenschutzgruppe in ihrem Arbeitspapier WP 185 nimmt generell an, dass Standortdaten einen Bezug zu einer natürlichen Person zuließen.[55]

Die rein abstrakten Ortungsdaten des Fahrzeuges, insbesondere wenn es sich nur um die Koordinaten handelt, lassen ohne Zusatzinformationen jedoch keinen unmittelbaren Rückschluss auf die Person zu. Es handelt sich somit um Sachdaten, die einen nicht personifizierten Standort auf der Welt markieren. Diese Koordinaten können auch um eine postalische Adresse spezifiziert werden, wobei ebenfalls erstmal keinen Bezug zu einer natürlichen Person herbeigeführt wird. Damit sind diese Daten nicht zwingend personenbezogen. Ortungs- oder Standortdaten allein lassen nämlich noch keine Identifizierung einer natürlichen Person zu, sondern stellen erstmal Sachdaten dar. Insbesondere existieren Längen- und Breitengerade unabhängig davon, ob sich dort derzeit eine natürliche Person aufhält.[56] Sofern dieses der Fall ist, wäre eine tatsächliche Identifikation der Person bei dem Vorliegen reiner Standortdaten nur möglich, wenn zusätzliche Informationen hinzugezogen würden, z.B. wenn sich der Verantwortliche in der Nähe der Koordinaten befände und die Person vor Ort identifizieren oder zumindest zuordnen könnte. Ein Personenbezug kann bzw. wird somit vor allem unter Zuhilfenahme von weiteren Merkmalen hergestellt werden.[57] Werden zusammen mit den Ortungsdaten weitere Daten übermittelt, die einen Bezug zu einer natürlichen Person herstellen können und in diesem Kontext verarbeitet werden, sind auch Ortungsdaten personenbezogene Daten. Gerade im Bereich des vernetzten und autonomen Fahrens lässt sich anhand der Standortdaten der Bezug zu einem spezifischen Fahrzeug herstellen, da hier immer weitere Identifikatoren übermittelt werden, u.a. die FIN oder die Seriennummer des Navigationssystems. Selbst wenn der Verantwortliche nicht den Namen der Person hat, lassen sich anhand von Standort- und Fahrzeugdaten Bezüge zu einer Person herstellen. Es ließe sich nicht nur feststellen, wo sich das Auto eines über die FIN identifizierbaren Halters befindet, sondern auch Rückschlüsse auf den Nutzer ziehen, z.B. dass der Nutzer des Fahrzeuges X sich zu bestimmten Zeitpunkten an Ort Y aufhält, welches die typischen Arbeitszeiten sind, und zu anderen Zeiten an Ort Z, welches die typischen Feierabendzeiten sind. Anhand der Daten lassen sich somit Wohnort und Arbeitsplatz des sonst unbekannten Fahrzeugnutzers ermitteln. Verknüpft mit der einem Navigationssystem innewohnenden Karte, lassen sich die Orte auch einer postalischen Adresse zuordnen und es ist im Ergebnis ohne unverhältnismäßigen Aufwand möglich die Person zu identifizieren. Somit lassen sich die Ortungsdaten dem Fahrzeug zuordnen, anhand dessen wiederrum der Halter ermittelt werden kann und eventuell sogar unterschiedliche Nutzer.

Geodaten stellen im Kontext des vernetzten und autonomen Fahrens in der Regel somit ein personenbezogenes Datum dar.

- Netzwerkdaten

[55] Art.-29-WP, Opinion 13/2011 on geolocation services on smart mobile devices, 10.
[56] So schon *Forgó/Krügel*, MMR 2010, 17, 19.
[57] Eine ähnliche Ansicht vertreten im Ergebnis *Forgó/Krügel*, MMR 2010, 17.

Damit Geräte in einem Netzwerk erreichbar sind, erhalten sie individuelle Nummern (numerische Bezeichnungen), sogenannte IP-Adressen. Die IP-Adresse basiert auf dem Internetprotokoll und ist dazu gedacht die Kommunikation mit anderen Geräten im Netzwerk zu ermöglichen. Damit ähnelt die IP-Adresse einer individuellen Hausanschrift oder Telefonnummer. Daher ist die IP-Adresse für die Identifizierung der Host- oder Netzwerkschnittstelle und des potenziellen Standorts verantwortlich.[58] Den Internet-Service-Providern werden IP-Adressen zugewiesen, die diese Adressen dann an die Benutzer des Netzwerkes verteilen. Die Adressen werden jedoch nur temporär vergeben, so dass der Benutzer mit jeder neuen Verbindung eine andere Adresse erhält (dynamische IP-Adressen).

Den jeweiligen Kommunikationspartnern sind nur die gegenseitigen IP-Adressen bekannt. Weitere Angaben, die sich auf eine natürliche Person beziehen, werden in diesem Kommunikationsprozess nicht übermittelt. Die IP-Adresse wird in der Regel beim Provider gespeichert, der zusätzlich auch die Daten des Vertragspartners, dem hier der Internetzugang gewährt wird, speichert. Zusammen mit dem Datum und der Uhrzeit kann der Anbieter somit feststellen, welchem Vertragspartner die IP-Adresse zu diesem konkreten Zeitpunkt zugewiesen war und damit anhand der Vertragsdaten den Anschlussinhaber identifizieren.[59] Somit kann zumindest der Dienstanbieter den Betroffenen identifizieren. Eine Identifikation der Person ist durch Dritte nicht unmittelbar möglich, da das notwendige Zusatzwissen fehlt und die Nutzung von dynamischen IP-Adressen auch die längerfristige Zuordnung von Anfragen zu einem bestimmten Anschluss verhindert. Eine IP-Adresse ist jedoch eine Kennnummer anhand derer es objektiv möglich ist einen Personenbezug herzustellen. Fraglich ist daher immer ob es einen vertretbaren Aufwand bedeutet und wahrscheinlich ist, den Inhaber zu identifizieren, oder ob dieses Unmöglich scheint bzw. einen unverhältnismäßigen Aufwand bedeutet.[60] Um den Benutzer identifizieren zu können, müssen sich die Dritten an den entsprechenden Dienstanbieter wenden und eine Reihe gesetzlicher Anforderungen erfüllen[61]. Die gesetzlichen Ansprüche stehen jedem zur Verfügung und somit wäre eine Identifizierung ohne unverhältnismäßig hohen Aufwand möglich.[62] Allerdings wäre auch ein Interesse an der Identifizierung nötig. Nicht jede Verarbeitung von IP-Adressen ist zur Identifizierung der Personen gedacht, sondern dient vielmehr, wie erwähnt, dem originären Zweck der Internetkommunikation. Werden die Adressen weiterverarbeitet, z.B. gespeichert, um möglichen Missbrauch oder andere rechtliche relevante Sachverhalte aufzuklären, besteht zumindest ein grundsätzliches Interesse an der Identifizierung der jeweiligen Missetäter.[63] Beim vernetzten und autonomen Fahren dienen die Adressen auch grundsätzlich erstmal der Möglichkeit zur Kommunikation mit dem Internet. Wird die IP-Adresse durch einen Webseitenbetreiber zu obengenannten Zwecken gespeichert, so handelt es sich auch in diesem Kontext um ein personenbezogenes Datum. Der Hersteller des Fahrzeuges, der möglicherweise gleichzeitig der Betreiber der Backend-Infrastruktur ist, wäre in der Lage die IP-Adresse mit den übermittelten Daten zu speichern. Somit könnte dieser, die IP-Adresse anhand der ihm bekannten Daten einer Person, zumindest dem Käufer oder Halter des Fahrzeuges, zuordnen. IP-Adressen können daher grundsätzlich als personenbezogene Daten anzusehen sein, insbesondere wenn die Infrastruktur durch den Autohersteller selber zur Verfügung gestellt wird.

Eine IMEI Nummer wird jeder mobilen Empfangseinheit zugewiesen, die mittels GSM oder UMTS kommunizieren. Die Adresse besteht aus 15 Ziffern mit denen das zugehörige Endgerät, hier das vernetzte

[58] Vgl. RFC 760, DOD Standard Internet Protocol (Januar 1980).
[59] Vgl. EuGH, Urteil vom 19.10.2016 – C-582/14 „Breyer“.
[60] Vgl. hierzu Erwägungsgrund 26 S. 3 und 4 DS-GVO.
[61] U.a. § 100j StPO i.V.m. § 113 TKG und § 406e StPO; §§ 101, 9 UrhG.
[62] EuGH MMR 2016, 842; BGH ZD 2017, 424.
[63] Vgl. dazu EuGH, Urteil vom 19.10.2016 – C-582/14 – Breyer.

Fahrzeug, eindeutig identifiziert werden kann. Die Ziffernfolgen setzen sich aus dem Code für die Zulassung des Endgerätes sowie die entsprechende Zulassungsstelle (8 Ziffern), der Seriennummer des Endgerätes (6 Ziffern) und einer Prüfziffer zusammen.[64] Mit der IMEI können die Netzwerkprovider feststellen um was für ein Gerät es sich handelt und ob dieses berechtigt ist das Netzwerk zu nutzen. Primärer Zweck der IMEI war es rechtswidrig erlangte Geräte von der Netzwerknutzung auszuschließen und damit quasi unbrauchbar zu machen. Das Gerät lässt sich somit individuell identifizieren, eine konkrete Zuordnung zu einer Person ist indes allein anhand dieser Kennung nicht möglich. Die Identifizierung von Personen ist dementsprechend nur in Verbindung mit weiteren Daten möglich, wie den entsprechenden Vertragsdaten oder sonstigen Nutzerkennungen. Solche einmaligen Ziffernfolgen, die dauerhaft mit einem entsprechenden Gerät verbunden sind und durch verschiedene involvierte Partner einem konkreten Nutzer zugeordnet werden können, können daher grundsätzlich ein personenbezogenes Datum darstellen. Die Art. 29 Datenschutzgruppe und auch der Düsseldorfer Kreis, das Gremium der unabhängigen Datenschutzbehörden des Bundes und der Länder, klassifizieren diese ständigen und eindeutigen „Geräte- und Kartenkennungen" grundsätzlich als „bestimmbar".[65] Ähnliches gilt für die IMSI Adresse. Die IMSI Adresse dient der Teilnehmererkennung in einem mobilen Netzwerk und ist auf der SIM-Karte des Vertragspartners gespeichert. Die Adresse setzt sich aus 15 Ziffern zusammen und enthält Angaben zum Land (sog. Länderkennung), zum genutzten Netzwerk und eine individuelle Nummer. Das zur Verfügung stellende Netzwerkunternehmen kann anhand der Vertragsdaten die IMSI Adresse einer Person zuordnen. Gegenüber dem Telekommunikationsanbieter handelt es sich somit um ein personenbezogenes Datum. Datenschutzbehörden und auch die Art. 29 Datenschutzgruppe sehen die IMSI Adresse wiederum als generell personenbezogenes Datum an.[66]

Im Ergebnis muss die IMEI Nummer sowie die IMSI Adresse als Sachdatum mit Doppelbezug klassifiziert werden, dass nur personenbeziehbar wird, wenn, wie bei den IP Adressen erläutert, die Verarbeitung in einen personenbezogenen Kontext gesetzt wird. Die gleiche Bewertung gilt für die unterschiedlichen Geräte-IDs (UDID, Device ID, Sender ID, etc.). Dabei handelt es sich um nummerische Kennungen, die durch den Mobilfunkanbieter oder Plattformanbieter einer Person zugeordnet werden können. Diese Daten sind bekannt durch mobile Netzwerkeinheiten (Smart Devices) und eine Zuordnung zu Personen ist somit möglich.[67]

- Kamerabilder

Die Kamera nimmt Videos der Umgebung auf und der Algorithmus wertet diese Bilder zusammen mit den anderen Sensordaten aus. Die Aufnahme von Bildern stellen technisch bereits Verarbeitungsvorgänge dar. Fraglich ist, ob die Verarbeitung von Aufnahmen auch datenschutzrechtlich als Verarbeitungsvorgang i.S.d. Art. 4 Nr. 2 DS-GVO einzuordnen ist. Dazu müssten die Aufnahmen personenbezogene Daten sein. Dies kann insbesondere der Fall sein, wenn Personen von der Aufnahme betroffen sind. Gesichter, aber auch individuelle Verhaltensweisen wie Bewegungsbilder oder biometrische Merkmale von natürlichen Personen, sind personenbezogene Daten. Um biometrische Merkmale auswerten zu können, werden Bilder von extrem hoher Auflösung benötigt und wohl auch in bestimmten Aufnahmewinkeln. Die Personen sind anhand der Gesichter grundsätzlich identifizierbar bzw. sogar identifiziert und Foto- und Videoaufnahmen somit personenbezogen. Betroffen von dieser Datenverarbeitung sind

[64] 3GPP, TS 22.016: International Mobile station Equipment Identities (IMEI), (V9.0, 2009).
[65] Düsseldorfer Kreis, Orientierungshilfe zu den Datenschutzanforderungen an App-Entwickler und App-Anbieter, 5; Art.-29-WP, Opinion 02/2013 on apps on mobile devices, 3.1.
[66] Ibid.
[67] *Weichert*, SVR 2014, 201, 204.

nicht nur andere Verkehrsteilnehmer, die zur Umgebungsanalyse aufgenommen werden, sondern auch der Fahrer selbst im Rahmen der Müdigkeitserkennung, sofern diese mittels einer Kamera durchgeführt wird.

- Daten im Infotainment-Service

Im Rahmen des „Infotainment-Services" werden unterschiedliche Daten verarbeitet. Dazu gehören viele der oben genannten Daten, inklusive der technischen Daten der Sensoren. So können dem Nutzer des Fahrzeuges unterschiedliche Services angeboten werden, die er basierend auf den Daten benötigt. Das können Daten für Werkstätten sein, um die analysierten Fehler zu beheben oder die nächste Tankstelle anzuzeigen. Um weitere Services nutzen zu können, z.B. Apps dritter Anbieter, sind zudem weitere Daten erforderlich, insbesondere Login-Daten inklusive der Mailadresse oder auch Zahlungsdaten. Diese Daten sind immer an eine Person geknüpft und damit personenbezogen.[68]

3.4. ZUSAMMENFASSUNG DER KATEGORISIERUNG DER DATEN

Viele der verarbeiteten Daten weisen damit einen Personenbezug auf, der nicht immer direkt im Datum zu finden ist aber zumindest im entsprechenden Verarbeitungskontext, weshalb der datenschutzrechtliche Anwendungsbereich eröffnet ist. Die Verknüpfung aller erhobenen Daten kann zur Profilbildung der unterschiedlichen Fahrzeugführer genutzt werden. Sobald die Daten mit anderen Daten (auch rein technischen) verknüpft werden und damit ein Informationsgehalt zur Person gewonnen werden kann, sind die Daten als personenbezogene Daten zu bewerten, auch wenn der konkrete Name nicht bekannt ist.[69]

3.5. VERARBEITUNG DER PERSONENBEZOGENEN DATEN

Des Weiteren muss für die Anwendbarkeit der DS-GVO gem. Art. 2 Abs. 1 DS-GVO die ganz oder teilweise automatisierte Verarbeitung der Daten vorliegen. Eine Verarbeitung ist gem. Art. 4 Nr. 2 DS-GVO jede mit oder ohne die Hilfe automatisierter Verfahren ausgeführten Vorgänge oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten. Die Verarbeitung in Form der Erhebung der Daten findet dabei zuallererst unmittelbar im Fahrzeug statt und eine Weiterverarbeitung und zumindest die temporäre Speicherung ebenso. Das Fahrzeug befindet sich dabei zumindest im Besitz des jeweiligen Betroffen und die Daten verlassen damit nicht dessen Herrschaftssphäre. Das Ziel der DS-GVO ist es, die personenbezogenen Daten von natürlichen Personen bei der Verarbeitung durch Dritte zu schützen. Verbleiben die Daten in der Sphäre des Betroffenen unterfallen die Daten grundsätzlich nicht dem Datenschutzrecht, da der Schutzbereich nicht eröffnet ist. Allerdings ist im Zusammenhang mit der Datenspeicherung in Fahrzeugen zu bedenken, dass der Fahrzeugnutzer keine Möglichkeiten hat, das Erheben der Daten zu steuern. Zwar kann der Betroffene eigene Einstellungen vornehmen, im Prinzip wird aber ein Großteil der Daten ohne eine reelle Einflussmöglichkeit des Nutzers erhoben und teilweise sogar ohne seine explizite Kenntnis. Damit befinden sich die Daten zwar physisch in der Herrschaftssphäre des Nutzers, aber niemand außer dem Hersteller, oder von ihm zertifizierte Dritte, kann auf die Daten zugreifen. Somit ist dem Betroffenen die Kontrolle über seine Daten entzogen.

[68] Darstellung der Möglichkeiten bei *Johannig/Mildner*, Car IT Kompakt, S. 6 (2015).
[69] *Weichert*, NZV 2017, 507, 510 aE.

Damit können zwar zu diesem Zeitpunkt keine Dritten über die Daten verfügen, aber dem Nutzer ist auch die Möglichkeit entzogen über die Daten zu verwalten und er kann daher auch nicht auf potentielle Übermittlungsvorgänge einwirken.

Das Datenschutzrecht ist jedenfalls anwendbar, wenn die Daten das Fahrzeug verlassen, also eine Übermittlung erfolgt. Bei nicht-vernetzten Fahrzeugen ist das der Fall, wenn der interne Fahrzeugspeicher bzw. die Steuergeräte durch eine Werkstatt oder den Hersteller ausgelesen werden. Sobald das Fahrzeug über eine Netzwerkfunktionalität verfügt und die im Fahrzeug befindlichen Daten an das Backendsystem des Herstellers oder eines sonstigen Dritten übermittelt werden, handelt es sich um eine Datenverarbeitung im Sinne der DS-GVO und der Schutzzweck ist somit eröffnet. Die vernetzten und autonomen Autos sind dabei per definitionem vernetzt und die Daten werden kurz nach der Erhebung auch bereits übermittelt. Dazu gehören nicht nur die Backend-Server der Hersteller sondern es wird auch mit den Betreibern der Infrastruktur kommuniziert, mit anderen Verkehrsteilnehmern sowie weiteren involvierten Dritten.

4. RAHMENBEDINGUNGEN DER VERARBEITUNG

Die im Smart Car erhobenen Daten sind somit zu einem Großteil personenbezogen oder werden durch die Verknüpfung mit anderen erhobenen Daten in einen personenbezogenen Kontext gesetzt. Daher sind für diese Verarbeitungsvorgänge die datenschutzrechtlichen Vorschriften anwendbar.

4.1. GESETZLICHER RAHMEN

Seit Mai 2018 ist das anwendbare Recht grundsätzlich die EU-Datenschutzgrundverordnung. Ergänzt wird dieser Rechtsrahmen durch weitere europäische Regelungen wie der Richtlinie (EU) 2016/680 (JI-RL) aber auch der älteren Richtlinie 2002/58/EG (ePrivacy RL). Außerdem können für gewisse Rechtsbereich nationale Gesetze der Mitgliedstaaten anwendbar sein. Die konkrete Anwendbarkeit der jeweiligen Rechtsrahmen ergibt sich aus dem sachlich-persönlichen Anwendungsbereich.

4.2. SACHLICH-PERSÖNLICHER ANWENDUNGSBEREICH

Die Verarbeitung personenbezogener Daten unterliegt grundsätzlich den Vorschriften der DS-GVO. Anwendbar ist diese gem. Art. 2 DS-GVO sofern die Daten ganz oder teilweise automatisiert verarbeitet werden, aber auch die analoge Verarbeitung ist umfasst, sofern die personenbezogenen Daten systematisch gespeichert werden oder werden sollen. Ausgenommen von der Anwendbarkeit der DS-GVO sind nur Datenverarbeitungen gem. Art. 2 Abs. 2 DS-GVO die in den persönlich-familiären Bereich fallen (lit. c)) oder die aufgrund bestimmter Regelungen nicht in den Anwendungsbereich der DS-GVO fallen (lit. a) und b)). Außerdem werden für Verarbeitungstätigkeiten durch die zuständigen Behörden „*zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit*“[70] besondere Vorschriften in der JI-RL vorgehalten, sodass diese hier auch Vorrang vor den Vorschriften DS-GVO haben. Weiterhin sind die Organe, Einrichtungen, Ämter und Agenturen der Union von den Regelungen der DS-GVO ausgenommen (Abs. 3).

[70] Siehe Art. 1 Abs. 1 JI-RL oder auch Art. 2 Abs. 2 lit. d DS-GVO.

Auf nationaler Ebene sind in Deutschland die Bundes- und Landesdatenschutzgesetze anwendbar sowie zahlreiche Spezialvorschriften in den unterschiedlichen Gesetzen. Im BDSG und den LDSGen werden die zahlreichen Öffnungsklauseln der DS-GVO konkretisiert sowie die JI-RL in nationales, anwendbares Recht umgesetzt. Das BDSG ist gem. § 1 Abs. 4 anwendbar, wenn die Datenverarbeitung durch öffentliche Stellen vorgenommen wird. Die Anwendbarkeit für nicht-öffentliche Stellen gilt nur für Datenverarbeitungen im Inland. Bereichsspezifische Vorschriften gehen der Anwendbarkeit des BDSG vor, § 1 Abs. 2 BDSG. Das BDSG verdrängt allerdings das Verwaltungsverfahrensgesetz soweit es die Verarbeitung personenbezogener Daten regelt. Außerdem findet das BDSG Anwendung, sofern die Datenverarbeitung durch öffentliche Stellen nicht in den Anwendungsbereich der DS-GVO oder JI-RL fällt. Die unterschiedlichen LDSG sind dort anwendbar, wo dem Bund die Regelungskompetenz fehlt. Das betrifft die öffentlichen Stellen im Land, insbesondere die Behörden, Organe und andere öffentlich-rechtlichen Organisationen des Landes, der Kommunen und ähnlichen Körperschaften sowie nicht-öffentlichen Stellen, sofern ihnen Aufgaben der öffentlichen Verwaltung übertragen worden sind. Die LDSGe werden in der Regel auch durch speziellere Rechtsvorschriften verdrängt.

Die Regelungsgegenstände der nationalen Datenschutzgesetze umfassen zahlreiche Sachverhalte. Neben der Ermächtigung, dass die Mitgliedstaaten besondere Verarbeitungssituationen eigenständig national regulieren können (Kapitel IX der DS-GVO), sind die Mitgliedstaaten gem. Art. 6 Abs. 2 DS-GVO dazu ermächtigt die Rechtsgrundlagen aus Art. 6 Abs. 1 1 lit. c) und lit. e) DS-GVO durch spezifischere Vorschriften präziser zu bestimmen, während Art. 6 Abs. 3 DS-GVO nähere materielle Vorgaben zur nationalen Umsetzung macht.

Die Bereitstellung der öffentlichen Verkehrsinfrastruktur für das vernetzte und autonome Fahren liegt dabei grundsätzlich in der Kompetenz und Zuständigkeit der Länder und den Kommunen.[71] Wird daher durch die zuständige Straßenbaubehörde eine Infrastruktur aufgebaut, die eine Kommunikation im Rahmen der Car-2-Infrastructure ermöglicht oder auch im Rahmen von Verkehrsleitzentralen[72], erheben die Länder oder die damit beauftragten Stellen auch die personenbezogenen Daten, die im Rahmen dieser Kommunikation verarbeitet werden. Demnach wären hier wohl die Vorschriften der Landesdatenschutzgesetze anwendbar.[73] Der straßenverkehrs- und zulassungsrechtliche[74] Teil ist dagegen im Grundsatz durch Bundesgesetze geregelt und der Bund könnte somit einheitliche Regelungen zur technischen Ausgestaltung der vernetzten und automatisierten Fahrzeuge schaffen, an welcher sich die Infrastruktur der Länder ausrichten müsste. Die datenschutzrechtliche Relevanz ergibt sich hier nur bei der Bestimmung der verantwortlichen Stelle und des anwendbaren Rechts. Die unterschiedlichen Kompetenzen der involvierten Stellen wirken sich auch auf das Datenschutzrecht aus, das durch die DS-GVO für öffentliche Stellen nur zu einem Teil harmonisiert wird. Gerade für die Bereiche der Verkehrslenkung, der Meldung von Hindernissen oder Gefahrenstellen sowie anderen für den Verkehrsfluss erforderlichen Daten, die aus den Datenverarbeitungsprozessen der Fahrzeuge gewonnen wird, aber auch für die Verarbeitung der Daten zu Zwecken der Ordnungswidrigkeiten- oder Strafverfolgung, sind unterschiedliche Gesetze anwendbar. Im konkreten Anwendungsfall muss somit immer die anwendbare Rechtsgrundlage herausgefiltert werden, insbesondere wenn öffentliche Stellen in die Datenverarbeitung einbezogen sind.

[71] Vgl. dazu u.a. § 5b StVG, § 5 FernStG, § 12 StrWG, §§ 44, 45 StVO.
[72] Vgl. Statement des BMVI zum automatisierten und vernetzten Fahren - Digitale Testfelder, https://www.bmvi.de/DE/Themen/Digitales/Automatisiertes-und-vernetztes-Fahren/automatisiertes-und-vernetztes-fahren.html (zuletzt aufgerufen am 16.08.2018).
[73] U.a. § 1 Nds. LDSG.
[74] StVG, StVZO, FZV.

Neben den gesetzlichen Vorschriften haben sich die Fahrzeughersteller eigene Verhaltensregeln im Umgang mit vernetzten und autonomen Fahrzeugen gegeben. So hat der Verband der Automobilindustrie (VDA) bereits 2014 Datenschutzprinzipien verabschiedet, die das vernetzte Fahren adressieren.[75] Darin werden drei sehr allgemein gehaltene Prinzipien genannt, die Transparenz, Selbstbestimmung und Datensicherheit fordern. Im Jahr 2015 hat der Europäische Verband der Automobilhersteller (ACEA) ein ähnliches Dokument veröffentlicht[76], in dem fünf Prinzipien genannt werden. Diese enthalten neben der Transparenz, der Selbstbestimmung (hier „customers choice) und Datensicherheit noch die Prinzipien, Datenschutz von Beginn der Entwicklung an einzubeziehen (Privacy by Design) und Daten nur in einem angemessenen Rahmen zu verarbeiten. Auch diese Prinzipien sind damit sehr allgemein gehalten und dürften gerade so den gesetzlichen Anforderungen entsprechen. Im Januar 2016 wurde vom VDA zusammen mit den Datenschutzbehörden des Bundes und der Länder eine gemeinsame Erklärung veröffentlicht.[77] Die dortigen rechtlichen Einschätzungen beziehen sich noch auf das ehemalige BDSG, dürften aber im Ergebnis auf die DS-GVO übertragbar sein. In der Erklärung wird anerkannt, dass die Daten eines Kraftfahrzeuges dann personenbezogen sind, wenn sie mit der FIN oder dem Kfz.-Kennzeichen verknüpft sind, der Automobilhersteller und Dritte dann als Verantwortlicher gelten, wenn die Daten aus dem Fahrzeug übertragen werden und ein Auskunftsanspruch gegenüber den Herstellern nur insoweit besteht, als das sie personenbezogene Daten speichern. Der Auskunftsanspruch soll aber nicht gelten, wenn die Hersteller nur ein datenspeicherndes System eingebaut haben, hierfür sollen dann die jeweiligen erhebenden Stellen verantwortlich sein.

4.3. DAS VERNETZTE UND AUTONOME FAHREN IM KONTEXT DER GRUNDSÄTZE DER VERARBEITUNG PERSONENBEZOGENER DATEN

Die Datenschutz-Grundverordnung enthält in Art. 5 DS-GVO verschiedene Grundsätze für die Verarbeitung personenbezogener Daten, die stets einzuhalten und insofern auch für die Verarbeitung personenbezogener Daten im Kontext von autonomen und vernetzten Fahren relevant sind. Diese sind im Detail:

4.3.1. RECHTMÄßIGKEIT, VERARBEITUNG NACH TREU UND GLAUBEN, TRANSPARENZ

Die DS-GVO erlaubt die Verarbeitung personenbezogener Daten unter den Voraussetzungen der in Art. 6 Abs. 1 DS-GVO festgelegten Rechtsgrundlagen: Eine Einwilligung (lit. a)), zur Erfüllung eines Vertrages oder vorvertraglicher Maßnahmen (lit. b)), aufgrund einer rechtlichen Verpflichtung (lit. c)), zum Schutz lebenswichtiger Interessen (lit. d)), zur Wahrnehmung einer Aufgabe im öffentlichen Interesse (lit. e)), oder wenn ein berechtigtes Interesse vorliegt und die schutzwürdigen Interessen des Betroffenen gegen die Datenverarbeitung nicht überwiegen (lit. f)).

[75] VDA, Datenschutz-Prinzipien für vernetzte Fahrzeuge (2014).
[76] ACEA, Principles of Data Protection in Relation to Connected Vehicles and Services (2015).
[77] Gemeinsame Erklärung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder und des Verbandes der Automobilindustrie, Datenschutzrechtliche Aspekte
bei der Nutzung vernetzter und nicht vernetzter Kraftfahrzeuge (2016).

Im Kontext von autonomen und vernetzten Fahren sind jedenfalls einige dieser Rechtsgrundlagen in den allermeisten Fällen nicht einschlägig: Für eine Einwilligung ist eine eindeutige bestätigende Handlung erforderlich[78], die sich nicht bereits durch das bloße Einsteigen in ein KFZ ableiten lässt. Während es beim Halter eines Smart Cars naheliegt, eine entsprechende Einwilligung einzuholen, dürfte sich dies bei einigen Anwendungsgebieten in der Praxis jedenfalls als schwierig erweisen. Werden beispielsweise über das Infotainment-System personenbezogene Daten - z.B. Präferenzen zu Temperatur oder Musik - von Mitfahrern oder anderen Nutzern des Fahrzeuges erhoben, könnte eine Verarbeitung personenbezogener Daten durch den KFZ-Hersteller vorliegen. Die Einholung einer Einwilligung von Mitfahrern wäre in der Praxis jedoch nur schwer umsetzbar. Dieselbe Wertung gilt insoweit auch für die Durchführung eines Vertrages als Rechtsgrundlage für die Verarbeitung, da Mitfahrer in aller Regel nicht in einem Vertragsverhältnis mit dem KFZ-Hersteller stehen dürften. Erschwerend kommt hinzu, dass bei verknüpften Systemen im Rahmen des autonomen und vernetzten Fahrens eine durchaus unübersichtliche Situation auch mit Blick auf die möglichen Vertragsverhältnisse besteht. Auch ein Schutz lebenswichtiger Interessen dürfte in aller Regel nicht einschlägig sein, da hierfür zwar keine unmittelbare Lebensgefahr, jedenfalls aber ein unmittelbarer Bezug zur körperlichen Integrität gegeben sein muss.[79] Dies dürfte sich bei einer bloß abstrakten Gefahr, die bei der Nutzung eines autonomen und vernetzten Fahrzeuges entsteht, jedoch noch nicht ableiten lassen.

Von besonderer Relevanz sind daher vor allem die Rechtsgrundlagen, die auf die Wahrung öffentlicher Interessen, eine rechtliche Verpflichtung, oder auf ein berechtigtes Interesse seitens des Verantwortlichen abstellen. Insbesondere wird zu untersuchen sein, ob der Gesetzgeber die Nutzung bestimmter Funktionalitäten oder Standards vorschreibt, und so etwa KFZ-Hersteller zur damit einhergehenden Datenverarbeitung zwingt oder entsprechende hoheitliche Aufgaben auf die Hersteller überträgt. Dies ist mit Blick auf die großen infrastrukturellen Herausforderungen jedenfalls bis zu einem gewissen Grad wahrscheinlich. Ergibt sich eine Pflicht zur Datenverarbeitung nicht unmittelbar, ist ein Rückgriff auf ein berechtigtes Interesse erforderlich. Hierbei sind jedoch auch die gegenläufigen Interessen des Betroffenen zu berücksichtigen, Risiken für seine Grundrechte und Grundfreiheiten möglichst zu minimieren. Diese Rechtsgrundlage ist die zentrale Abwägungsklausel in der DS-GVO[80], wobei dem Betroffenen stets ein Widerspruchsrecht nach Art. 21 DS-GVO zusteht.

Außerdem ist es fraglich, inwiefern in einem Smart Car dem Grundsatz der Transparenz nachgekommen werden kann und wie dieser gegenüber den Betroffen in diesem Kontext angemessen erfüllt werden kann. Die Transparenz muss dabei nicht nur für eine wirksame Einwilligung gewährt werden, sondern für jede Datenverarbeitung, gleich auf welcher Rechtsgrundlage diese basiert. Nähere Vorgaben sind den Art. 12 ff. DS-GVO zu entnehmen und sind ein explizites Recht des Betroffenen.

4.3.2. ZWECKBINDUNG

Der Grundsatz der Zweckbindung hat zwei Eckpfeiler: Personenbezogene Daten müssen für festgelegte, eindeutige und legitime Zwecke erhoben werden (Zweckspezifizierung) und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden (kompatible Nutzung).[81] Das Gebot der Zweckbindung ist eines der wesentlichen Grundpfeiler des Datenschutzes.[82] Es ist daher

[78] Vgl. Erwägungsgrund 32 DS-GVO.
[79] BeckOK DatenschutzR/*Albers/Veit*, DS-GVO Art. 6 Rn. 36.
[80] Gola/*Schulz*, Art. 6 Rn. 50.
[81] Art.-29-WP, Opinion 03/2013 on purpose limitation, 00569/13/EN WP 203; Art. 5 (1) (b) GDPR.
[82] Vgl. auch Art.-29-WP, Opinion 03/2013 on purpose limitation (WP203), 4; *Dammann*, ZD 2016, 307, 311.

essenziell wichtig den Zweck zu spezifizieren, um die Legitimität, das anwendbare Recht für die Datenverarbeitung sowie eventuelle Limitierungen festzulegen. Demnach muss der Zweck bereits vor der Datenverarbeitung festgelegt werden, Daten dürfen gerade nicht auf Vorrat erhoben werden. Dennoch kann die Weiterverarbeitung zu anderen Zwecken zulässig sein, wenn der Zweck kompatibel mit dem Zweck ist, für den die Daten ursprünglich erhoben wurden. Art. 5 Abs. 1 lit. b) S. 2 DS-GVO enthält Anhaltspunkte, was unter Kompatibilität im Sinne der DS-GVO zu verstehen ist: Eine Weiterverarbeitung für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke gilt gem. Art. 89 Abs. 1 nicht als unvereinbar mit den ursprünglichen Zwecken („Zweckbindung"). Eine Weiterverarbeitung zu anderen Zwecken unter der DS-GVO ist somit grundsätzlich möglich.[83] Dies ergibt sich auch aus Art. 6 Abs. 4 DS-GVO.[84] Ob für diesen Aspekt der Datenverarbeitung eine weitere Rechtsgrundlage neben derjenigen, die die Verarbeitung ursprünglich legitimiert hat, nötig ist, ist strittig.[85] Allerdings müssen angemessene Schutzmaßnahmen getroffen werden, um die Privatsphäre der Betroffenen zu schützen, etwa die Nutzung von Pseudonymisierung und Anonymisierung.[86]

Der Grundsatz der Zweckbindung ist auch für autonomes und vernetztes Fahren relevant: Wird ein Fahrzeug erworben, so ist der Zweck des Erwerbes in aller Regel wohl die Erlangung von Eigentum an dem Fahrzeug zur Nutzung als Fortbewegungsmittel. Das zur Verfügung stellen eines funktionsfähigen Fahrzeuges wird daher der Primärzweck bei jeder einzelnen Nutzung des Fahrzeuges nach dem Erwerb sein. Basierend auf diesem Zweck können Daten für die Nutzung der Fahrassistenzsysteme sowie den gebuchten extra Leistungen (Navigation, Freisprechanlage, etc.) verarbeitet werden. Etwas weitreichender ist der Zweck, sofern die Daten zum autonomen Fahren verarbeitet werden müssen. Hierzu ist zwangsweise eine Verkettung der einzelnen Daten erforderlich, um ein Gesamtbild erstellen zu können und darauf basierend die Fahrfunktionen anzupassen. Oftmals lassen sich, gerade aus größeren Datenmengen, auch weiterführende Informationen ableiten und umfangreiche Verhaltensprofile erstellen. In Ergänzung dazu können auch andere Zwecke wie Qualitätssicherung oder Produktsicherheit im Fokus der Verarbeitung stehen und somit weitere Verarbeitungsvorgänge erforderlich machen.[87] Vorbehaltlich der Frage, ob diese Daten nicht anonymisiert werden können (oder bereits anonym sind), wäre eine solche Verarbeitung aber nur rechtmäßig, wenn zuvor der Zweck entsprechend festgelegt wurde. Mit Blick auf die starke Vernetzung verschiedener Systeme kann sich eine genaue Beschreibung der Verarbeitungszwecke, bzw. eine Prüfung der Kompatibilität, jedoch als Herausforderung gestalten. Insbesondere die zunehmende Interoperabilität von Systemen und ihrer Daten-Pools kann sich mit Blick auf den Grundsatz der Zweckbindung als Herausforderung darstellen. Solch umfangreiche Datensätze sind oftmals weiteren Begehrlichkeiten ausgesetzt. Daten aus vernetzten und autonomen Fahrzeugen sind dabei besonders wertvoll, da diese Daten nicht nur „Big Data" sind, sondern durch ihre klare Zuordnung auch intelligent verknüpft werden können und somit einen noch größeren Nutzen aufweisen als beispielsweise Daten aus reinem Web-Traffic. So könnten Daten aus vernetzten Fahrzeugen einer-

[83] Vgl. auch Erwägungsgrund 50 DS-GVO.

[84] Zur Zweckänderung siehe ausführlich Kapitel 5.5.

[85] So wird etwa vertreten, dass Art. 6 Abs. 4 DS-GVO eine eigenständige Rechtsgrundlage darstelle, *Richter* DuD 2015, 735, 736; *Ziegenhorn/von Heckel* NVwZ 2016, 1585, 1590 f.; Dem wird entgegengehalten, dass kompatible Zwecke auf dieselbe Rechtsgrundlage gestützt werden wie die ursprüngliche Verarbeitung, so etwa Gola/*Schulz*, Art. 6 Rn. 185; BeckOK DatenschutzR/*Albers/Veit*, DS-GVO Art. 6 Rn. 75.

[86] Art. 89 DS-GVO.

[87] Vgl. Die umfassenden Zwecke u.a. bei Tesla Fahrzeugen, https://www.tesla.com/de_DE/about/legal, (zuletzt besucht am 20.08.2018).

seits zu Werbezwecken weitergenutzt werden und z.B. zielgerichtete Anzeigen für den Fahrer geschaltet werden. Andererseits ergeben sich jedoch auch gänzlich neue Geschäftsmodelle, wie pay as you drive oder vergleichbare Anwendungen.

Vor diesem Hintergrund scheint der Grundsatz der Zweckbindung beim vernetzten und autonomen Fahren von besonders hoher Relevanz. Weitere Ausführungen zu den Risiken einer Zweckänderung finden sich in Kapitel 5.5.

4.3.3. DATENMINIMIERUNG

Die Datenminimierung ist ein weiteres wichtiges Prinzip der DS-GVO für die Verarbeitung personenbezogener Daten.[88] Demnach müssen personenbezogene Daten dem Zweck angemessen und erforderlich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein. Im Kontext von autonomem und vernetztem Fahren bedeutet dies, dass die anfallenden personenbezogenen Daten auf das absolut nötige Minimum zu reduzieren sind. Durch die hohe Verfügbarkeit von Systemen, die zur Erhebung personenbezogener Daten geeignet sind, ist hierauf ein besonderes Augenmerk zu legen. So können Daten einerseits erhoben werden, um überhaupt den Fahrbetrieb zu ermöglichen, andererseits um z.B. ein hohes Maß an Komfort zu gewährleisten. Hier ist jeweils zu prüfen, welche Daten tatsächlich erforderlich sind und wie das Datenaufkommen reduziert werden kann. in Kapitel 2 erläuterten Technologien erfordern tendenziell eher mehr als weniger Daten, jedoch kann die Möglichkeit, die Daten besser zu verknüpfen, erlauben den Verantwortlichen diese besser zu nutzten, sodass anstatt von Big Data von Smart Data zu sprechen ist. Das Potential dieser Anwendungen steigt mit der Nutzung von intelligenten Systemen zur Analyse von Daten. Zugleich können im Smart Car Kontext die Daten bereits bei der Erhebung viel besser zugeordnet werden. Dadurch könnte - bei entsprechender Umsetzung - das Aufkommen von Daten minimiert werden.

Eine weitere Möglichkeit zur Datenminimierung kann in der Anonymisierung zum frühestmöglichen Zeitpunkt bestehen.[89] Die autonomen und vernetzten Fahrzeuge produzieren eine erhebliche Menge an Daten[90] und sobald diese die Sphäre des Betroffenen verlassen, ist die Rechtfertigung notwendig. Die Erhebung von Daten über den eigentlichen Zweck hinaus muss, soweit die Zwecke nicht nach Art. 6 Abs. 4 DS-GVO vereinbar sind, dagegen gesondert begründet und auf einer eigenen Rechtsgrundlage basieren.

Ferner kann auch die Implementierung von Privacy by Design und Privacy by Default zur Datenminimierung beitragen.[91] Weitere Ausführungen hierzu finden sich in Kapitel 5.6.

[88] Art. 5 Abs. 1 lit. c) DS-GVO.
[89] Beispiele zur Umsetzung der Datenminimierung finden sich etwa im Standard-Datenschutzmodell unter https://www.huntonprivacyblog.com/wp-content/uploads/sites/28/2017/04/SDM-Methode_V_1_0.pdf.
[90] Vgl. Kapitel 3.
[91] Ehmann/Selmayr/*Heberlein*, Art. 5 Rn. 23.

4.3.4. RICHTIGKEIT

Personenbezogene Daten, die verarbeitet werden, müssen außerdem korrekt sein und, wo erforderlich, aktuell gehalten werden. Dieses Prinzip erlegt den Verantwortlichen eine Pflicht auf mit allen vertretbaren Schritten sicherzustellen[92], dass die verarbeiteten Daten korrekt sind. Im Kontext von autonomen und vernetzten Fahrens ist zu differenzieren: Da die im Fahrzeug verbauten Systeme weitestgehend mit „live-Daten" arbeiten und hier die Korrektheit der Daten für einen ordnungsgemäßen Betrieb absolut erforderlich ist, dürften sich in der Praxis nur wenige Probleme ergeben, insofern es sich um für das autonome und vernetzte Fahren erforderliche Daten handelt, beispielsweise von den Sensoren. Umgekehrt ergeben sich im Falle falscher Daten im Betrieb im Zweifel weitaus gravierendere Rechtsfolgen als eine Verletzung des Datenschutzes, etwa bei einem durch unrichtige Daten verursachten Unfall. Die Einhaltung dieses Prinzips ist, insbesondere hinsichtlich für den Fahrbetrieb erforderlich Daten, bereits faktisch ein großes Interesse der Verantwortlichen. Für die Richtigkeit von Bestandsdaten, etwa Informationen über den Fahrer, ergibt sich wiederum ein anderes Bild. Problematisch wird das Erfordernis der Richtigkeit der Daten, sobald das Fahrzeug von unterschiedlichen Fahrern genutzt wird oder der Eigentümer wechselt. Werden die Daten hier vermischt oder nicht korrekt zugeordnet, können die Hersteller bzw. der Verantwortliche falsche Annahmen treffen, die sich möglicherweise negativ auf den Betroffenen auswirken.

4.3.5. SPEICHERBEGRENZUNG

Das Prinzip der Speicherbegrenzung besagt, dass personenbezogene Daten in einer Form gespeichert werden müssen, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist.[93] Eine weiterführende Speicherung ist gem. Art. 5 Abs. 1 lit. e) 2. Hs. DS-GVO nur für im öffentlichen Interesse liegende Archivzwecke oder für wissenschaftliche und historische Forschungszwecke oder für statistische Zwecke gem. Art. 89 Abs. 1 DS-GVO möglich. Das Prinzip der Speicherbegrenzung ist eine Konkretisierung des Zweckbindungs- und Verhältnismäßigkeitsgrundsatzes in zeitlicher Hinsicht.[94] Eine weitere Konkretisierung erfolgt teils direkt in der DS-GVO: Gem. Art. 13 Abs. 2 lit. a), Art. 14 Abs. 2 lit a) und Art. 15 Abs. 1 lit. d) DS-GVO ist dem Betroffenen die Dauer der Speicherung mitzuteilen, oder falls dies nicht möglich ist, die Kriterien für ihre Festlegung. Demnach muss die Speicherbegrenzung nicht in einer absoluten, kalendarischen Festlegung erfolgen, sondern beispielsweise auch durch die Bestimmung einer Maximalfrist.[95]

Für autonomes und vernetztes Fahren hat der Grundsatz der Speicherbegrenzung insofern Bedeutung, als dass – wie bereits bei der Datenminimierung – überlegt werden muss, wann personenbezogene Daten frühestmöglich gelöscht, bzw. anonymisiert werden können. Insbesondere ist also zu prüfen, für welche konkreten Zwecke ein möglicher Personenbezug erforderlich ist (etwa bei der Berechnung von Fahrtrouten o.ä.) und wann nicht (etwa bei der Prognose von Verkehrsaufkommen auf Basis vorangehender Zahlen). Insbesondere wenn die Daten für die aktuellen Fahrfunktionen notwendig sind und nur für die jeweilige Situation, ließe sich begründen, dass nach Ende der Situation die Daten nicht mehr erforderlich sind und somit gelöscht, bzw. anonymisiert werden müssten. Auch eine Übermittlung der Daten an den Hersteller ließe sich unter diesem Aspekt nicht begründen, da eine lokale Verarbeitung notwendig ist, um die Übertragungswege und damit die Reaktionswege klein zu halten. Erforderlich

[92] Vgl. Erwägungsgrund 39.
[93] Art. 5 Abs. 1 lit. e) DS-GVO.
[94] Gola/*Pötters*, Art. 5 Rn. 25.
[95] Ehmann/Selmayr/*Heberlein*, Art. 5 Rn. 25.

wäre grundsätzlich nur die Kommunikation mit dem direkten Fahrzeugumfeld sowie den Einrichtungen zur Navigation oder Sicherheitseinrichtungen.

4.3.6. INTEGRITÄT UND VERTRAULICHKEIT

Neben den Grundsätzen zur Verarbeitung als solcher fordert die DS-GVO auch, dass personenbezogene Daten in einer Weise verarbeitet werden, bei der die Integrität und die Vertraulichkeit gewahrt wird.[96] Ohne Datensicherheit kann es keinen wirksamen Datenschutz geben.[97] Entsprechend dürfen personenbezogene Daten auch nur verarbeitet werden, wenn ein angemessenes Sicherheitsniveau stets gewährleistet ist. Dies umfasst den Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung.[98] Um dies zu erreichen, sind geeignete technische und organisatorische Maßnahmen umzusetzen.[99] Diese Maßnahmen umfassen die Pseudonymisierung und Verschlüsselung von Daten soweit erforderlich bzw. möglich, sowie ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der umgesetzten Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung. Hinsichtlich der Anforderung, die Daten nicht nur vor unberechtigtem Zugriff zu schützen, sondern auch vor unbeabsichtigtem Verlust, steht die Vorschrift im Spannungsverhältnis mit anderen Grundsätzen wie der Datenminimierung und Speicherbegrenzung, da Sicherungskopien nicht vom Archivzweck erfasst sind und somit diesen Grundsätzen zuwiderlaufen.[100]

Die Integrität und Vertraulichkeit von Systemen autonomer oder vernetzter Fahrzeuge sind, wie auch bereits die Korrektheit der Daten, kein rein datenschutzrechtliches Interesse. Der unrechtmäßige Zugriff auf kritische Infrastrukturen kann schwerwiegendste Folgen haben. Gleichwohl ist sicherzustellen, dass angemessene IT-Sicherheitsmaßnahmen auch dann angewendet werden, wenn Daten nicht in kritischen Infrastrukturen verarbeitet werden. Im Sinne der Richtlinie 2008/114/EG sind Transport und Verkehr, aber auch Informationstechniken und Telekommunikation, kritische Infrastrukturen. Im Rahmen des vernetzten und autonomen Fahrens kommen beide Aspekte zusammen und sind geeignet, bei einem Ausfall oder im Fall von Manipulation konkret Menschenleben zu gefährden. Zudem kann das Eindringen in die Systeme einen erheblichen Eingriff in die Privatsphäre der Betroffenen darstellen. Denn die im Fahrzeug gespeicherten Daten lassen einen umfassenden Rückschluss auf die Verhaltensweisen des Betroffenen zu und liefern Informationen zu aktuellen Tätigkeiten und Positionen. Die Integrität und Vertraulichkeit der Daten sind somit sowohl aus Aspekten des Datenschutzes aber auch der Sicherheit für die Betroffenen von hoher Bedeutung.

4.3.7. RECHENSCHAFTSPFLICHT

Die Rechenschaftspflichten legen dem Verantwortlichen die Pflicht auf, nachzuweisen, dass er sich an die durch die DS-GVO auferlegten Pflichten hält, hier insbesondere Grundsätze der Datenverarbeitung aus Art. 5 Abs. 1 DS-GVO. Dies kann z.B. durch die Dokumentation relevanter Handlungen erfolgen, z.B. die Einholung von Einwilligungen, die Umsetzung technischer und organisatorischer Maßnahmen

[96] Vgl. Art. 5 Abs. 1 lit. f) DS-GVO.
[97] Auernhammer/*Kramer/Meints*, DS-GVO Art. 5 Rn. 5.
[98] Kühling/Buchner/*Herbst*, Art. 5 Rn. 74 f.
[99] Vgl. Art. 32 DS-GVO.
[100] Plath/*Plath*, Art. 5 Rn. 20.

gem. Art. 24 DS-GVO, sowie das Bereithalten des Verzeichnisses der Verarbeitungstätigkeiten gem. Art. 30 DS-GVO.[101]

Für autonomes und vernetztes Fahren ergeben sich hier keine spezifischen Probleme. Zu beachten ist jedoch, dass zunächst wirksame technische und organisatorische Maßnahmen getroffen werden. Das umfasst auch die Maßnahmen für die Kommunikation mit den vernetzten und automatisierten Fahrzeugen sowie die Verarbeitung in diesen Fahrzeugen. Weiterhin sind während der Produktentwicklung die in Art. 25 DS-GVO stipulierten Grundsätze des "Privacy by Design" und "Privacy by Default" einzuhalten.[102]

Bezüglich der Frage, wie die Nachweise erbracht werden können, ergeben sich Anhaltspunkte aus Art. 35 Abs. 7 lit. d) DS-GVO, wonach Garantien, Sicherheitsvorkehrungen und Verfahren einzuführen sind, um den Schutz personenbezogener Daten sicherzustellen.[103] Im Umkehrschluss kann also angenommen werden, dass dokumentierte Verfahren der Nachweispflicht genügen.[104] Dies scheint auch vor dem Hintergrund, dass die Nachweispflicht insbesondere im Hinblick auf Überprüfungen durch Aufsichtsbehörden relevant ist[105], naheliegend.

Weitere Ausführungen, insbesondere zur Umsetzung beim vernetzten und autonomen Fahren, finden sich in Kapitel 5.6.

4.3.8. DIE BETROFFENENRECHTE

Wenngleich die Betroffenenrechte keines der in Art. 5 DS-GVO genannten Prinzipien sind, stellen die Betroffenenrechte einen integralen Bestandteil des in der DS-GVO verankerten Schutz personenbezogener Daten dar. Die Betroffenenrechte sind in den Art. 15 - 21 DS-GVO verankert und dort näher erläutert. Diese sind auch für Anwendungen beim autonomen und vernetzten Fahren relevant.

- **Informationspflichten:** Die Informationspflichten legen dem Verantwortlichen die Pflicht auf, Betroffene bei der Erhebung ihrer personenbezogenen Daten zu informieren. Diese Pflicht umfasst insbesondere Informationen über[106]:

    a) den Namen und die Kontaktdaten des Verantwortlichen sowie gegebenenfalls seines Vertreters;
    b) gegebenenfalls die Kontaktdaten des Datenschutzbeauftragten;
    c) die Zwecke, für die die personenbezogenen Daten verarbeitet werden sollen, sowie die Rechtsgrundlage für die Verarbeitung;
    d) wenn die Verarbeitung auf Artikel 6 Absatz 1 Buchstabe f beruht, die berechtigten Interessen, die von dem Verantwortlichen oder einem Dritten verfolgt werden;
    e) gegebenenfalls die Empfänger oder Kategorien von Empfängern der personenbezogenen Daten und
    f) gegebenenfalls die Absicht des Verantwortlichen, die personenbezogenen Daten an ein Drittland oder eine internationale Organisation zu übermitteln, sowie das Vorhandensein oder das Fehlen eines Angemessenheitsbeschlusses der Kommission oder im Falle von Übermittlungen gemäß Artikel 46 oder Artikel 47 oder Artikel 49 Absatz 1

[101] Kühling/Buchner/*Herbst*, Art. 5 Rn. 80.
[102] Gola/*Pötters*, Art. 5 Rn. 29.
[103] Plath/*Plath*, Art. 5 Rn. 23.
[104] A.a.O.
[105] Kühling/Buchner/*Herbst*, Art. 5 Rn. 79.
[106] Siehe Art. 13 DS-GVO.

Unterabsatz 2 einen Verweis auf die geeigneten oder angemessenen Garantien und die Möglichkeit, wie eine Kopie von ihnen zu erhalten ist, oder wo sie verfügbar sind.

g) die Dauer, für die die personenbezogenen Daten gespeichert werden oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer;
h) das Bestehen eines Rechts auf Auskunft seitens des Verantwortlichen über die betreffenden personenbezogenen Daten sowie auf Berichtigung oder Löschung oder auf Einschränkung der Verarbeitung oder eines Widerspruchsrechts gegen die Verarbeitung sowie des Rechts auf Datenübertragbarkeit;
i) wenn die Verarbeitung auf Artikel 6 Absatz 1 Buchstabe a oder Artikel 9 Absatz 2 Buchstabe a beruht, das Bestehen eines Rechts, die Einwilligung jederzeit zu widerrufen, ohne dass die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung berührt wird;
j) das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde;
k) ob die Bereitstellung der personenbezogenen Daten gesetzlich oder vertraglich vorgeschrieben oder für einen Vertragsabschluss erforderlich ist, ob die betroffene Person verpflichtet ist, die personenbezogenen Daten bereitzustellen, und welche möglichen Folgen die Nichtbereitstellung hätte und
l) das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling gemäß Artikel 22 Absätze 1 und 4 und — zumindest in diesen Fällen — aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person.

Werden die Daten nicht direkt beim Betroffenen erhoben, gelten gem. Art. 14 DS-GVO weiterführende Pflichten:

a) den Namen und die Kontaktdaten des Verantwortlichen sowie gegebenenfalls seines Vertreters
b) zusätzlich die Kontaktdaten des Datenschutzbeauftragten;
c) die Zwecke, für die die personenbezogenen Daten verarbeitet werden sollen, sowie die Rechtsgrundlage für die Verarbeitung;
d) die Kategorien personenbezogener Daten, die verarbeitet werden;
e) gegebenenfalls die Empfänger oder Kategorien von Empfängern der personenbezogenen Daten;
f) gegebenenfalls die Absicht des Verantwortlichen, die personenbezogenen Daten an einen Empfänger in einem Drittland oder einer internationalen Organisation zu übermitteln, sowie das Vorhandensein oder das Fehlen eines Angemessenheitsbeschlusses der Kommission oder im Falle von Übermittlungen gemäß Artikel 46 oder Artikel 47 oder Artikel 49 Absatz 1 Unterabsatz 2 einen Verweis auf die geeigneten oder angemessenen Garantien und die Möglichkeit, eine Kopie von ihnen zu erhalten, oder wo sie verfügbar sind;
g) die Dauer, für die die personenbezogenen Daten gespeichert werden oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer;
h) wenn die Verarbeitung auf Artikel 6 Absatz 1 Buchstabe f beruht, die berechtigten Interessen, die von dem Verantwortlichen oder einem Dritten verfolgt werden;
i) das Bestehen eines Rechts auf Auskunft seitens des Verantwortlichen über die betreffenden personenbezogenen Daten sowie auf Berichtigung oder Löschung oder auf Einschränkung der Verarbeitung und eines Widerspruchsrechts gegen die Verarbeitung sowie des Rechts auf Datenübertragbarkeit;
j) wenn die Verarbeitung auf Artikel 6 Absatz 1 Buchstabe a oder Artikel 9 Absatz 2 Buchstabe a beruht, das Bestehen eines Rechts, die Einwilligung jederzeit zu widerrufen, ohne dass die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung berührt wird;
k) das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde;

l) aus welcher Quelle die personenbezogenen Daten stammen und gegebenenfalls ob sie aus öffentlich zugänglichen Quellen stammen;
m) das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling gemäß Artikel 22 Absätze 1 und 4 und — zumindest in diesen Fällen — aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person

Dabei müssen die Informationen, wenn sie nicht direkt beim Betroffenen erhoben wurden, nach spätestens einem Monat zur Verfügung gestellt werden. Die bereits zuvor genannte Vernetzung der für autonomes und vernetztes Fahren erforderlichen Systeme stellt hier erneut eine besondere Herausforderung dar: Mit steigender Komplexität und Interoperabilität der Systeme steigen auch die involvierten Verantwortlichen, sodass sich eine Vielzahl an Informationspflichten ergeben kann. Gleichzeitig ist jedoch auch den Betroffenen nicht geholfen, wenn sie mit einer Vielzahl an Informationen überschüttet werden. Die Entwicklung von Lösungen, wie Betroffene sinnvoll und im Einklang mit der Rechtslage informiert werden können, ist daher ein wichtiger Aspekt für weitere Entwicklungen in diesem Bereich.

- **Recht auf Auskunft:** Eng verknüpft mit den Informationspflichten hat der Betroffene gem. Art. 15 DS-GVO außerdem das Recht von dem Verantwortlichen eine Bestätigung darüber zu verlangen, ob sie betreffende personenbezogene Daten verarbeitet werden. Ist dies der Fall, so hat sie ein Recht auf Auskunft über diese personenbezogenen Daten und auf folgende Informationen:

  a) die Verarbeitungszwecke;
  b) die Kategorien personenbezogener Daten, die verarbeitet werden;
  c) die Empfänger oder Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, insbesondere bei Empfängern in Drittländern oder bei internationalen Organisationen;
  d) falls möglich die geplante Dauer, für die die personenbezogenen Daten gespeichert werden, oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer;
  e) das Bestehen eines Rechts auf Berichtigung oder Löschung der sie betreffenden personenbezogenen Daten oder auf Einschränkung der Verarbeitung durch den Verantwortlichen oder eines Widerspruchsrechts gegen diese Verarbeitung;
  f) das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde;
  g) wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben werden, alle verfügbaren Informationen über die Herkunft der Daten;
  h) das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling gemäß Artikel 22 Absätze 1 und 4 und – zumindest in diesen Fällen – aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person.

  Ferner können bei der Übermittlung in ein Drittland besondere Pflichten gelten. Der Verantwortliche muss außerdem eine Kopie der personenbezogenen Daten, die verarbeitet werden, zur Verfügung zu stellen, sofern nicht Rechte Dritter entgegenstehen.

- **Recht auf Berichtigung:** Die betroffene Person hat gem. Art. 16 DS-GVO das Recht, dass sie betreffende personenbezogene Daten korrekt sind, d.h. unrichtige Daten müssen unverzüglich korrigiert werden. Dies kann auch die Vervollständigung der Daten betreffen. Im Kontext von autonomem und vernetztem Fahren scheint dieses Betroffenenrecht jedoch eher wenig relevant. Insbesondere dürften hiervon Fahrzeughalter betroffen sein, da Daten über Mitfahrer oder sonstige Verkehrsteilnehmer - sofern sie überhaupt personenbezogen sind - wohl unmittelbar erhoben würden, sodass sich hier eine vergleichsweise geringe Fehleranfälligkeit ergibt. Da Fahrzeughalter in aller

Regel in einem Vertragsverhältnis mit dem Fahrzeughersteller o.ä. stehen werden, dürfte eine Umsetzung dieses Rechts hier vergleichsweise einfach sein. Ist die Richtigkeit personenbezogener Daten strittig, ist die Verarbeitung gem. Art. 18 DS-GVO einzuschränken. Außerdem sind im Falle einer Berichtigung personenbezogener Daten Stellen, denen die Daten offengelegt wurden, zu informieren, Art. 19 DS-GVO.

- **Recht auf Löschung:** Der Betroffene soll gem. Art. 17 DS-GVO außerdem das Recht haben, vom Verantwortlichen die Löschung eigener personenbezogener Daten zu verlangen. Die Löschung muss dabei unverzüglich erfolgen, sofern einer der folgenden Gründe zutrifft:
    a) Die personenbezogenen Daten sind für die Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet wurden, nicht mehr notwendig.
    b) Die betroffene Person widerruft ihre Einwilligung, auf die sich die Verarbeitung gemäß Artikel 6 Absatz 1 Buchstabe a oder Artikel 9 Absatz 2 Buchstabe a stützte, und es fehlt an einer anderweitigen Rechtsgrundlage für die Verarbeitung.
    c) Die betroffene Person legt gemäß Artikel 21 Absatz 1 Widerspruch gegen die Verarbeitung ein und es liegen keine vorrangigen berechtigten Gründe für die Verarbeitung vor, oder die betroffene Person legt gemäß Artikel 21 Absatz 2
    d) Widerspruch gegen die Verarbeitung ein.
    e) Die personenbezogenen Daten wurden unrechtmäßig verarbeitet.
    f) Die Löschung der personenbezogenen Daten ist zur Erfüllung einer rechtlichen Verpflichtung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten erforderlich, dem der Verantwortliche unterliegt.
    g) Die personenbezogenen Daten wurden in Bezug auf angebotene Dienste der Informationsgesellschaft gemäß Artikel 8 Absatz 1 erhoben.

  Zu beachten ist jedoch, dass die Löschpflichten nicht schrankenlos gelten. So existieren etwa Ausnahmen zur Erfüllung einer rechtlichen Verpflichtung, die die Verarbeitung nach dem Recht der Union oder der Mitgliedstaaten, dem der Verantwortliche unterliegt, erfordert, sowie zur Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde (Art. 17 Abs. 3 DS-GVO). Diese Ausnahmeregeln könnten – je nachdem, wie autonomes und vernetztes Fahren im Endeffekt rechtlich ausgestaltet sein wird, vorliegend einschlägig sein. Andernfalls würde sich wiederum – wie auch bereits bei den Informationspflichten - die Problematik ergeben, dass sich die Löschung in der Praxis als schwierig erweisen könnte, insbesondere dann, wenn Mitfahrer oder andere Verkehrsteilnehmer betroffen sind.

- **Recht auf Datenübertragbarkeit:** Gem. Art. 20 DS-GVO haben Betroffene außerdem das Recht, die sie betreffenden personenbezogenen Daten, die sie einem Verantwortlichen bereitgestellt hat, in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten und diese Daten einem anderen Verantwortlichen zu übermitteln, ohne durch den Verantwortlichen, dem die personenbezogenen Daten bereitgestellt wurden, behindert zu werden. Hierbei sind verschiedene Konstellationen zu unterscheiden.

  Betreffen kann dies zunächst fahrerbezogene Informationen, z.B. beim Wechsel der Automarke. Hier ist zunächst zu prüfen, ob diese vom Anwendungsbereich des Art. 20 DS-GVO erfasst sind. Ausweislich Art. 20 Abs. 1 DS-GVO gilt dieses Recht nur für Daten, die vom Betroffenen bereitgestellt wurden. Nicht davon erfasst sind Daten, die auf einer Verarbeitung im Sinne einer Auswertung

durch den Verantwortlichen basieren.[107] Vielmehr müssen die Daten wissentlich und durch aktives Handeln vom Betroffenen bereitgestellt werden.[108] Insofern kämen hierfür allenfalls Stammdaten und selbst vom Nutzer eingestellte Informationen wie Adressen, Präferenzen, etc. in Betracht. Zu unterscheiden ist hierbei jedoch zwischen Informationen, die aktiv bereitgestellt werden und solchen, die mittels Analyse ermittelt wurden. So würde ein Anspruch auf Datenübertragung hinsichtlich der bevorzugten Sitzposition beispielsweise bestehen, wenn diese selbst vom Fahrer ausgewählt wurde, nicht jedoch, wenn diese ohne eigenes Zutun des Fahrers aus den typischen Sitzeinstellungen ermittelt wird.
Dieser Wertung folgend wären auch fahrtbezogene Informationen, die durch die Autohersteller bereitgestellt werden (z.B. zum Fahrverhalten), nicht von einem Anspruch auf Datenübertragung erfasst.

Ein weiterer Anwendungsfall kann in der Infrastruktur für das vernetzte und autonome Fahren gesehen werden. Für den allergrößten Teil der Infrastruktur dürfte sich hier jedoch gar kein praktischer Anwendungsfall zeigen, da diese nur einmalig existieren und ein „Umzug" von Daten insofern nicht in Frage kommt. Ohnehin dürfte ein Anspruch auf Datenübertragbarkeit hier ausgeschlossen sein: Gem. Art 20 Abs. 3 DS-GVO gilt dieses Recht nicht für eine Verarbeitung, die für die Wahrnehmung einer Aufgabe erforderlich ist, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde. Diese Begriffe finden sich bereits im Erlaubnistatbestand des Art. 6 Abs. 1 lit. e) DS-GVO wieder.[109] Eine abweichende Interpretation des Anwendungsbereiches liegt vorliegend fern.[110] In der Praxis sind Behörden demnach vom Anwendungsbereich des Art. 20 DS-GVO ausgenommen.[111] Das Gleiche gilt für nicht-öffentliche Stellen, die Daten im öffentlichen Interesse verarbeiten und in Einzelfällen öffentliche Gewalt ausüben.[112] Diese Ausnahmen dürften im Ergebnis jedenfalls sämtliche Bereiche bezüglich der für autonomes und vernetztes Fahren erforderlichen Infrastruktur betreffen. Der Anwendungsfall würde sich insofern auf Daten beschränken, die von den Automobilherstellern zu nicht-öffentlichen Interessen erhoben werden.

- **Recht auf Widerspruch:** Wird die Verarbeitung personenbezogener Daten auf Art. 6 Abs. 1 lit. e) oder f) DS-GVO gestützt, haben Betroffene außerdem das Recht, der Verarbeitung zu widersprechen, Art. 21 DS-GVO. Der Verantwortliche darf dann die personenbezogenen Daten nicht mehr verarbeiten, es sei denn, er kann zwingende schutzwürdige Gründe für die Verarbeitung nachweisen, die die Interessen, Rechte und Freiheiten der betroffenen Person überwiegen. Alternativ kann die Verarbeitung auch der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen dienen, um eine Weiterverarbeitung zu rechtfertigen.

  Hier dürften sich in der Praxis diverse Umsetzungsschwierigkeiten bezüglich des Widerspruchsrechtes ergeben, insbesondere von Mitfahrern und anderen Verkehrsteilnehmern.

[107] Kühling/Buchner/*Herbst*, Art. 20 Rn. 11.
[108] Gola/*Piltz*, Art. 20 Rn. 13.
[109] Paal/Pauly/*Frenzel*, DS-GVO Art. 6 Rn. 23 ff.
[110] BeckOK DatenschutzR/*von* Lewinsk,i DS-GVO Art. 20 Rn. 19.
[111] Gola/*Piltz*, Art. 20 Rn. 5.
[112] BeckOK DatenschutzR/*von Lewinski*, DS-GVO Art. 20 Rn. 21.

- **Automatisierte Entscheidungen im Einzelfall einschließlich Profiling:** Ferner haben Betroffene gem. Art. 22 DS-GVO das Recht, nicht einer ausschließlich auf automatisierter Verarbeitung – einschließlich Profiling – beruhenden Entscheidung unterworfen zu werden, die ihnen gegenüber rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt. Diese automatisierten Entscheidungen beziehen sich naturgemäß auf den Einsatz von Computerprogrammen, die selbstständig Entscheidungen treffen können, ohne dass es der Mitwirkung eines Menschen bedarf, was die Grundlage für das autonome Fahren bildet.[113]

  Mit Blick auf diesen Anwendungsbereich ergibt sich zunächst eine große Relevanz für das autonome und vernetzte Fahren, insbesondere auch vor dem Hintergrund, dass fast jede Entscheidung wenigstens mittelbar auch eine rechtliche Wirkung entfalten kann. Dies würde jedoch zu einem sehr breiten Anwendungsbereich der Norm führen, sodass eine einschränkende Auslegung geboten ist.[114] Die Untersuchung, welche Bereiche des autonomen und vernetzten Fahrens von dieser Norm erfasst sein können, ist daher für die Beurteilung der datenschutzrechtlichen Zulässigkeit von besonderer Relevanz. Genauere Ausführungen finden sich in Kapitel 5.4.

- **Recht auf Widerruf der Einwilligung:** Basiert die Verarbeitung personenbezogener Daten auf einer Einwilligung (Art. 6 Abs. 1 lit. a) DS-GVO), hat der Betroffene das Recht, die Einwilligung jederzeit zu widerrufen, vgl. Art. 7 Abs. 3 S. 1 DS-GVO. Der Widerruf der Einwilligung wirkt ex nunc.[115] Entsprechend wird die Rechtmäßigkeit von in der Vergangenheit erhobener Daten nicht berührt. Gleichwohl steht den Betroffenen ein Recht auf Löschung zu, sofern keine andere Rechtsgrundlage für die Verarbeitung einschlägig ist, vgl. Art. 17 Abs. 1 lit. b) DS-GVO.

- **Beschwerderecht bei der Aufsichtsbehörde:** Zuletzt steht Betroffenen auch das Recht zu, sich bei der Aufsichtsbehörde zu beschweren, wenn Sie der Auffassung sind, dass bei der Verarbeitung personenbezogener Daten gegen die DS-GVO verstoßen wird, vgl. Art. 13 Abs. 2 lit. d), Art. 14 Abs. 2 lit. e) sowie Art. 15 Abs. 1 lit. f) i.V.m. Art. 77 DS-GVO. Dabei ist durch den Verantwortlichen jedenfalls die für den Betroffenen zuständige Aufsichtsbehörde anzugeben.[116] Darüber hinaus kann sich der Betroffene durchaus auch an andere Aufsichtsbehörden wenden, gem. Art. 77 Abs. 1 DS-GVO so etwa in dem Mitgliedstaat ihres jeweiligen Aufenthaltsortes, ihres Arbeitsplatzes oder des Orts des mutmaßlichen Verstoßes.

Wenngleich das Beschwerderecht bei einer Aufsichtsbehörde – wie bei jeder Datenverarbeitung – durchaus relevant ist, dürften sich im Kontext des autonomen und vernetzten Fahrens keine spezifischen Herausforderungen für die Verantwortlichen ergeben. Die Bestimmung der jeweils zuständigen Behörden dürfte keine speziellen Probleme bereiten, wenngleich sich durch Betroffenen aus anderen Bundesländern bzw. dem (EU-)Ausland eine größere Komplexität ergibt. Dies ist allerdings kein spezifisches Problem des autonomen und vernetzten Fahrens, sondern eher allgemeiner Natur. Insofern ist davon auszugehen, dass die Aufsichtsbehörden hier entsprechende Erfahrungen sammeln und Verfahren zur Zusammenarbeit etablieren werden, sodass sich im Ergebnis kein nennenswertes Problem ergibt.

[113] Zu den einzelnen Automatisierungsgraden, vgl. Kapitel 2.1.
[114] BeckOK DatenschutzR/*von Lewinski*, DS-GVO Art. 22 Rn. 28.
[115] Paal/Pauly/*Frenzel*, DS-GVO Art. 7 Rn. 16.
[116] Paal/Pauly/*Paal*, DS-GVO Art. 15 Rn. 29.

4.3.9. DATENSCHUTZ-FOLGENABSCHÄTZUNG

Ein ebenfalls neu mit der DS-GVO eingeführtes Konzept ist die Datenschutz-Folgenabschätzung, Art. 35 DS-GVO. Diese ist gem. Art. 35 Abs. 1 DS-GVO durchzuführen, wenn eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat. Dies ist gem. Abs. 3 insbesondere in den folgenden Fällen erforderlich:

- systematische und umfassende Bewertung persönlicher Aspekte natürlicher Personen, die sich auf automatisierte Verarbeitung einschließlich Profiling gründet und die ihrerseits als Grundlage für Entscheidungen dient, die Rechtswirkung gegenüber natürlichen Personen entfalten oder diese in ähnlich erheblicher Weise beeinträchtigen;
- umfangreiche Verarbeitung besonderer Kategorien von personenbezogenen Daten gemäß Artikel 9 Absatz 1 oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gemäß Artikel 10 oder
- systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche;

Diese Auflistung ist jedoch nicht abschließend.[117] So können die Aufsichtsbehörden Positiv- wie Negativlisten erstellen, aus denen die Notwendigkeit bzw. Nichtnotwendigkeit einer Datenschutz-Folgenabschätzung hervor geht, vgl. Art. 35 Abs. 4 und 5 DS-GVO. Positiv-Listen wurden bereits von diversen Aufsichtsbehörden veröffentlicht, etwa Schleswig-Holstein[118], Hamburg[119], Baden-Württemberg[120], Rheinland-Pfalz[121] oder Niedersachsen[122]. Eine zusammenfassende Übersicht bietet die Auflistung der Datenschutz-Konferenz.[123]

Ausweislich der Auflistung der Datenschutz-Konferenz ist eine Datenschutz-Folgenabschätzung insbesondere dann durchzuführen, wenn eine umfangreiche Verarbeitung von personenbezogenen Daten über den Aufenthalt von natürlichen Personen vorliegt, vgl. Nr. 2.[124] Als typische Einsatzfelder werden hier

- die Fahrzeugdatenverarbeitung – Car Sharing / Mobilitätsdienste,
- Fahrzeugdatenverarbeitung – Zentralisierte Verarbeitung der Messwerte oder Bilderzeugnisse von Umgebungssensoren sowie
- Verkehrsstromanalyse auf der Grundlage von Standortdaten des öffentlichen Mobilfunknetzes

[117] Ehmann/Selmayr/*Baumgartner*, Art. 35 Rn. 20.
[118] https://www.datenschutzzentrum.de/uploads/datenschutzfolgenabschaetzung/20180525_LfD-SH_DSFA_Muss-Liste_V1.0.pdf.
[119] https://datenschutz-hamburg.de/assets/pdf/Liste%20Art%2035-4%20DSGVO%20HmbBfDI-%C3%B6ffentlicher%20Bereich_v1.0.pdf.
[120] https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2018/05/Liste-von-Verarbeitungsvorg%C3%A4ngen-nach-Art.-35-Abs.-4-DS-GVO-LfDI-BW.pdf.
[121] https://www.datenschutz.rlp.de/fileadmin/lfdi/Dokumente/Orientierungshilfen/DSFA_-_Muss-Liste_RLP_NOE.pdf.
[122] https://www.lfd.niedersachsen.de/download/131098/Liste_von_Verarbeitungsvorgaengen_nach_Art._35_Abs._4_DS-GVO.pdf.
[123] https://www.ldi.nrw.de/mainmenu_Aktuelles/submenu_EU-Datenschutzreform/Inhalt/EU-Datenschutzreform/DSFA-Muss-Liste-1_0.pdf.
[124] A.a.O.

genannt.[125] Darüber hinaus umfasst Nr. 4 die mobile optisch-elektronische Erfassung personenbezogener Daten in öffentlichen Bereichen, sofern die Daten aus ein oder mehreren Erfassungssystemen in großem Umfang zentral zusammengeführt werden. Hierzu zählt etwa die Fahrzeugdatenverarbeitung durch Umgebungssensoren.[126]

Vor diesem Hintergrund ist eine Datenschutz-Folgenabschätzung im Zuge des vernetzten und autonomen Fahrens hinsichtlich diverser Funktionalitäten erforderlich. Ein besonderes Risiko kann sich einerseits mit Blick auf die Gesamtheit des Systems und der damit verbundenen, umfangreichen Verarbeitung personenbezogener Daten ergeben, aber auch für Funktionalitäten, die ein Tracking erforderlich machen (Mobilitätsdienstleister, Kartendienste), sowie für die Nutzung von Sensoren und insbesondere Kamerasystemen.[127]

Ist eine Datenschutz-Folgenabschätzung erforderlich, so muss diese gem. Art. 35 Abs. 7 DS-GVO mindestens die folgenden Punkte beinhalten:

- eine systematische Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke der Verarbeitung, gegebenenfalls einschließlich der von dem Verantwortlichen verfolgten berechtigten Interessen;
- eine Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf den Zweck;
- eine Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen gemäß Absatz 1 und
- die zur Bewältigung der Risiken geplanten Abhilfemaßnahmen, einschließlich Garantien, Sicherheitsvorkehrungen und Verfahren, durch die der Schutz personenbezogener Daten sichergestellt und der Nachweis dafür erbracht wird, dass diese Verordnung eingehalten wird, wobei den Rechten und berechtigten Interessen der betroffenen Personen und sonstiger Betroffener Rechnung getragen wird.

Ebenfalls berücksichtigt werden können genehmigte Verhaltensregeln i.S.d. Art. 40 DS-GVO, vgl. Art. 35 Abs. 8 DS-GVO. Das Ziel der Datenschutz-Folgeabschätzung ist insofern, durch die Implementierung geeigneter Sicherungsmaßnahmen dafür zu sorgen, dass die identifizierten Risiken für die Betroffenen auf ein vertretbares und angemessenes Niveau reduziert werden.[128] Dementsprechend werden in den nachfolgenden Kapiteln neben der allgemeinen Zulässigkeit verschiedener Datenverarbeitungen ebenfalls Maßnahmen, die zu einer Reduzierung der Eingriffsintensität zugunsten der Betroffenen beitragen können, diskutiert.

5. PROBLEMORIENTIERTE ANWENDUNGSFÄLLE

5.1. VERANTWORTLICHKEIT UND ANWENDBARES RECHT

Beim autonomen und vernetzten Fahren kann sich eine insgesamt relativ komplexe Situation ergeben, sowohl bezüglich der involvierten Stellen, als auch – daraus resultierend – hinsichtlich der einschlägigen Rechtsnormen. Das folgende Kapitel soll daher die datenschutzrechtlich verantwortlichen identifizieren, als auch das jeweils einschlägige, anwendbare Recht aufzeigen.

[125] A.a.O.
[126] A.a.O.
[127] Siehe dazu im Detail Kapitel 5.3.
[128] Paal/Pauly/*Martini*, DS-GVO Art. 35 Rn. 54.

5.1.1. ÜBERSICHT

In diesen smarten Fahrzeugen können verschiedenste Stellen in eine Datenverarbeitung involviert sein. Die folgende Auflistung soll einen ersten Überblick über mögliche Konstellationen bieten:

- Natürliche Personen in Verbindung mit dem Fahrzeug
  - Der Eigentümer
  - Der Halter
  - Der Fahrer
  - Mitfahrer
- Die Autohersteller
  - Sitz in Deutschland
  - Sitz in Europa
  - Sitz außerhalb Europas
- Betreiber von Infrastruktur
  - Staatliche Stellen (Behörden, Kommunen, etc.)
  - Beliehene (Private Betreiber von Infrastruktur)
  - Privatunternehmen (u.a. Hersteller)
- Softwareanbieter
  - Navigation
  - Fahrzeugsteuerung
  - Fahrzeugzustand und -wartung
  - Infotainment
- Werkstätten
  - Ggf. im Ausland oder EU-Ausland
- Arbeitgeber
  - Ggf. im Ausland oder EU-Ausland
- Mobilitäts-Dienstleister
  - Fuhrparkbetreiber
  - Mietwagen-Firmen

Die nachfolgenden Kapitel sollen helfen die datenschutzrechtliche Einordnung dieser Stellen zu erleichtern. Insbesondere mit Blick auf eine Weitergabe von personenbezogenen Daten oder dem den vernetzten Systemen immanenten gemeinsamen Zugriff ist zwischen einer Übermittlung zu einem weiteren Verantwortlichen, gemeinsamer Verantwortlichkeit oder einer Auftragsverarbeitung zu differenzieren.

5.1.2. DEFINITION UND ABGRENZUNGSFRAGEN

5.1.2.1. VERANTWORTLICHKEIT GEM. ART. 4 NR. 7 DS-GVO

Der Begriff des Verantwortlichen ist in Art. 4 Nr. 7 DS-GVO definiert. Demnach ist „Verantwortlicher“ die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Hinsichtlich der Bestimmung des Verantwortlichen oder die dafür anwendbaren Kriterien können außerdem abweichende Regelungen durch das Unionsrecht oder das Recht der Mitgliedstaaten vorgesehen werden. An den Verantwortlichen knüpfen die Rechte und Pflichten aus der DS-GVO an, sie sind somit Normadressat.[129]

[129] BeckOK DatenschutzR/*Schild*, DS-GVO Art. 4 Rn. 88.

Die Verarbeitung von personenbezogenen Daten ist in Art. 4 Nr. 2 DS-GVO legaldefiniert als jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung. Somit ist jede Stelle, die dem Anwendungsbereich der DS-GVO unterliegt und über die Zwecke und Mittel einer der zuvor genannten Datenverarbeitungen entscheidet, verantwortlich im Sinne der DS-GVO. Dabei können auch mehrere Stellen gemeinsam verantwortlich sein.

5.1.2.2. GEMEINSAM VERANTWORTLICHE

Eine weitere Form der Zusammenarbeit bei der Verarbeitung personenbezogener Daten kann sich durch eine gemeinsame Verantwortlichkeit i.S.d. Art. 26 DS-GVO ergeben. Das Rechtsinstitut der gemeinsamen Verantwortlichen ist dabei neu im Unionsrecht: Zwar erwähnte auch Richtlinie 95/46/EC eine gemeinsame Verantwortung mehrerer Beteiligter (Art. 2 lit. d)), ohne jedoch die Voraussetzungen oder Rechtsfolgen näher zu spezifizieren.[130] Insofern knüpft Art. 26 DS-GVO an die bisher vorhandenen, lediglich grundsätzlichen (und teils strittigen) Wertungen an, die nun mit der DS-GVO weiter ausgeführt werden.[131]

Art. 26 Abs. 1 DS-GVO erfordert, dass zwei oder mehr Verantwortliche gemeinsam die Zwecke der und die Mittel zur Verarbeitung festlegen müssen, um gemeinsame Verantwortliche zu sein. Entsprechend ist die Gemeinsamkeit der Festlegung maßgeblich für den Anwendungsbereich.[132] Die gemeinsame Verantwortlichkeit ist vor allem dadurch gekennzeichnet, dass jeder der Beteiligten als „Herr der Daten" auf den Verarbeitungsvorgang, nämlich das erwartete und beabsichtigte Ergebnis („warum") der Datenverarbeitung und die Art und Weise, dieses Ergebnis zu erreichen („wie"), steuernd einzuwirken in der Lage ist.[133] Die gemeinsame Festlegung grenzt dabei die gemeinsame Verantwortung von der Auftragsverarbeitung (s.o.) ab[134], eine hierarchische Festlegung der Verantwortung und Zwecke erfolgt gerade nicht.[135] Auch eine symmetrische Aufteilung der Festlegung oder des Einfluss der beteiligten Parteien ist nicht erforderlich.[136] Gleichwohl muss jede Partei einen eigenen Zweck verfolgen, wobei auch dieser gemeinsam sein kann.[137] Dies ist insbesondere im Lichte der EuGH Entscheidung[138] zur gemeinsamen Verantwortung relevant. Demnach trage der Betreiber einer Facebook-Fanpage zusammen mit Facebook die Verantwortlichkeit bei der Verarbeitung der personenbezogenen Daten der Besucher der Fanpage. Dabei erkennen die Richter zwar an, dass in erster Linie die Facebook Inc. und, was die Union betrifft, Facebook Ireland über die Zwecke und Mittel der Verarbeitung der personenbezogenen Daten der Facebook-Nutzer und der Personen entscheidet.[139] Gleichwohl sei festzuhalten, dass der Betreiber einer auf Facebook unterhaltenen Fanpage durch die von ihm vorgenommene Parametrierung u. a. entsprechend seinem Zielpublikum sowie den Zielen der Steuerung oder Förderung

[130] Paal/Pauly/*Martini*, DS-GVO Art. 26 Rn. 17.
[131] Auernhammer/*Thomale*, DS-GVO Art. 26 Rn. 4.
[132] BeckOK DatenschutzR/*Spoerr*, DS-GVO Art. 26 Rn. 14.
[133] Paal/Pauly/*Martini*, DS-GVO Art. 26 Rn. 19.
[134] Ehmann/Selmayr/*Bertermann*, Art. 26 Rn. 6.
[135] BeckOK DatenschutzR/*Spoerr*, DS-GVO Art. 26 Rn. 16.
[136] A.a.O.
[137] BeckOK DatenschutzR/*Spoerr*, DS-GVO Art. 26 Rn. 17.
[138] EuGH Urteil vom 05.06.2018, Az. C-210/16.
[139] EuGH Urteil vom 05.06.2018, Az. C-210/16, Rn. 30.

seiner Tätigkeiten an der Entscheidung über die Zwecke und Mittel der Verarbeitung der personenbezogenen Daten der Besucher seiner Fanpage beteiligt ist.[140] Eine gleichwertige Verantwortlichkeit sei gerade nicht zwingend erforderlich - vielmehr können die Akteure in die Verarbeitung personenbezogener Daten in verschiedenen Phasen und in unterschiedlichem Ausmaß in der Weise einbezogen sein, so dass der Grad der Verantwortlichkeit unter Berücksichtigung aller maßgeblichen Umstände des Einzelfalls zu beurteilen sei.[141] Dem Schlussantrag des Generalanwalts in einem anderen Verfahren folgend sind die Wertungen zur gemeinsamen Verantwortlichkeit, die auf die inzwischen nicht mehr anwendbare Richtlinie zurück gehen, sinngemäß übertragbar, da die sich hinsichtlich der Auslegung von Schlüsselbegriffen keine nennenswerten Unterschiede ergeben.[142]

Ebenfalls relevant für die Frage einer gemeinsamen Verantwortlichkeit ist die für die Datenverarbeitung genutzte Infrastruktur. Dies insbesondere vor dem Hintergrund, dass im Kontext des autonomen und vernetzten Fahrens unterschiedliche Stellen involviert sind, die jedoch eng miteinander verknüpft sind und laufend Informationen austauschen müssen. Unproblematisch dürfte dies jedenfalls in einem einheitlichen Datenverarbeitungsvorgang auf einer gemeinsam betriebenen Infrastruktur sein.[143] Nicht jedoch abzustellen ist auf das Eigentum an der Datenverarbeitungsanlage – die körperliche Sachherrschaft kann auch bei einer gemeinsamen Verantwortlichkeit alleinig in den Händen eines Verantwortlichen liegen.[144] Auch kann die Funktionsherrschaft über einzelne Vorgänge an einen der Verantwortlichen übertragen werden, ohne dass dies einer gemeinsamen Verantwortlichkeit entgegensteht.[145] Gemeinsame Verantwortlichkeit kann sowohl von Anfang an – also mit der Erhebung der Daten – als auch nachträglich entstehen, etwa in einer Verarbeitungskette.[146] Bei einer nachträglichen Begründung erfolgt eine Offenlegung personenbezogener Daten durch Übermittlung, wenn dabei Daten physikalisch übertragen werden, oder „eine andere Form der Bereitstellung“ i.S.d. Art. 4 Nr. 2 DS-GVO.[147]

Im Falle einer gemeinsamen Verantwortlichkeit ist ferner eine Vereinbarung erforderlich.[148] Dabei ist die Vereinbarung jedoch keine Voraussetzung, sondern eine Rechtsfolge.[149] Die Rechtsfolgen der gemeinsamen Verantwortlichkeit werden in Kapitel 5.1.3.3 weiter ausgeführt.

Auch die gemeinsame Verantwortlichkeit scheint vor diesem Hintergrund für das autonome und vernetzte Fahren durchaus große praktische Relevanz zu haben. Die Abgrenzung zur bloßen Übermittlung ist jedoch, genau wie die zur Auftragsverarbeitung, jeweils im Einzelfall zu prüfen. Als entscheidendes Merkmal ist hier anzuführen, dass kein hierarchisches Verhältnis zwischen den Parteien besteht, beide einen (ggf. gemeinsamen) Zweck verfolgen, und beide auf den Verarbeitungsvorgang einwirken können.

---

[140] EuGH Urteil vom 05.06.2018, Az. C-210/16, Rn. 39.
[141] EuGH Urteil vom 05.06.2018, Az. C-210/16, Rn. 43.
[142] Schlussanträge des Generalanwalts Michal Bobek vom 19. Dezember 2018, Rechtssache C-40/17, Rn. 87. Abrufbar unter: http://curia.europa.eu/juris/document/document.jsf?text=&docid=209357&pageIndex=0&doclang=DE&mode=lst&dir=&occ=first&part=1&cid=2861666.
[143] Kühling/Buchner/*Hartung*, Art. 26 Rn. 15.
[144] BeckOK DatenschutzR/*Spoerr*, DS-GVO Art. 26 Rn. 19.
[145] Gola/*Piltz*, Art. 26 Rn. 10.
[146] Ehmann/Selmayr/*Bertermann*, Art. 26 Rn. 7.
[147] BeckOK DatenschutzR/*Spoerr*, DS-GVO Art. 26 Rn. 24.
[148] Ehmann/Selmayr/*Bertermann*, Art. 26 Rn. 10.
[149] Gola/*Piltz*, Art. 26 Rn. 9.

5.1.2.3. AUFTRAGSVERARBEITUNG

Erfolgt eine Verarbeitung im Auftrag eines Verantwortlichen (s.o.), unterliegt sie den Regelungen des Art. 28 DS-GVO. Gleichwohl ist der Begriff der Auftragsverarbeitung nicht näher in Art. 28 DS-GVO definiert.[150] Lediglich der Begriff des Auftragsverarbeiters ist gem. Art. 4 Nr. 8 DS-GVO als eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet, definiert. Eine vergleichbare Regelung enthielt bereits Art. 17 Abs. 2-3 der Richtlinie 95/46/EC.[151] Entsprechend kann zur weiteren Definition und Abgrenzung auch auf die Stellungnahme[152] der Art. 29 Datenschutzgruppe zurückgegriffen werden: Demnach seien insbesondere zwei Merkmale erforderlich, nämlich, dass die Organisation in Bezug auf den Verantwortlichen rechtlich eigenständig ist und dass die Verarbeitung nur in dessen Auftrag erfolgt.

Entscheidend ist also, dass der Verantwortliche weiterhin Herr der Verarbeitung ist.[153] Dabei kommt es vor allem auf die Weisungsgebundenheit des Auftragnehmers an.[154] Der Begriff der Weisung erfasst jede an den Normadressaten gerichtete Anordnung, die sich auf den Gegenstand und die Art des Umgangs mit Daten und der darauf bezogenen technischen und organisatorischen Maßnahmen bezieht.[155] Auch muss die Weisung hinreichend konkret sein; ein bloßes Dulden ist hingegen nicht ausreichend.[156] Charakteristisch ist also, dass der Auftragsverarbeiter zwar die Daten in seinem Machtbereich hat, diese jedoch nur dem Willen des Verantwortlichen entsprechend verarbeiten darf.[157] Im Umkehrschluss liegt also eine Auftragsverarbeitung dann nicht mehr vor, wenn dem Auftragnehmer die Möglichkeit offen steht, Daten auch ohne entsprechende Weisung zu verarbeiten. Dies wäre auch der Fall, wenn der Auftragnehmer eigene Interessen unmittelbar an den personenbezogenen Daten verfolgt, und diese etwa zu selbst gesetzten Zwecken verarbeitet.[158] Gem. Art. 28 Abs. 10 DS-GVO gilt ein Auftragsverarbeiter, der unter Verstoß gegen die DS-GVO die Zwecke und Mittel der Verarbeitung bestimmt, in Bezug auf diese Verarbeitung als Verantwortlicher. Dies ist auch von einer gemeinsamen Verantwortlichkeit abzugrenzen, da der Auftragsverarbeiter sich hier einseitig zum Entscheider aufschwingt.[159]

Schwierigkeiten bei der Frage, ob eine Weisungsgebundenheit vorliegt, ergeben sich aus dem Umstand, dass der DS-GVO nicht unmittelbar zu entnehmen ist, dass die Mittel der Verarbeitung ebenfalls durch den Verantwortlichen vorgegeben werden müssen. Dies könnte sich letztlich aus dem Umstand ergeben, dass Art. 4 Nr. 7 Hs. 1 DS-GVO dies als Merkmal der Verantwortlichkeit stipuliert.[160] Gleichwohl sind gem. Art. 28 Abs. 3 DS-GVO in einer Vereinbarung über die Auftragsverarbeitung lediglich Gegenstand und Dauer der Verarbeitung, Art und Zweck der Verarbeitung, die Art der personenbezogenen Daten, die Kategorien betroffener Personen und die Pflichten und Rechte des Verantwortlichen festzulegen. Im Umkehrschluss macht die Vorschrift deutlich, dass der Verantwortliche andere Aspekte

[150] BeckOK DatenschutzR/*Spoerr* DS-GVO Art. 28 Rn. 16.
[151] Ehmann/Selmayr/*Bertermann*, Art. 28 Rn. 1.
[152] Stellungnahme 1/2010 der Art. 29 Datenschutzgruppe zu den Begriffen „für die Verarbeitung Verantwortlicher“ und „Auftragsverarbeiter“, WP 169, 30.
[153] Kühling/Buchner/*Hartung*, Art. 28 Rn. 25 ff.
[154] Ehmann/Selmayr/*Bertermann*, Art. 28 Rn. 3.
[155] Paal/Pauly/*Martini*, DS-GVO Art. 29 Rn. 18.
[156] A.a.O.
[157] BeckOK DatenschutzR/*Spoerr*, DS-GVO Art. 28 Rn. 18.
[158] BeckOK DatenschutzR/*Spoerr*, DS-GVO Art. 28 Rn. 19.
[159] *Eckhardt*: DS-GVO: Anforderungen an die Auftragsverarbeitung als Instrument zur Einbindung Externer, CCZ 2017, 111 (116).
[160] Paal/Pauly/*Martini*, DS-GVO Art. 28 Rn. 35.

des „wie“ jedoch nicht vorgeben muss.[161] Dementsprechend haben Auftragsverarbeiter bei der Wahl der Mittel durchaus einen Entscheidungsspielraum.

Keine Auftragsverarbeitung liegt vor, wenn lediglich Hilfstätigkeiten ausgeführt werden, die nur bei Gelegenheit Zugang zu personenbezogenen Daten ermöglichen, ohne dass dies für die Hilfstätigkeit nötig oder sinnvoll ist.[162] Hier ist also im Einzelfall zu prüfen, ob diese Bedingungen vorliegen.

Insgesamt lässt sich also festhalten, dass für die Abgrenzung der Auftragsverarbeitung zur (gemeinsamen) Verantwortlichkeit die Beurteilung der Weisungsgebundenheit entscheidend ist. Hierbei kommt es weniger auf die Wahl der Mittel an, sondern auf die Frage, ob der Auftragnehmer ein eigenes Interesse an der Datenverarbeitung hat und ggf. selber über die Zwecke (mit-)bestimmen kann.

5.1.2.4. ÜBERMITTLUNG AN EINEN ANDEREN VERANTWORTLICHEN

Zuletzt kommt bei der Nutzung vernetzter Systeme auch eine Übermittlung an einen anderen Verantwortlichen in Betracht. Dies wäre der Fall, wenn Daten von einem Verantwortlichen an eine andere Stelle übermittelt werden, ohne dass eine Auftragsverarbeitung (s.o.) oder eine gemeinsame Verantwortlichkeit (s.o.) vorliegen.

Zu beachten ist hierbei, dass die Übermittlung als „Offenlegung“ gilt, mithin also eine Verarbeitung i.S.d. Art. 4 Nr. 2 DS-GVO darstellt.[163] Demnach ist für die Übermittlung – und auch für die nachfolgende Verarbeitung – jeweils eine Rechtsgrundlage erforderlich, vgl. Art. 6 DS-GVO. Im Gegensatz zur gemeinsamen Verantwortlichkeit oder der Auftragsverarbeitung ist diese aber weder bereits impliziert, noch ergeben sich grundsätzlich aus den Art. 26 und Art. 28 DS-GVO vergleichbare Vorschriften für eine Umsetzung.[164] Zudem werden die personenbezogenen Daten bei einer Übermittlung an Dritte dem Einflussbereich des Verantwortlichen entzogen, was Betroffene schutzwürdiger erscheinen lässt.

Im Kontext des autonomen und vernetzten Fahrens dürften hier insbesondere die Rechtsgrundlagen, die auf die Wahrung öffentlicher Interessen, eine rechtliche Verpflichtung, oder auf ein berechtigtes Interesse seitens des Verantwortlichen abstellen, relevant sein. Dies hängt jedoch auch stark davon ab, wie der Gesetzgeber zukünftig agieren wird, etwa ob bestimmte Funktionalitäten oder Standards verpflichtend vorgeschrieben werden, sodass hierfür entsprechende Rechtsgrundlagen vorhanden sind.

Je nach Anwendungsfall kann außerdem darüber nachgedacht werden, die personenbezogenen Daten vor der Übermittlung zu pseudonymisieren oder zu anonymisieren. Die Pseudonymisierung könnte dabei die Eingriffsintensität verringern und dazu beitragen, dass eine Übermittlung rechtmäßig erfolgen kann, z.B. bei einer Abwägung nach Art. 6 Abs. 1 lit. f) DS-GVO. Im Falle einer Anonymisierung entfiele der Personenbezug, sodass die DS-GVO keine Anwendung mehr finden würde. Entsprechend würde sich auch die Problematik einer erforderlichen Rechtsgrundlage nicht mehr ergeben.

[161] Paal/Pauly/*Martini*, DS-GVO Art. 28 Rn. 36.
[162] BeckOK DatenschutzR/*Spoerr*, DS-GVO Art. 28 Rn. 21.
[163] Auernhammer/*Eßer*, DS-GVO Art. 4 Rn. 17.
[164] zur Übermittlung in Drittländer siehe Kapitel 5.1.2.5.

5.1.2.5. ÜBERMITTLUNG VON DATEN IN DRITTLÄNDER

Bei der Übermittlung von personenbezogenen Daten in ein Drittland oder an eine internationale Organisation, sind außerdem – unabhängig ob im Rahmen einer Auftragsverarbeitung oder einer sonstigen Übermittlung – besondere, zusätzliche Regeln zu beachten, vgl. Art. 44 ff. DS-GVO.

Der Begriff des Drittlandes ist in der DS-GVO nicht definiert. Im europarechtlichen Kontext ist jedoch von einem Drittland bzw. Drittstaat in Abgrenzung zum Gemeinschaftsgebiet bzw. Mitgliedstaat die Rede, es handelt sich also demnach um ein Land, das nicht Mitglied in der Union ist.[165] Zugunsten der EWR-Staaten gibt es eine Übernahme-Entscheidung, die die DS-GVO in das EWR-Abkommen aufnehmen.[166]

Ausweislich Art. 4 Nr. 26 DS-GVO ist eine „internationale Organisation" eine völkerrechtliche Organisation und ihre nachgeordneten Stellen oder jede sonstige Einrichtung, die durch eine zwischen zwei oder mehr Ländern geschlossene Übereinkunft oder auf der Grundlage einer solchen Übereinkunft geschaffen wurde. Eine besondere Relevanz für das autonome und vernetzte Fahren ergibt sich für eine Übermittlung an eine solche Organisation derzeit nicht.

Die Übermittlung von Daten in Drittländer könnte im Kontext des autonomen und vernetzten Fahrens allerdings dann relevant sein, wenn Daten an Autohersteller mit Sitz in einem Drittland übermittelt werden. Von einer Übermittlung in ein Drittland ist grundsätzlich immer auszugehen, wenn Daten an einen Ort außerhalb des territorialen Geltungsbereiches der DS-GVO übermittelt werden.[167] Werden Daten ausschließlich durch eine rechtlich selbstständige, europäische Zweigstelle als Verantwortlichen verarbeitet, sind die Art. 44 ff. DS-GVO nicht einschlägig. Für eine Übermittlung innerhalb der Unternehmensgruppe müssten jedoch die Voraussetzungen der DS-GVO erfüllt sein: diesbezüglich schafft Kapitel V der DS-GVO einen abschließenden Katalog an Erlaubnistatbeständen.[168] Die dort festgelegten Voraussetzungen gelten zusätzlich zu den allgemeinen Anforderungen der DS-GVO an die Verarbeitung personenbezogener Daten.[169] Sie sind Im Rahmen einer zweistufigen Prüfungen zu evaluieren: Zunächst ist zu klären, ob die Übermittlung als solche - also unabhängig von einem Bezug zum Drittland - zulässig ist, entsprechend der in Art. 5 DS-GVO normierten Grundsätze.[170] In einem zweiten Schritt wird das Vorliegen eines Erlaubnistatbestandes der DS-GVO geprüft.[171] In Frage kommen verschiedene Szenarien:

- Gem. Art. 45 Abs. 1 DS-GVO darf eine Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation vorgenommen werden, wenn die Kommission beschlossen hat, dass das betreffende Drittland, ein Gebiet oder ein oder mehrere spezifische Sektoren in diesem Drittland oder die betreffende internationale Organisation ein angemessenes Schutzniveau bietet.
- Gem. Art. 46 Abs. 1 DS-GVO darf ein Verantwortlicher oder ein Auftragsverarbeiter personenbezogene Daten an ein Drittland oder eine internationale Organisation nur übermitteln, sofern der Verantwortliche oder der Auftragsverarbeiter geeignete Garantien vorgesehen hat und so-

[165] BeckOK DatenschutzR/*Kamp*, DS-GVO Art. 44 Rn. 6.
[166] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:22018D1022&from=DE.
[167] *Ambrock/Karg*: Ausnahmetatbestände der DS-GVO als Rettungsanker des internationalen Datenverkehrs?, ZD 2017, 154, 155.
[168] Paal/Pauly/*Pauly*, DS-GVO Art. 44 Rn. 11.
[169] BeckOK DatenschutzR/*Kamp*, DS-GVO Art. 44 Rn. 28.
[170] *Ambrock/Karg:* Ausnahmetatbestände der DS-GVO als Rettungsanker des internationalen Datenverkehrs?, ZD 2017, 154, 155.
[171] A.a.O.

fern den betroffenen Personen durchsetzbare Rechte und wirksame Rechtsbehelfe zur Verfügung stehen. Mögliche Garantien sind in Art. 46 Abs. 2 DS-GVO näher ausgeführt und beinhalten beispielsweise ein rechtlich bindendes und durchsetzbares Dokument zwischen den Behörden oder öffentlichen Stellen, oder Standarddatenschutzklauseln der Kommission oder der Aufsichtsbehörden nach Genehmigung durch die Kommission, oder genehmigten Verhaltensregeln gem. Art. 40 DS-GVO bzw. eine genehmigte Zertifizierung gem. Art. 42 DS-GVO.

- Gem. Art. 46 Abs. 2 lit. b) i.V.m. Art. 47 DS-GVO beim Vorliegen von im Kohärenzverfahren nach Artikel 63 DS-GVO genehmigten, verbindlichen internen Datenschutzvorschriften, sofern diese rechtlich bindend sind, den betroffenen Personen ausdrücklich durchsetzbare Rechte in Bezug auf die Verarbeitung ihrer personenbezogenen Daten übertragen und die in Art. 47 Abs. 2 DS-GVO festgelegten Anforderungen erfüllen.
- Im Falle des Fehlens der zuvor genannten Garantien und Sicherheiten kann eine Übermittlung auf einen in Art. 49 DS-GVO ausformulierten Katalog von Ausnahmen gestützt werden. Dies könnte im Kontext des autonomen und vernetzten Fahrens etwa die Übermittlung aus wichtigen Gründen des öffentlichen Interesses sein.

Insgesamt ist eine Übermittlung in ein Drittland also – unter Einhaltung der besonderen Voraussetzungen – möglich. Werden personenbezogene Daten innerhalb einer Unternehmensgruppe übermittelt, z.B. von einer rechtlich selbstständigen Zweigstelle in der europäischen Union an einen Hauptsitz im Drittland, könnte ein angemessenes Schutzniveau beispielsweise mit Standard-Vertragsklauseln i.S.d. Art. 46 DS-GVO erreicht werden. Spezifische Probleme für das autonome und vernetzte Fahren ergeben sich vor diesem Hintergrund nicht.

5.1.3. EINORDNUNG, RECHTSFOLGEN UND AUSWIRKUNGEN

Neben den bereits skizzierten Abgrenzungsschwierigkeiten bei der rechtlichen Einordnung gestaltet sich auch die Subsumtion im Einzelfall als schwierig. Insbesondere ist eine Vielzahl unterschiedlicher Konstellationen denkbar, die sowohl in der Sache als auch rechtlich zu einer unterschiedlichen Beurteilung führen können. Im folgenden Kapitel soll daher eine erste – beispielhafte – Einordnung der Beteiligten vorgenommen werden. Eine abschließende Beurteilung ist jedoch nur jeweils im konkreten Einzelfall möglich. Ferner werden die Rechtsfolgen, die sich aus den verschiedenen Modellen zur Verantwortlichkeit ergeben können, beschrieben.

5.1.3.1.1. NATÜRLICHE PERSON IN VERBINDUNG MIT KFZ

Als erste Gruppe sind natürliche Personen, die mit einem KFZ in Verbindung stehen, zu nennen, also etwa der Eigentümer, Fahrzeughalter oder Fahrer. Beim vernetzten und autonomen Fahren ist auch die Erfassung von Daten über die Insassen oder den Personenkreis im unmittelbaren Umfeld des Fahrzeuges denkbar, sofern über diese Personen, etwa weil sie sich zu einem Service im Fahrzeug anmelden, Daten erhoben werden. Sofern es sich hier um personenbezogene Daten handelt, stellt sich die Frage, in welcher Rolle der Halter bzw. Fahrer hier auftritt. Verantwortlicher i.S.d. DS-GVO ist, wie zuvor erläutert, die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet.

Dabei ist zunächst zu unterscheiden, in welchem Kontext die Daten erhoben werden. Sind Daten beispielsweise erforderlich, um den ordnungsgemäßen Betrieb des Fahrzeuges zu gewährleisten (z.B. Kamera- und Sensordaten), haben insbesondere die Autohersteller ein großes Interesse daran, diese Daten zu erfassen und zu verarbeiten, sie verfolgen eigene Verarbeitungszwecke. Zwar ist ein mangelfreies Auto auch im Interesse des Kunden, allerdings bezieht sich dieses Interesse weniger auf die Art oder Zwecke der Datenverarbeitung als solche, sondern primär darauf, ein funktionstüchtiges Fahrzeug

zu haben. Selbst wenn jedoch eine gemeinsame Zweckbestimmung angenommen würde, ist festzuhalten, dass der Fahrer bzw. Halter zunächst keinerlei Einfluss auf die Mittel der Verarbeitung hat. Gleichwohl ist im Lichte der EuGH Entscheidung zur gemeinsamen Verantwortlichkeit bei Facebook-Fanpages[172] zu beachten, dass die Schwelle dafür, eine gemeinsame Festlegung der Mittel anzunehmen, durchaus gering angelegt werden kann. Zwar bezieht sich das Urteil noch auf die inzwischen durch die DS-GVO ersetzte Richtlinie 95/46/EC, die noch keine konkreten Ausführungen zur gemeinsamen Verantwortlichkeit enthält; gleichwohl dürften sich die rechtlichen Wertungen grundsätzlich übertragen lassen, da die Definition in Art. 2 Buchst. d) DSRL im Kern inhaltsgleich in Art. 4 Nr. 7 und Art. 26 DS-GVO übernommen wurde.[173] Konkret führt der EuGH aus, dass "der Betreiber einer auf Facebook unterhaltenen Fanpage [...] durch die von ihm vorgenommene Parametrierung u. a. entsprechend seinem Zielpublikum sowie den Zielen der Steuerung oder Förderung seiner Tätigkeiten an der Entscheidung über die Zwecke und Mittel der Verarbeitung der personenbezogenen Daten der Besucher seiner Fanpage beteiligt" sei.[174] Gleichwohl wird anerkannt, dass "in erster Linie die Facebook Inc. und, was die Union betrifft, Facebook Ireland über die Zwecke und Mittel der Verarbeitung der personenbezogenen Daten der Facebook-Nutzer und der Personen entscheiden, die die auf Facebook unterhaltenen Fanpages besucht haben".[175] Dieser Wertung folgend ist also bereits ein minimaler Anteil bei der Bestimmung der Zwecke und Mittel ausreichend. Dies gilt insbesondere, wenn trotz fehlender Zweckidentität eine Einheit der Zwecke angenommen werden kann.[176]

In der vorliegenden Konstellation muss dennoch bezweifelt werden, dass ein Fahrzeughalter oder Fahrer hinsichtlich insassenbezogener Daten in einer gemeinsamen Verantwortlichkeit mit dem Autohersteller ist. Eine vergleichbare Möglichkeit wie bei Facebook-Fanpages zur Parametrierung des Zielpublikums ist im Kontext des vernetzten und autonomen Fahrens nicht erkennbar. Auch können - im Gegensatz zu Facebook-Fanpages - hier keine primär eigenen Interessen, wie etwa die Nutzung zu Werbezwecken, angenommen werden. Da der Halter bzw. Fahrer insassenbezogene Daten zum ordnungsgemäßen Betrieb des Fahrzeuges nicht selber verarbeitet oder sonst wie nutzt, fehlt es an der benötigten Mitwirkung. Die Tatsache, dass die Daten über die Systeme des Fahrzeuges gesammelt werden, kann dem nicht entgegenstehen, da es trotz dessen an entsprechenden Möglichkeiten zur Einflussnahme fehlt.

Eine andere Einschätzung kann sich hingegen bei Komfort-Funktionen wie dem Infotainment-System ergeben. Hier hat der Autohersteller zwar ein Interesse daran, gegenüber dem Kunden bestmöglichen Service zu bieten, gleichzeitig hat der Fahrzeughalter bzw. Fahrer wesentlich mehr Möglichkeiten zur Einflussnahme. Lassen sich etwa eigene Nutzerprofile für verschiedene Fahrer anlegen oder Präferenzen für Mitfahrer einstellen (z.B. Temperatur, Musikauswahl, etc.), dürfte ein entsprechender Beitrag anzunehmen sein. Sind durch eine entsprechende Nutzer- bzw. Admin-Oberfläche entsprechende Möglichkeiten gegeben, und werden diese durch den Halter bzw. Fahrer genutzt, läge eine hinreichende Mitwirkungsmöglichkeit vor, um ihn als Verantwortlichen zu qualifizieren. Gleichzeitig wäre im Einzelfall

[172] EuGH Urteil vom 05.06.2018, Az. C-210/16.
[173] *Petri*, Datenschutzrecht: Verantwortlichkeit von Facebook und des Betreibers einer Facebook-Fanpage für die Verarbeitung personenbezogener Daten, EuZW 2018, 534 (540).
[174] EuGH Urteil vom 05.06.2018, Az. C-210/16, Rn. 39.
[175] A.a.O, Rn. 30.
[176] Schlussanträge des Generalanwalts Michal Bobek vom 19. Dezember 2018, Rechtssache C-40/17, Rn. 105. Abrufbar unter: http://curia.europa.eu/juris/document/document.jsf?text=&docid=209357&pageIndex=0&doclang=DE&mode=lst&dir=&occ=first&part=1&cid=2861666

zu prüfen, ob der Autohersteller in dieser Konstellation die Daten überhaupt zu eigenen Zwecken verarbeitet oder ob diese nur lokal genutzt werden. Ohne weitergehende Verarbeitung durch den Autohersteller dürfte sich eine Verantwortlichkeit nur durch das bloße Bereitstellen der Software nicht ergeben.

Wenngleich eine datenschutzrechtliche Verantwortlichkeit des Halters bzw. Fahrers in diesem Kontext per Definition denkbar scheint, ist jedoch einschränkend anzumerken, dass im privaten bzw. familiären Kontext die Anwendbarkeit der DS-GVO ausgeschlossen ist, vgl. Art. 2 Abs. 2 lit. c) DS-GVO. Dies ist der Fall, wenn die Verarbeitung ohne Bezug zu einer beruflichen oder wirtschaftlichen Tätigkeit vorgenommen wird.[177] Bei der Frage, ob eine persönliche bzw. familiäre Tätigkeit vorliegt, kommt es indes nicht darauf an, ob tatsächlich Geld fließt.[178] Sie richtet sich vielmehr nach der Verkehrsanschauung.[179] Zur nicht-privaten Nutzung gehört u.a. der Dual Use, sowie vorbereitende Tätigkeiten wie beispielsweise Marktforschung oder Marketing.[180] Werden personenbezogene Daten - unter Mitwirkung einer natürlichen Person, z.B. Daten über Mitfahrer unter Mitwirkung des Eigentümers bzw. Halters - zu diesen Zwecken genutzt, kann also die Ausnahmeregelung entfallen. Ein weiteres denkbares Szenario für die Verarbeitung personenbezogener Daten Dritter könnte in der Erfassung von Passanten durch die im Fahrzeug verbauten Sensor-Systeme bestehen.[181] Nicht mehr von der Ausnahmeregelung des Art. 2 Abs. 2 lit. c) DS-GVO erfasst ist die Aufzeichnung des öffentlichen Raumes durch ein automatisiertes Kamerasystem, unabhängig davon, zu welchem Zwecke dies geschieht.[182] Dies betrifft insofern auch die Nutzung von Kamerasystemen im Auto.[183] Diese Wertung dürfte sich auch auf andere Sensorsysteme übertragen lassen, die personenbezogene Daten verarbeiten. Hier stellt sich jedoch auch die Frage, ob der Halter bzw. Fahrer überhaupt Zugriff auf die Daten oder - wie zuvor bezüglich fahrtbezogener Daten - keinerlei Mitwirkungsmöglichkeit hätte. In diesem Fall käme eine datenschutzrechtliche Verantwortlichkeit nicht in Betracht.

Insgesamt lässt sich somit festhalten, dass zunächst nach der Art der verwendeten Daten zu differenzieren ist. Daten, die lediglich für die technischen Abläufe erforderlich sind, dürften letztlich nicht der Verantwortlichkeit des Halters bzw. Fahrers unterfallen. Für Daten, auf die eine Zugriffs- bzw. Mitwirkungsmöglichkeit besteht, kann sich eine Verantwortlichkeit jedoch auch für den Halter bzw. Fahrer ergeben. Diese kann - wiederum je nach Zugriffs- und Mitwirkungsmöglichkeit des Autoherstellers - als gemeinsame oder alleinige Verantwortlichkeit ausgestaltet sein.

5.1.3.1.2. AUTOHERSTELLER

Den Autoherstellern kommt bei der Verarbeitung personenbezogener Daten im Kontext des vernetzten und autonomen Fahrens eine zentrale Rolle zu. Sie produzieren nicht nur die Fahrzeuge, sondern stellen auch die integrierte Software zur Verfügung.

Vor diesem Hintergrund kann festgehalten werden, dass Autohersteller zunächst Zweck und Mittel der Datenverarbeitung festlegen und somit als Verantwortliche i.S.d. Art. 4 Nr. 7 DS-GVO angesehen werden können. Allerdings sind auch andere Konstellationen denkbar:

Zunächst käme in Betracht, dass eine eigene Verantwortlichkeit ausgeschlossen ist, wenn der Autohersteller in bestimmten Bereichen selber keine personenbezogenen Daten verarbeitet. Gem. Art. 4 Nr. 2 DS-GVO bezeichnet „Verarbeitung“ jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten

[177] S. Erwägungsgrund 18 DS-GVO.
[178] Paal/Pauly/*Ernst*, DS-GVO Art. 2 Rn. 19.
[179] Kühling/Buchner/*Kühling/Raab*, Art. 2 Rn. 24.
[180] A.a.O.
[181] Vgl. Kapitel 5.3.
[182] EuGH EuZW 2015, 234.
[183] Paal/Pauly/*Ernst*, DS-GVO Art. 2 Rn. 18.

Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung. Ist ein Zugriff auf die im Fahrzeug stattfindenden Verarbeitungsprozesse ausgeschlossen, wäre der Autohersteller demnach nicht mehr als Verantwortlicher zu qualifizieren. Dies könnte beispielsweise der Fall sein, wenn lediglich die Software zur Verfügung gestellt wird, jedoch nach Übergabe des Autos an den Kunden keinerlei Zugriffsmöglichkeit auf die Daten mehr besteht. Denkbar wäre dies beispielsweise für Daten, die lediglich lokal benötigt werden, etwa aus dem Infotainment-System. Auch für Kartendaten sowie GPS-Informationen ist eine lediglich lokale Verarbeitung denkbar, allerdings dürfte sich mit Blick auf die zunehmende Vernetzung und die Anreicherung mit aktuellen Informationen wie etwa zur Verkehrslage, Verzögerungen durch Stau, Errechnung schnellerer Routen, etc., eine Vernetzung mit einem zentralen System des Autoherstellers erforderlich sein. In diesem Fall würde auch entsprechend eine Verantwortlichkeit des Autoherstellers bestehen.

Bezüglich Sensor- und Kameradaten kann zunächst die gleiche Frage aufgeworfen werden. Für das autonome Fahren ist primär eine rein lokale Verarbeitung erforderlich. Allerdings ist davon auszugehen, dass entsprechende Informationen in einer Art Black-Box gespeichert werden, um etwa im Falle eines Unfalles die Ursachen untersuchen zu können.[184] Die Speicherung ist jedoch ebenfalls vom Begriff der Verarbeitung erfasst.[185] Die Tatsache, dass Daten möglicherweise nicht vernetzt oder nur unter bestimmten Bedingungen abgerufen werden, kann der Verantwortlichkeit des Autoherstellers nicht entgegenstehen, wenn die Zweckbestimmung eine Zugriffsmöglichkeit prinzipiell vorsieht. Für Sensor- und Kameradaten dürfte der Autohersteller somit in der Regel ebenfalls Verantwortlicher sein, selbst wenn diese nur lokal verarbeitet werden.

Bei Kommunikationsdaten - inklusive Sensor- und Kameradaten, die mit anderen Systemen geteilt werden - ist zu hinterfragen, wie genau die Verwendung hier erfolgt. Werden diese Informationen ebenfalls nur lokal und außerhalb jeglicher Zugriffsmöglichkeit für den Autohersteller verarbeitet, scheidet eine Verantwortlichkeit aus. Dies ist jedoch im Kontext des vernetzten und autonomen Fahrens allenfalls in Einzelfällen denkbar, da es gerade auf die Vernetzung der Fahrzeuge untereinander und mit der Infrastruktur ankommt. Hier findet also entsprechend ein Datenaustausch statt. Die Übermittlung von Daten erfolgt durch Bekanntgabe gespeicherter oder durch Datenverarbeitung gewonnener Daten an einen Dritten.[186] Auch das Auslesen und Abfragen von Informationen ist als Verarbeitung i.S.d. Art. 4 Nr. 2 DS-GVO zu qualifizieren.[187] Bei der Kommunikation des Fahrzeugs mit anderen Fahrzeugen und Infrastruktur ist somit immer von einer Datenverarbeitung auszugehen. Wie bereits zuvor festgestellt wurde, hat der Fahrzeughalter bzw. -fahrer keinerlei Einflussmöglichkeit auf die Datenverarbeitung, er kann weder Zweck noch Mittel festlegen oder die Verarbeitung unterbinden. Die datenschutzrechtliche Verantwortlichkeit hierfür liegt folglich beim Autohersteller, denn diesem stehen jene Möglichkeiten zur Verfügung.

Zusammenfassend ist also davon auszugehen, dass in den allermeisten Fällen der Autohersteller als Verantwortlicher einzuordnen ist. Gegebenenfalls kann sich hier auch eine gemeinsame Verantwortung mit anderen Stellen ergeben, vgl. die nachfolgenden Kapitel.

---

[184] Wie beispielsweise im verunfallten Uber-Testfahrzeug, wo die Daten zur Auswertung der Unfallursache genutzt wurden, siehe https://www.ntsb.gov/investigations/AccidentReports/Reports/HWY18MH010-prelim.pdf.
[185] Kühling/Buchner/*Herbst*, Art. 4 Nr. 2 Rn. 24.
[186] Kühling/Buchner/*Herbst*, Art. 4 Nr. 2 Rn. 29 ff.
[187] Paal/Pauly/*Ernst*, DS-GVO Art. 4 Rn. 28.

5.1.3.1.3. BETREIBER VON INFRASTRUKTUR

Die Betreiber von Infrastruktur spielen neben den Autoherstellern eine der wichtigsten Rollen beim vernetzten und autonomen Fahren. Durch die Bereitstellung erforderlicher Infrastruktur wird erst das autonome Fahren ermöglicht - durch Vernetzung der Fahrzeuge untereinander und mit der Infrastruktur kann der Verkehrsfluss erheblich optimiert werden.

Ähnlich wie bei den Autoherstellern ist zu Beginn die Frage zu klären, ob eine Verarbeitung durch die Betreiber der Infrastruktur vorliegt. Die zuvor beschriebene Car-2-Infrastructure[188] ermöglicht die Kommunikation des Fahrzeugs mit Verkehrseinrichtungen (z.B. Ampeln oder Verkehrsschildern), um so eine Anpassung an die örtlichen Gegebenheiten zu gewährleisten. Ferner können so auch Gefahrenstellen oder andere Informationen übermittelt werden. Die Infrastruktur übernimmt somit eine steuernde Funktion, wobei Anweisungen an die Fahrzeuge übermittelt bzw. Informationen von den Fahrzeugen empfangen werden. Dabei kann auch ein Personenbezug entstehen.[189]

Da die Betreiber von Infrastruktur entsprechend ihrerseits personenbezogene Daten verarbeiten, ist zu klären, ob sie dabei auch Verantwortliche i.S.d. Art. 4 Nr. 7 DS-GVO sind. Es ist davon auszugehen, dass bei der Bereitstellung der Systeme diverse Einflussmöglichkeiten hinsichtlich der Verarbeitungszwecke und -mittel bestehen. Insbesondere dürften zwar mit Blick auf die diversen Schnittstellen zur Kommunikation Absprachen mit den Autoherstellern bestehen. Gleichwohl ist davon auszugehen, dass die Betreiber von Infrastruktur nicht einer Weisungsgebundenheit durch die Autohersteller unterliegen, die eine Auftragsverarbeitung nahelegen würde. Die telekommunikative Zwischenspeicherung, soweit akzessorisch zu Kommunikationsvorgängen, dürfte insofern nicht als Auftragsverarbeitung zu sehen sein.[190] Ein weiteres Indiz ist der Umstand, dass die Bereitstellung von Infrastruktur typischerweise eine öffentlich-rechtliche Aufgabe ist, während die Autohersteller allesamt der Privatwirtschaft angehörig sind. Selbst wenn für die Bereitstellung von Infrastruktur ein privates Unternehmen beliehen würde, ergibt sich vorliegend keine andere Konstellation, da die Datenverarbeitung immer noch primär durch die öffentlich-rechtlich geprägten Anforderungen bestimmt ist und nicht durch ein für eine Auftragsverarbeitung erforderliche Vereinbarung mit dem Autohersteller.

Auch umgekehrt lässt sich keine Auftragsverarbeitung des Betreibers von Infrastruktur zugunsten öffentlich-rechtlicher Einrichtungen annehmen: Zwar sind Faktoren wie die Verkehrsregeln fest vorgegeben, über die konkrete Ausgestaltung der Datenverarbeitung, die u.a. auch den Kommunikationsweg umfasst, könnte der Anbieter jedoch trotzdem selbst bestimmen. Somit steht ihm ein eigener Entscheidungsspielraum hinsichtlich der Zwecke und Mittel der Datenverarbeitung offen. Der Betreiber von Infrastruktur ist daher kein Auftragsverarbeiter, sondern selbst Verantwortlicher.

Eine Besonderheit ist jedoch, dass autonome und vernetzte Fahrzeuge ohne das Zusammenspiel mit der Infrastruktur nicht funktionieren würden. Eine enge und regelmäßige Kommunikation über die vorgesehenen Schnittstellen ist unerlässlich. Vor diesem Hintergrund scheint es denkbar, hier eine gemeinsame Verantwortlichkeit i.S.d. Art. 26 DS-GVO der Autohersteller - jedenfalls für Kommunikationsdaten - und der Betreiber von Infrastruktur anzunehmen. Um gemeinsame Verantwortliche zu sein, müssen zwei oder mehr Verantwortliche gemeinsam die Zwecke der und die Mittel zur Verarbeitung

[188] Vgl. Kapitel 2.2.6.
[189] Einfache Anweisungen wie etwa die zulässige Höchstgeschwindigkeit stellen als solche noch keinen Personenbezug her. Ebenfalls können Daten durch Aggregation anonymisiert werden, z.B. zur Verkehrslage. Für die Kommunikation und die dafür erforderliche Identifikation der Fahrzeuge im Netzwerk ist jedoch ein Personenbezug gegeben, vgl. Kapitel 3.3.
[190] BeckOK DatenschutzR/*Spoerr*, DS-GVO Art. 28 Rn. 49 m.w.N.

festlegen. Ein erstes Indiz hierfür ergibt sich aus dem Umstand, dass sich Autohersteller und Betreiber der Infrastruktur auf die Nutzung gemeinsamer Schnittstellen verständigt haben, um den Kommunikationsweg zu gewährleisten. Anzumerken ist jedoch, dass mittels Schnittstellen auch lediglich eine fremde Infrastruktur genutzt werden kann, ohne dass der Anbieter der Infrastruktur zwingend Einfluss auf die Mittel und Zwecke der Datenverarbeitung nehmen könnte.[191] Da die Infrastruktur jedoch - wie beschrieben - eine steuernde Funktion einnehmen soll, ist eine bloße Zurverfügungstellung der Infrastruktur im Sinne einer "Plattform" nicht gegeben. Letztlich wird die Frage, ob eine gemeinsame Verantwortlichkeit vorliegt, davon abhängen, wie autark die Systeme betrieben werden, wie weitreichend ein Datenaustausch stattfindet, und wie die Zugriffsrechte auf gesammelte Daten sowie die Verarbeitungsprozesse ausgestaltet sind.

Zuletzt ist anzumerken, dass gem. Art. 4 Nr. 7 DS-GVO die Zwecke und Mittel der Verarbeitung auch durch das Unionsrecht oder das Recht der Mitgliedstaaten vorgegeben werden kann, d.h. der Verantwortliche beziehungsweise die Kriterien für seine Benennung können nach dem Unionsrecht oder dem Recht der Mitgliedstaaten bestimmt werden. Wie bereits in Kapitel 4.3.1 ausgeführt, würde der Gesetzgeber sinnvollerweise die rechtlichen Rahmenbedingungen für die Nutzung vernetzter und autonomer Fahrzeuge sowie der dazugehörigen Infrastruktur schaffen. Mit Blick auf die durchaus schwierigen und vom Einzelfall abhängigen Abgrenzungsfragen scheint es naheliegend, von dieser Option Gebrauch zu machen und für rechtliche Klarheit zu sorgen.

5.1.3.1.4. SOFTWAREANBIETER

Neben der für das vernetzte und autonome Fahren erforderlichen Hardware - GPS, Sensoren, Kameras sowie Netzwerk- und Kommunikationstechnik - ist Software ein entscheidender Faktor für die Nutzung solcher Fahrzeuge. Jede Entscheidungsfindung durch das Fahrzeug basiert letztlich auf Software und der darin enthaltenen Algorithmen.[192] Die kontinuierliche Evaluation und Weiterentwicklung der Software ist somit von entscheidender Bedeutung. Software kann dabei einerseits von den Autoherstellern selber zur Verfügung gestellt, allerdings auch durch Drittanbieter bereitgestellt werden. Eine Integration von Fremdsoftware ist andererseits auch im Rahmen des Infotainment-Systems denkbar, und somit auch möglich, wenn sich die Anbieter von Hard- und Softwaresystemen unterscheiden, wobei der Hardwareanbieter lediglich die Plattform stellt, auf der der Softwareanbieter seine Programme betreibt. Das folgende Kapitel soll Konstellationen beschreiben, die nicht bereits durch die vorherigen Ausführungen abgedeckt sind, bezieht sich mithin also nicht auf Autohersteller oder die Betreiber von Infrastruktur.

Wie bereits zuvor ist auch bei den Softwareherstellern zunächst zu fragen, ob sie selbst (gemeinsam) Verantwortliche im Sinne der DS-GVO sind oder ob eine Auftragsverarbeitung vorliegt. Eine pauschale Antwort auf diese Frage ist jedoch nicht möglich; vielmehr kommt es darauf an, wie die Umsetzung im konkreten Fall erfolgt. Lagert beispielsweise ein Autohersteller die Bereitstellung bestimmter Software-Komponenten (z.B. die GPS-Koordination) an einen externen Softwareanbieter aus, hängt die Beurteilung maßgeblich davon ab, ob der Softwareanbieter rein weisungsgebunden arbeitet. Werden personenbezogene Daten streng nach den Vorgaben des Auftraggebers verarbeitet, ohne dass dem Softwareanbieter die Möglichkeit zustünde, selbst die Mittel oder Zwecke der Datenverarbeitung zu bestimmen, läge eine Auftragsverarbeitung vor. Hätte der Softwareanbieter hingegen die Möglichkeit, die Daten auch für eigene Zwecke zu verwenden, läge stattdessen eine Übermittlung vor, bei der der Softwareanbieter selbst zum Verantwortlichen würde.

[191] BeckOK DatenschutzR/*Spoerr*, DS-GVO Art. 26 Rn. 18.
[192] Zur rechtlichen Implikation solcher Algorithmen vgl. Kapitel 5.3.

Im Lichte des vernetzten und autonomen Fahrens lassen sich aus diesen Wertungen zumindest gewisse Grundtendenzen ableiten: Bedient sich etwa der Autohersteller externer Dienstleister, um Software für den unmittelbaren Fahrtbetrieb zu verwenden, dürften die Vorgaben über die Anforderungen an die Software wesentlich enger gesteckt sein als bei reinen Komfort-Funktionen. Hier hätte der Autohersteller nicht nur ein weitaus größeres Interesse an möglichst umfassenden Einfluss auf die Datenverarbeitung zu Zwecken der Qualitätskontrolle und -sicherung, auch mit Blick auf die Komplexität der Systeme ergibt sich diese Anforderung bereits aus technischer Sicht. Das IT-Outsourcing dürfte insofern in der Regel als Auftragsverarbeitung zu betrachten sein.[193]

Im Gegenzug können sich bei Komfort-Funktionen durchaus größere Freiheiten für den Softwareanbieter ergeben: Hier geht es gerade darum, das Infotainment-System mit zusätzlichen Angeboten zu erweitern und somit das Nutzungserlebnis zu verbessern. Die Einbindung bereits etablierter Dienste wie etwa Google Maps, Musik-Streaming Dienste wie Spotify, Deezer, o.ä., oder eine Anbindung an App-Stores kann dazu beitragen, den Komfort für den Kunden zu erhöhen. Gleichzeitig stellt das Fahrzeug hier lediglich die Plattform für die Verarbeitung; die eigentliche Datenverarbeitung erfolgt jedoch im Rahmen dieser Dienste. In dieser Konstellation läge die Verantwortlichkeit bei den Softwareanbietern.

Je nachdem, wie die Integration im Infotainment-System des Autoherstellers erfolgt, könnte in diesen Fällen auch eine gemeinsame Verantwortlichkeit in Betracht kommen. Letztlich unterstützt bzw. ermöglicht der Autohersteller hier die Datenverarbeitung durch Drittanbieter von Software erst, auch wenn auf den eigentlichen Verarbeitungsprozess möglicherweise keine oder nur eine geringe Möglichkeit der Einflussnahme angenommen werden kann.[194]

5.1.3.1.5. WERKSTÄTTEN

Anknüpfend an den Umstand, dass Software für das vernetzte und autonome Fahren eine zentrale Rolle einnimmt, ist auch die datenschutzrechtliche Einordnung von Werkstätten näher zu betrachten. Da Werkstätten in aller Regel Informationen über den Fahrer haben, ist ein Personenbezug hinsichtlich im Fahrzeug gespeicherter Daten vorhanden. Gleichzeitig fallen durch die zunehmende Nutzung von Software in Fahrzeugen immer mehr Daten an. Der freie Zugang von Werkstätten zu den Fahrzeugdaten eines Pkws ist zudem gewollt, um den Wettbewerbsmarkt für Autoreparaturen aufrecht zu erhalten.[195]

Im Gegensatz zu allen vorherigen Konstellationen werden Werkstätten im Allgemeinen aber keinen Einfluss auf die Datenverarbeitung als solche nehmen, sondern lediglich defekte Teile ersetzen. Der Zugriff auf Daten erfolgt auch letztlich nur zu Zwecken der Analyse, ohne dass weitere, eigene Zwecke ersichtlich wären. Ist die Verarbeitung personenbezogener Daten zu Analysezwecken erforderlich, dürfte sich eine Verarbeitung in aller Regel auf Art. 6 Abs. 1 lit. b) DS-GVO zur Erfüllung des Reparaturvertrages stützen lassen. Die Werkstätten wären dann selbst Verantwortliche i.S.d. Art. 4 Nr. 7 DS-GVO.

Die gleiche Wertung gilt für Wartungsverträge mit Vertrags-Werkstätten der Autohersteller, wenn etwa Software-Updates eingespielt werden oder sonst wie in einem größerem Umfang Zugriff auf Daten, z.B.

[193] BeckOK DatenschutzR/*Spoerr*, DS-GVO Art. 28 Rn. 49 m.w.N.
[194] Vgl. insofern die Ausführungen zur EuGH-Entscheidung zu Facebook-Fanseiten in Kapitel **Fehler! Verweisquelle konnte nicht gefunden werden.**.
[195] *Drexl:* Neue Regeln für die Europäische Datenwirtschaft?, NZKart 2017, 415, 416.

durch spezielle, den Autoherstellen vorbehaltene Zugänge, erfolgt, falls dieser zur Erfüllung einer Vertragspflicht erforderlich ist. Sofern Daten an die Autohersteller weitergegeben werden, könnte - je nach Ausgestaltung - auch eine gemeinsame Verantwortlichkeit in Betracht kommen.

Dies müsste jedoch im Einzelfall geprüft werden, etwa hinsichtlich der Frage, ob die Vertragswerkstatt rechtlich selbstständig oder Teil der Unternehmensgruppe des Autoherstellers ist, und in welchem Umfang die Vertragswerkstatt die Möglichkeit hätte, Zwecke und Mittel der Verarbeitung selbst festzulegen.

Zusammenfassend lässt sich also festhalten, dass Werkstätten in der Regel als eigene Verantwortliche einzuordnen sind. Bei Vertragswerkstätten könnte unter Umständen auch eine gemeinsame Verantwortlichkeit zusammen mit dem Autohersteller angenommen werden.

5.1.3.1.6. ARBEITGEBER

Auch für Arbeitgeber ergeben sich - primär wirtschaftliche - Interessen an den von vernetzten und autonomen Fahrzeugen erzeugten Daten. Denkbare Anwendungsfälle sind etwa das Tracking von Fahrzeugen, um Mitarbeiter zu kontrollieren und Verkehrsverstöße bzw. sonstiges Fehlverhalten zu erkennen. Aber auch für das Management des Fuhrparks kann die Verarbeitung von Daten aus vernetzten und autonomen Fahrzeugen relevant sein.

Das Beschäftigten-Datenschutzrecht ist in Deutschland in § 26 BDSG (2018) i.V.m. Art. 88 DS-GVO geregelt. Demnach können die Mitgliedstaaten durch Rechtsvorschriften spezifischere Vorschriften zur Gewährleistung des Schutzes der Rechte und Freiheiten hinsichtlich der Verarbeitung personenbezogener Beschäftigtendaten im Beschäftigungskontext als in der DS-GVO erlassen, insbesondere für Zwecke der Einstellung, der Erfüllung des Arbeitsvertrags einschließlich der Erfüllung von durch Rechtsvorschriften oder durch Kollektivvereinbarungen festgelegten Pflichten, des Managements, der Planung und der Organisation der Arbeit, der Gleichheit und Diversität am Arbeitsplatz, der Gesundheit und Sicherheit am Arbeitsplatz, des Schutzes des Eigentums der Arbeitgeber oder der Kunden sowie für Zwecke der Inanspruchnahme der mit der Beschäftigung zusammenhängenden individuellen oder kollektiven Rechte und Leistungen und für Zwecke der Beendigung des Beschäftigungsverhältnisses. Gem. § 26 Abs. 1 BDSG (2018) dürfen personenbezogene Daten von Beschäftigten für Zwecke des Beschäftigungsverhältnisses verarbeitet werden, wenn dies für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses oder nach Begründung des Beschäftigungsverhältnisses für dessen Durchführung oder Beendigung oder zur Ausübung oder Erfüllung der sich aus einem Gesetz oder einem Tarifvertrag, einer Betriebs- oder Dienstvereinbarung (Kollektivvereinbarung) ergebenden Rechte und Pflichten der Interessenvertretung der Beschäftigten erforderlich ist.

Das Gesetz sieht hier für die Verarbeitung personenbezogener Daten im Beschäftigtenkontext enge Zweckbestimmungen vor. Hinsichtlich des Trackings von Mitarbeitern ergeben sich damit nur eingeschränkte Anwendungsfälle. Mit Blick auf die datenschutzrechtliche Verantwortlichkeit des Arbeitgebers ergibt sich im Lichte dieser Zweckbestimmungen, dass der Arbeitgeber aber als eigener Verantwortlicher i.S.d. Art. 4 Nr. 7 DS-GVO einzustufen wäre, wenn die Systeme eines vernetzten und autonomen Fahrzeuges zum Tracking der Mitarbeiter genutzt würden.

5.1.3.1.7. MOBILITÄTS-DIENSTLEISTER

Letztlich können personenbezogene Daten auch durch Mobilitäts-Dienstleister verarbeitet werden. Hierzu zählt einerseits das Fuhrpark-Management, andererseits das Tracking von Fahrzeugen zur Qualitätssicherung oder - bei teilautonomen Fahrzeugen - Feststellung von Fehlverhalten.

In allen diesen Konstellationen würde eine Datenverarbeitung durch den Mobilitäts-Dienstleister erfolgen. Dabei würde der Anbieter sowohl die Mittel als auch die Zwecke der Verarbeitung selbst festlegen.

Eine gemeinsame Verantwortung mit anderen Stellen scheint dabei zunächst nicht in Frage zu kommen und könnte allenfalls bei sehr engen Kollaborationen, etwa zwischen einem Unternehmen, das den gesamten Fuhrpark an einen Mobilitäts-Dienstleister ausgelagert hat, in Frage kommen. Es mag auch denkbar erscheinen, dass die Bereitstellung einzelner Funktionen an IT-Dienstleister ausgelagert wird, allerdings läge hier allenfalls eine Auftragsverarbeitung vor, nicht jedoch eine Übermittlung bzw. gemeinsame Verantwortlichkeit. Insgesamt dürften Mobilitäts-Dienstleister daher stets als Verantwortliche im Sinne des Datenschutzrechts anzusehen sein, wobei die Wertung im Einzelfall abweichen kann.

5.1.3.2. RECHTSFOLGEN DER AUFTRAGSVERARBEITUNG

Wie im vorigen Kapitel dargelegt, gibt es Konstellationen, in denen eine Auftragsverarbeitung in Betracht kommt. In diesen Fällen braucht es für die Weitergabe an und Verarbeitung durch den Auftragnehmer keiner anderen Rechtsgrundlage als jene, auf die sich der Verantwortliche stützt.[196] Dabei sind jedoch verschiedene Anforderungen zu beachten, um die Rechtmäßigkeit der Auftragsverarbeitung zu gewährleisten.

Erfolgt eine Verarbeitung im Auftrag eines Verantwortlichen, so ist dieser gem. Art. 28 Abs. 1 DS-GVO gehalten, nur mit Auftragsverarbeitern zu arbeiten, die hinreichend Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen der DS-GVO erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet ist. Der Verantwortliche hat dementsprechend, ähnlich wie bereits Art. 17 Abs. 2 DSRL, eine Auswahlverantwortung.[197] Die Anforderungen, die sich aus Art. 24, 25 DS-GVO ergeben[198], werden dem Auftragsverarbeiter zwar nicht direkt, über die Anforderung nach Art. 28 Abs. 1 DS-GVO jedoch mittelbar aufgebunden.[199] Wenngleich keine explizite Überprüfungspflicht des Verantwortlichen in Art. 28 DS-GVO statuiert ist, ist davon auszugehen, dass die getroffene Formulierung ("arbeitet mit") sich nicht bloß auf die Auswahl bezieht, sondern auch auf die laufende Kollaboration.[200] Eine ununterbrochene Pflicht zur Überprüfung folgt jedoch auch nicht.[201] Die Einhaltung genehmigter Verhaltensregeln gem. Art. 40 DS-GVO oder eines genehmigten Zertifizierungsverfahrens gem. Art. 42 DS-GVO kann ausweislich Art. 28 Abs. 5 DS-GVO als geeignete Garantie angesehen werden. Ein Zertifizierungsverfahren nach Art. 42 DS-GVO würde sich für das vernetzte und autonome Verfahren durchaus anbieten, ist bislang jedoch noch nicht absehbar.

Ferner sind auch die Grundlagen der Auftragsverarbeitung in Art. 28 Abs. 3 DS-GVO näher beschrieben. Demnach ist zunächst ein Vertrag oder ein anderes Rechtsinstrument nach dem Unionsrecht oder dem Recht der Mitgliedstaaten erforderlich, der bzw. das den Auftragsverarbeiter in Bezug auf den Verantwortlichen bindet und in dem Gegenstand und Dauer der Verarbeitung, Art und Zweck der Verarbeitung, die Art der personenbezogenen Daten, die Kategorien betroffener Personen und die Pflichten und Rechte des Verantwortlichen festlegt. Insbesondere hätten die Mitgliedstaaten also die Möglichkeit, eine andere Gestaltungsform für die Rechtsbeziehungen zwischen Verantwortlichem und Auftragsverarbeiter vorzusehen.[202] Dies scheint im Anwendungsbereich des vernetzten und autonomen Fahrens und

[196] DSK, Kurzpapier Nr. 13, S. 2 (abrufbar unter https://www.lfd.niedersachsen.de/download/126580/DSK-Kurzpapier_Nr._13_-_Auftragsverarbeitung.pdf).
[197] Auernhammer/*Thomale*, DS-GVO Art. 28 Rn. 14.
[198] Vgl. Kapitel 5.6.
[199] Paal/Pauly/*Martini*, DS-GVO Art. 28 Rn. 20.
[200] Paal/Pauly/*Martini*, DS-GVO Art. 28 Rn. 21.
[201] BeckOK DatenschutzR/*Spoerr*, DS-GVO Art. 28 Rn. 35.
[202] Kühling/Buchner/*Hartung*, Art. 28 Rn. 110 ff.

der bereits zuvor aufgezeigten Unsicherheit bei der verbindlichen Einordnung involvierter Stellen durchaus sinnvoll.

Wird von dieser Öffnungsklausel kein Gebrauch gemacht, richten sich die Modalitäten in aller Regel jedoch nach einem Vertrag. Gem. Art. 28 Abs. 3 DS-GVO soll ein solcher Vertrag insbesondere vorsehen, dass der Auftragsverarbeiter

- die personenbezogenen Daten nur auf dokumentierte Weisung des Verantwortlichen – auch in Bezug auf die Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation – verarbeitet, sofern er nicht durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, hierzu verpflichtet ist; in einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet;
- gewährleistet, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen;
- alle gemäß Artikel 32 erforderlichen Maßnahmen ergreift;
- die in den Absätzen 2 und 4 genannten Bedingungen für die Inanspruchnahme der Dienste eines weiteren Auftragsverarbeiters als Unterauftragnehmer einhält;
- angesichts der Art der Verarbeitung den Verantwortlichen nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei unterstützt, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der in Kapitel III genannten Rechte der betroffenen Person nachzukommen;
- unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen den Verantwortlichen bei der Einhaltung der in den Artikeln 32 bis 36 genannten Pflichten unterstützt;
- nach Abschluss der Erbringung der Verarbeitungsleistungen alle personenbezogenen Daten nach Wahl des Verantwortlichen entweder löscht oder zurückgibt und die vorhandenen Kopien löscht, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht;
- dem Verantwortlichen alle erforderlichen Informationen zum Nachweis der Einhaltung der in diesem Artikel niedergelegten Pflichten zur Verfügung stellt und Überprüfungen – einschließlich Inspektionen –, die vom Verantwortlichen oder einem anderen von diesem beauftragten Prüfer durchgeführt werden, ermöglicht und dazu beiträgt.

Die Vertragsgestaltung muss hier also immer im Einzelfall erfolgen, sodass eine abstrakte Beurteilung im Kontext des vernetzten und autonomen Fahrens schwierig erscheint. Gleichwohl dürfte es möglich sein, auch in diesem Kontext standardisierte Vertragsklauseln und gängige Geschäftspraxen zu entwickeln, die eine rechtskonforme Ausgestaltung solcher Verträge vereinfachen.

Der Vertrag muss dabei schriftlich verfasst sein, was auch die elektronische Form umfasst, vgl. Art. 28 Abs. 9 DS-GVO. Nach deutschem Recht müsste demnach das Formerfordernis des § 126 oder § 126a BGB eingehalten werden.[203] Das Formerfordernis gilt jedoch nur für den Vertrag als solchen, nicht etwa für die Dokumentation von Weisungen.[204] Hier ist die Form lediglich hinsichtlich der Beweisfunktion

[203] BeckOK DatenschutzR/*Spoerr*, DS-GVO Art. 28 Rn. 103.
[204] Kühling/Buchner/*Hartung*, Art. 28 Rn. 99.

relevant. Beim vernetzten und autonomen Fahren ergibt sich hier jedoch keine spezifische Herausforderung.

Mit Blick auf die Vielzahl der verschiedenen Systeme, Komponenten und Software ist auch eine Unterbeauftragung im Anwendungsbereich des vernetzten und autonomen Verfahrens von Relevanz. Art. 28 Abs. 2 und 4 DS-GVO stellen diesbezüglich wiederum spezifische Anforderungen: Demnach darf der Auftragsverarbeiter keinen weiteren Auftragsverarbeiter ohne vorherige gesonderte oder allgemeine schriftliche Genehmigung des Verantwortlichen in Anspruch nehmen. Die Zustimmung kann dabei entweder gesondert, also speziell für den jeweiligen Unterauftrag, oder allgemein erfolgen.[205] Sie muss in beiden Konstellationen schriftlich erfolgen.[206] Die Schriftform könnte - mangels entsprechender Formulierung - strenger auszulegen sein als in Art. 28 Abs. 9 DS-GVO, um insbesondere dem Risiko einer allgemeinen Zustimmung gesondert Rechnung zu tragen.[207] Auch dies dürfte jedoch weitestgehend unproblematisch sein und lediglich bei kurzfristig erforderlichen Weisungen zu relevanten Verzögerungen führen.

Darüber hinaus verpflichtet Art. 28 Abs. 4 DS-GVO den Auftragsverarbeiter, die Dienste eines weiteren Auftragsverarbeiters nur dann in Anspruch zu nehmen, um bestimmte Verarbeitungstätigkeiten im Namen des Verantwortlichen auszuführen, wenn diesem weiteren Auftragsverarbeiter dieselben Datenschutzpflichten auferlegt werden, die in dem Vertrag (mit den zuvor genannten Anforderungen) oder anderen Rechtsinstrument zwischen dem Verantwortlichen und dem Auftragsverarbeiter festgelegt sind. Demnach muss auch der Unterauftragnehmer geeignete Garantien dafür bieten, dass die Verarbeitung entsprechend den Anforderungen der DS-GVO genügt. Auch hier kann als Nachweis die Einhaltung genehmigter Verhaltensregeln (Art. 28 Abs. 5, Art. 40 DS-GVO) oder eines genehmigten Zertifizierungsverfahrens (Art. 28 Abs. 5, Art. 42 DS-GVO) herangezogen werden.[208] Entsprechende Verfahren durch die Mitgliedstaaten oder Aufsichtsbehörden wären dementsprechend für das vernetzte und autonome Fahren wünschenswert.

Eine weitere Möglichkeit, die Nutzung von Auftragsverarbeitung beim vernetzten und autonomen Fahren zu erleichtern, könnte in der Bereitstellung von Standardvertragsklauseln i.S.d. Art. 28 Abs. 6 DS-GVO bestehen. Demnach kann die Kommission im Einklang mit dem Prüfverfahren gem. Art. 93 Abs. 2 DS-GVO sowie eine Aufsichtsbehörde im Einklang mit dem Kohärenzverfahren gem. Art. 63 Standardvertragsklauseln zur Regelung der Auftragsverarbeitung oder einer Unterbeauftragung i.S.d. Art. 28 Abs. 3 und 4 DS-GVO festlegen.

Werden Daten an einen Auftragsverarbeiter in einem Drittland übermittelt, sind ferner die Art. 44 ff. DS-GVO zu berücksichtigen.

Zusammenfassend lässt sich festhalten, dass sich in einem komplexen Umfeld wie dem vernetzten und autonomen Fahren auch komplexe Situationen für eine Auftragsverarbeitung entstehen können. Die Nutzung von Verfahren zur Standardisierung, wie etwa Standard-Vertragsklauseln, genehmigte Verhaltensregeln oder Zertifizierungsverfahren, sowie die Möglichkeit, durch anderweitige Rechtsinstrumente eine Zuordnung zu treffen, ist dabei ein sinnvoller Weg, um die Transparenz zu erhöhen und eine datenschutzrechtlich konforme Umsetzung des vernetzten und autonomen Fahrens zu gewährleisten.

[205] Ehmann/Selmayr/*Bertermann*, Art. 28 Rn. 22.
[206] Auernhammer/*Thomale*, Art. 28 Rn. 34.
[207] Paal/Pauly/*Martini*, DS-GVO Art. 28 Rn. 62., so auch BeckOK DatenschutzR/*Spoerr*, DS-GVO Art. 28 Rn. 39.
[208] BeckOK DatenschutzR/*Spoerr*, DS-GVO Art. 28 Rn. 43.

5.1.3.3. RECHTSFOLGEN BEI GEMEINSAMER VERANTWORTLICHKEIT

Sind mehrere gemeinsam für eine Datenverarbeitung verantwortlich, sind die Rechtsfolgen des Art. 26 DS-GVO zu beachten. Gem. Art. 26 Abs. 1 S. 2 DS-GVO legen die Verantwortlichen in einer Vereinbarung in transparenter Form fest, wer von ihnen welche Verpflichtung gem. der DS-GVO erfüllt, insbesondere was die Wahrnehmung der Rechte der betroffenen Person angeht, und wer welchen Informationspflichten gem. den Art. 13 und 14 DS-GVO nachkommt. Die Pflicht, in transparenter Form eine Vereinbarung zu treffen, ist dabei keine Voraussetzung für die gemeinsame Verantwortlichkeit, sondern eine Rechtsfolge, die mit einer Geldbuße bewährt sein kann.[209] Dies verdeutlicht einmal mehr die Notwendigkeit, beim vernetzten und autonomen Fahren für hinreichende Rechtsklarheit zu sorgen, damit die Verantwortlichen entsprechende Maßnahmen einleiten können.

Inhaltlich soll die Vereinbarung dazu dienen, Klarheit darüber zu schaffen, welche datenschutzrechtlichen Pflichten von wem zu erfüllen sind.[210] Die Verantwortungsverteilung kann jedoch nicht zur Entbehrlichkeit allgemeiner Anforderungen an die Rechtmäßigkeit der Datenerhebung führen, es ist trotz dessen eine Ermächtigungsgrundlage erforderlich.[211] Die datenschutzrechtlichen Pflichten, die mittels Vereinbarung i.S.d. Art. 26 DS-GVO zugewiesen werden können, können neben der Wahrnehmung der Betroffenenrechte z.B. auch eine Anlaufstelle für den Betroffenen beinhalten (Art. 26 Abs. 1 S. 3 DS-GVO), die Zuständigkeit für die jeweiligen technischen Abläufe festlegen, oder auch Klarheit bezüglich der Implementierung technischer und organisatorischer Maßnahmen (Art. 32 DS-GVO) schaffen. Die Einzelheiten, die jeweils in einer entsprechenden Vereinbarung aufgenommen werden sollten, hängen vom Einzelfall ab und müssten im Bereich des vernetzten und autonomen Fahrens jeweils geprüft werden. Sinnvoll erscheinen sicherlich Regelungen hinsichtlich der IT-Sicherheit sowie der Wahrnehmung der Betroffenenrechte, da Betroffene gerade bei vernetzten Systemen sonst vor der Herausforderung stünden, zunächst die zuständige Stelle identifizieren zu müssen, was im Ergebnis nicht ohne größere Schwierigkeiten möglich sein dürfte. Gleichzeitig ließen sich ohne eine Vereinbarung nur schwerlich entsprechende Verfahren durch die Verantwortlichen etablieren, die eine Wahrnehmung der Betroffenenrechte gewährleisten würden.

Die Anforderung an die Transparenz ist dabei umstritten: In Ansehung von Erwägungsgrund 58 muss die Information „präzise, leicht zugänglich und verständlich sowie in klarer und einfacher Sprache verfasst sein. Zwar gelte der Erwägungsgrund primär für die Transparenznorm des Art. 12 Abs. 1 S. 1 DS-GVO, er wirke aber auch auf die Auslegung des Begriffes der Transparenz in Art. 26 Abs. 1 S. 2 maßstabsbildend ein.[212] Nach anderer Auffassung seien im Lichte der Transparenzbestimmungen zugunsten Betroffener deutlich höhere Anforderungen der Allgemeinverständlichkeit anzunehmen, während bei Art. 26 Abs. 1 S. 2 DS-GVO Transparenz im Sinne der Eindeutigkeit und Nachvollziehbarkeit, aber nicht der Alltagsverständlichkeit zu verstehen sei, die Anforderung also nicht so zu verstehen sei, dass auch eine durchschnittliche Person in der Lage sein muss, eine entsprechende Vereinbarung zu verstehen.[213] Diese Auffassung schient im Ergebnis - insbesondere im Licht des vernetzten und autonomen Fahrens - vorzugswürdig. In der Praxis können sich sehr komplexe Konstellationen ergeben, die eine genaue Auseinandersetzung mit der Thematik erfordern, um eine ausgewogene Verteilung der jeweiligen datenschutzrechtlichen Pflichten zu gewährleisten. Eine in diesem Maße detaillierte Regelung kann nur noch schwerlich für einen durchschnittlichen Anwender transparent sein. Zudem sieht Art. 26 Abs. 2 S. 2 DS-GVO vor, dass lediglich *das Wesentliche* der Vereinbarung dem Betroffenen zur Verfügung gestellt werden soll. Eine Zurverfügungstellung der gesamten Vereinbarung ist also gerade

[209] Paal/Pauly/*Martini*, DS-GVO Art. 26 Rn. 22.
[210] BeckOK DatenschutzR/*Spoerr*, DS-GVO Art. 26 Rn. 30.
[211] Kühling/Buchner/*Hartung*, Art. 26 Rn. 27.
[212] Plath/*Plath*, Art. 26 Rn. 5; Gola/*Piltz*, Art. 26 Rn. 12; Paal/Pauly/*Martini*, DS-GVO Art. 26 Rn. 24 f;
[213] BeckOK DatenschutzR/*Spoerr*, DS-GVO Art. 26 Rn. 29.

nicht erforderlich und - mit Blick auf möglicherweise ersichtliche Geschäftsgeheimnisse - auch nicht zielführend. Somit ist der Betroffene vom Adressatenkreis des Art. 26 Abs. 1 DS-GVO ausgeklammert. Es überzeugt daher nicht, die Verantwortlichen zu verpflichten, auch ihren Vertragstext in ausschließlich transparenter Sprache zu halten.

Wie auch bereits bei der Auftragsverarbeitung hat der Gesetzgeber die Möglichkeit, die jeweiligen Aufgaben der Verantwortlichen durch Rechtsvorschriften der Union oder der Mitgliedstaaten, denen die Verantwortlichen unterliegen, festzulegen. Die vertragliche Dispositionsfreiheit wird durch diese Regelung entsprechend eingeschränkt. Mit der Möglichkeit, die Aufgaben der Verantwortlichen zu regeln, hat der Gesetzgeber insofern einen erheblichen Gestaltungsspielraum. Grundsätzlich überwiegen im Kontext des vernetzten und autonomen Fahrens die Vorteile solcher gesetzgeberischen Vorgaben: Durch das erforderliche Ineinandergreifen der verschiedenen Systeme und den hohen Grad der Vernetzung ist eine gemeinsame Verantwortlichkeit in durchaus einigen Anwendungsbereichen denkbar. Gleichzeitig ermöglicht die Architektur der Systeme zum vernetzten und autonomen Fahren eine hinreichend präzise Identifikation der einschlägigen Anwendungsfälle. Wenngleich es im Einzelfall zu Abweichungen kommen kann, ist jedenfalls die Vernetzung größerer Systeme wie etwa die Infrastruktur und die Fahrzeuge gut auf einem abstrakteren Level abbildbar. Dementsprechend wären gesetzgeberische Vorgaben in diesem Bereich wünschenswert, um für Rechtssicherheit für die involvierten Verantwortlichen einerseits, aber auch für eine Wahrung der Rechte der Betroffenen andererseits, zu sorgen. Allerdings ist zu bedenken, dass das vernetzte und autonome Fahren im Endeffekt ein länderübergreifender Sachverhalt ist. Dementsprechend ist eine Harmonisierung umso wichtiger. Eine Nutzung der Gestaltungsspielräume durch Mitgliedstaaten könnte eine Implementierung des vernetzten und autonomen Fahrens deutlich erschweren. Eine gesetzgeberische Lösung auf europäischer Ebene, etwa im Rahmen einer Verordnung, wäre daher wünschenswert.

5.1.3.4. RECHTSFOLGEN BEI ÜBERMITTLUNG

Werden personenbezogene Daten von einen Verantwortlichen an einen Dritten bekanntgegeben, ohne dass diese gemeinsame Verantwortliche sind, findet eine Verarbeitung im Sinne einer Übermittlung statt, vgl. Art. 4 Nr. 2 DS-GVO.[214]

Für diese Übermittlung ist zunächst eine Rechtsgrundlage erforderlich. Hier kommen die Tatbestände des Art. 6 Abs. 1 DS-GVO in Betracht: Eine Einwilligung (lit. a)), zur Erfüllung eines Vertrages oder vorvertraglicher Maßnahmen (lit. b)), aufgrund einer rechtlichen Verpflichtung (lit. c)), zum Schutz lebens-wichtiger Interessen (lit. d)), zur Wahrnehmung einer Aufgabe im öffentlichen Interesse (lit. e)) oder wenn ein berechtigtes Interesse vorliegt und die schutzwürdigen Interessen des Betroffenen gegen die Datenverarbeitung nicht überwiegen (lit. f)). Wie bereits in Kapitel 4.3.1 beschrieben, sind vor allem die Rechtsgrundlagen von besonderer Relevanz, die auf die Wahrung öffentlicher Interessen, eine rechtliche Verpflichtung, oder auf ein berechtigtes Interesse seitens des Verantwortlichen abstellen.

Ist eine Rechtsgrundlage für die Übermittlung personenbezogener Daten an Dritte vorhanden, ist ferner Art. 14 DS-GVO zu beachten. Der Empfänger der Daten muss demnach den Betroffenen informieren, wenn er die Informationen nicht direkt beim Betroffenen erhoben hat.[215] Eine Einschränkung kann sich allenfalls ergeben, wenn der Betroffene bereits bei der ursprünglichen Erhebung unterrichtet wurde und insofern bereits über die (unveränderten) Informationen verfügt, weswegen die Informationspflicht gem. Art. 14 Abs. 5 lit. a) DS-GVO ausscheiden würde. Damit ließe sich die Problematik, den Betroffenen

[214] BeckOK DatenschutzR/*Schild*, DS-GVO Art. 4 Rn. 49.
[215] Der Umfang der Informationspflichten wurde bereits in Kapitel 0 erläutert.

auch in einem komplexen System wie einem vernetzten und autonomen Fahrzeug mitsamt der dazugehörigen Infrastruktur zeitnah zu unterrichten, jedenfalls etwas entschärfen.

Werden die Daten durch den Dritten für einen anderen als den ursprünglichen Zweck verarbeitet, ist der Betroffene hierüber ebenfalls zu informieren, Art. 14 Abs.4 DS-GVO. Dabei ist jedoch zu berücksichtigten, dass der neue Verarbeitungszweck gem. Art. 5 Abs. 1 lit. b) DS-GVO mit dem ursprünglichen Zweck kompatibel sein muss. Die Risiken einer schleichenden Ausweitung der Zweckbestimmung (sog. "function creep") ist in Kapitel 5.5 weiter ausgeführt.

Die Übermittlung stellt, verglichen mit gemeinsamer Verantwortlichkeit und Auftragsverarbeitung mangels des Erfordernisses einer Vereinbarung oder eines Vertrages, die geringsten formellen Anforderungen an eine Datenweitergabe. Gleichzeitig sind der Grundsatz der Zweckbindung und die Tatsache, dass für die Übermittlung eine Rechtsgrundlage vorhanden sein muss, limitierende Faktoren. Hinsichtlich der Modularität der verschiedenen Systeme, die beim vernetzten und autonomen Fahren zum Einsatz kommen, scheint es jedoch denkbar, dass jedenfalls der Gesetzgeber die rechtliche Basis für eine Übermittlung schaffen kann.

5.2. RECHTSGRUNDLAGEN UND GRUNDSÄTZE DER VERARBEITUNG

5.2.1.1. EINORDNUNG DER STELLEN

Anknüpfend an die bereits zuvor skizzierten relevanten Stellen ergibt sich die folgende rechtliche Einordnung:

5.2.2. RECHTSGRUNDLAGE DER VERARBEITUNG

Einer der zentralen Grundsätze des Datenschutzrechts ist das Verbot der Verarbeitung mit Erlaubnisvorbehalt, in der DS-GVO wiedergegeben durch Art. 5 Abs. 1 lit. a) DS-GVO und der Verpflichtung, dass die personenbezogenen Daten auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Art und Weise verarbeitet werden müssen. Somit wird für jeden Verarbeitungsvorgang eine Rechtsgrundlage benötigt. In der DS-GVO werden die Rechtsgrundlagen zur Datenverarbeitung in Art. 6 Abs. 1 DS-GVO geregelt und ermöglichen die Verarbeitung nach verschiedenen Alternativen. Die zentralen Grundlagen bilden in Reihenfolge der wesentlichen Prozesse: die Verarbeitung zur Erfüllung eines Vertrages (lit. b)), das berechtigte Interesse des Datenverarbeiters (lit. f)) und die Einwilligung (lit. a)).[216] Nur wenn eine rechtliche Grundlage vorliegt, dürfen personenbezogene Daten also überhaupt verarbeitet werden (das „Ob“ der Verarbeitung). Jeder Verarbeitungsvorgang unterliegt jedoch immer auch weiteren gesetzlichen Anforderungen (das „Wie“ der Verarbeitung).[217]

5.2.2.1. ERFÜLLUNG VON VERTRAGSZWECKEN GEMÄß ART. 6 ABS. 1 LIT. B) DS-GVO

Eine Datenverarbeitung ist rechtmäßig gem. Art. 6 Abs. 1 lit. b) DS-GVO, wenn die Datenverarbeitung zur Erfüllung eines Vertrages erforderlich ist. Damit besteht zwar eine gesetzliche Grundlage zur Ver-

[216] Vgl. bereits Kapitel 5.3.2.
[217] Vgl. dazu auch BeckOK DatenschutzR/*Albers/Veit*, DS-GVO Art. 6 Rn. 1.

arbeitung, aber diese stützt sich auf das Bestehen oder die Anbahnung eines privatrechtlichen Vertrages. Diese Norm stellt damit für den regulären Geschäftsverkehr (nicht-öffentlicher Stellen) eine sehr wichtige Rechtsgrundlage dar um Verträge überhaupt erfüllen zu können.

Hiernach dürfen alle Vertragsdaten verarbeitet werden, soweit dies für den Vertragszweck erforderlich ist. Eine andere Wertung wäre widersprüchlich, insbesondere mit Blick auf die Privatautonomie von Verträgen. Hier lässt sich, ähnlich der Einwilligung, der Betroffene freiwillig auf eine Beziehung mit dem Verantwortlichen ein und es ist in seinem Interesse, dass der Verantwortliche die erforderlichen Daten verarbeiten darf, um im Gegenzug seine vertraglich geschuldete Leistung zu erbringen. Der weite Begriff der Erfüllung des Vertrages lässt darauf schließen, dass auch Rücksichts- und Nebenpflichten erfasst sind.[218] Grundsätzlich nicht möglich ist es, vertraglich den Verkauf bzw. die Übermittlung von Daten Dritter als Vertragsgegenstand zu benennen, da diese auch schon nicht Vertragspartei sind.[219] Damit ist nicht nur ein „bloßer Bezug" zum Vertrag notwendig, sondern die Verarbeitung der Daten der Vertragsparteien muss erforderlich sein, um den Vertrag zu erfüllen.[220] Eine Verarbeitung von personenbezogenen Daten Dritter muss somit durch eine gesonderte Rechtsgrundlage gerechtfertigt werden.

- Vertragsschluss

Zu Beginn der Verarbeitung von personenbezogenen Daten im automatisierten und vernetzten Fahrzeug steht in der Regel ein Kaufvertrag, in dem sich Verkäufer und Käufer, der in diesem Zusammenhang zugleich die betroffene Person ist, über den Eigentumsübergang des Fahrzeuges an den Käufer einigen. Neben dem Verpflichtungsgeschäft muss der Gegenstand sich für eine gewöhnliche Verwendung eignen, die bei Sachen der gleichen Art üblich ist und der Käufer der Art der Sache nach erwarten kann.[221] Der Grund für einen Fahrzeugerwerb liegt (gewöhnlich) erstmal in der Nutzung als Fortbewegungsmittel. Dieses beinhaltet zu aller erst die mechanische Funktionsfähigkeit des Fahrzeuges, u.a. des Antriebs oder der Lenkung. Auch hier verarbeiten bereits Sensoren unterschiedliche Daten um allgemein Funktionalitäten zu bedienen, z.B. die Tankstandsanzeige, Reifendruck und ähnliche einfache Sensordaten. Der Verkäufer verarbeitet daher zu Beginn nur die notwendigen Vertragsdaten, welche insbesondere die Kontaktdaten des Vertragspartners beinhalten aber auch die Details des verkauften Fahrzeuges, in der Regel inklusive der Fahrzeugidentifikationsnummer und dem Kennzeichen. Um einen Vertrag schließen zu können, muss dieser die essentialia negotii enthalten. Dazu gehören die Namen und Kontakte der Vertragspartner sowie die Beschreibung und der Umfang der vertraglichen Leistungen bzw. des Kaufgegenstandes. Diese Daten müssen verarbeitet werden um den Vertrag abwickeln zu können und sind somit erforderlich im Sinne der Vorschrift. Diese Daten sind die Mindestbestandteile eines Vertrages und Verträge könnten ohne diese Daten somit nicht geschlossen werden. Ein Verbot der Verarbeitung dieser Daten würde dem Sinn und Zweck der Vorschrift zuwiderlaufen und auch den wirtschaftlichen Verkehr erheblich einschränken. Diese Verarbeitungsvorgänge können daher auf der Grundlage des Artikels 6 Abs. 1 lit. b) DS-GVO durchgeführt werden.[222]

- Zusatzleistungen als Teil des Vertrages

Möglicherweise sind aber als Teil des Vertrages auch die besonderen Fahrzeugausstattungen eingeschlossen. Dazu muss unterschieden werden, ob der Vertrag mit dem Händler auch diese Funktionen umfasst oder ob ein separater Vertrag mit dem Hersteller geschlossen wird. Die Regel wird wohl sein,

[218] Vgl. BeckOK DatenschutzR/*Albers/Veit*, DS-GVO Art. 6 Rn. 31.
[219] Paal/Pauly/*Frenzel*, DS-GVO Art. 6 Rn. 14.
[220] Paal/Pauly/*Frenzel*, DS-GVO Art. 6 Rn. 14; ähnlich: BeckOK DatenschutzR/*Wolff*, BDSG § 28 Rn. 33 ff.
[221] § 434 BGB.
[222] Vgl. Auch Roßnagel, SVR 2014, 281, 281.

dass ein separater Vertrag geschlossen wird, entweder digital im Fahrzeug oder schriftlich mit dem Verkäufer vor Ort als Stellvertreter bzw. als Bote des Herstellers. Der dortige Vertragspartner wird dann Verantwortlicher sein.[223] Im Ergebnis kommt es somit auf den Vertrag und seinen Inhalt an und ob die dort vereinbarten Leistungen erforderlich sind oder eine Einwilligung notwendig ist.

Zu diesen Funktionalitäten gehören alle Systeme, die das vernetzte und automatisierte Fahren im Ergebnis ausmachen. Hier sind zuerst die Fahrassistenzsysteme zu nennen. Dazu werden Sensordaten verarbeitet, die bereits die Umgebung analysieren und darauf basierend Aktionen durchführen. Dieses können Radarsystem für ACC Funktionalitäten sein, Rückfahrkamera oder auch Spurhalteassistenten und ähnliche unterstützende Systeme. Hinzu kommen außerdem Navigationssysteme die Standortdaten erheben und verarbeiten. Umso mehr die Fahrzeuge mit autonomen Fahrleistungen verkauft werden, desto mehr ist die Verarbeitung von Daten notwendig, bis alle oben besprochenen Daten in den Systemen verarbeitet werden.[224]

Sofern bestimmte Eigenschaften und Funktionalitäten des Fahrzeuges Teil des Vertrags sind, könnten diese auch auf der Rechtsgrundlage zur Erfüllung der Vertragszwecke verarbeitet. Sind die Daten erforderlich um die Funktionalitäten, die durch den Kunden zusammen mit dem Fahrzeug erworben wurden, sachgerecht nutzen zu können könnte hier somit Art. 6 Abs. 1 lit. b) DS-GVO im Verhältnis zum entsprechenden Vertragspartner einschlägig sein. Sofern eine Datenverarbeitung nicht stattfindet und die Funktionalitäten demnach nicht genutzt werden können, wäre die Sache mangelhaft und eine Erfüllung des Vertrages nicht möglich. Die Verarbeitung personenbezogener Daten könnte somit erforderlich und nach Art. 6 Abs. 1 lit. b) DS-GVO rechtmäßig sein.

Diese Datenverarbeitungsvorgänge zum Betrieb der Funktionalitäten könnten, ergänzend zu den eigentlichen Vertragsdokumenten, durch Leistungsbeschreibungen, die den Vertragsgegenstand konkretisieren und den Umfang beschreiben, oder Allgemeine Geschäftsbedingungen (AGB) in den Vertragsschluss mit einbezogen werden. Fraglich ist inwiefern Vereinbarungen über Datenverarbeitungsvorgänge in den Leistungsbeschreibungen und Allgemeinen Geschäftsbedingungen Teil des Vertrages werden und ob diese dann auch über Art. 6 Abs. 1 lit. b) DS-GVO gerechtfertigt sind oder ob die dortigen Verarbeitungsvorgänge gesondert über die Einwilligung gem. Art. 6 Abs. 1 lit. a DS-GVO gerechtfertigt sind. Diese für eine Vielzahl von Verträgen vorformulierten Bestimmungen werden gem. § 305 BGB ein Bestandteil des Vertrages. Um die Vertragsbedingungen zu erfüllen, könnten somit die dort genannten Datenverarbeitungsvorgänge gerechtfertigt sein. Werden Datenverarbeitungen über die AGB in den Vertrag einbezogen, kann der Anwendungsbereich der Rechtsgrundlage aus Art. 6 Abs. 1 lit. b) DS-GVO erheblich erweitert werden ohne die Restriktionen beachten zu müssen, die sich für vergleichbare Verarbeitungsvorgänge auf Basis einer Einwilligung ergeben. Die Fahrzeughersteller könnten somit umfangreiche Datenverarbeitungsvorgänge und Übermittlungen in die AGB mit aufnehmen, sodass Telematik-Protokolldaten, Fernanalysedaten, Wartungshistorie und sonstige Fahrzeugdaten an den Hersteller oder Dritte übermittelt und dort weiterverarbeitet werden könnten.[225] Nimmt man an, dass die Erforderlichkeit der Verarbeitung alle Aspekte des Vertrages umfasst und damit einer weiten Auslegung der

[223] Vgl. auch Kap. 6.1.

[224] S. Kap. 3 und 4.

[225] Z.B. der Fahrzeughersteller Tesla beschreibt in seinen AGB (https://www.tesla.com/de_DE/order/download-order-agreement?country=DE) sehr abstrakt, dass das Fahrzeug des Nutzers Telematikdaten an Tesla übermittelt um Funktionsüberprüfungen oder Updates durchführen zu können und das Tesla das Fahrzeug außerdem orten kann. In der Datenschutzerklärung (https://www.tesla.com/de_DE/about/legal#privacy-statement) wird genauer beschrieben, welche Datenverarbeitungsvorgänge in einem Tesla Fahrzeug vorgenommen werden (zuletzt besucht am 20.08.2018).

Vorschrift folgt, kann sich der Betroffene immer noch auf die Vorschriften der AGB-Kontrolle aus den §§ 306 ff. BGB und dem Grundsatz nach Treu und Glauben gem. § 242 BGB sowie einer möglichen Sittenwidrigkeit berufen.[226] Unwirksam könnten solche Regelungen sein, da sie gegen den Grundsatz der Transparenz aus Art. 5 Abs. 1 lit. a) DS-GVO verstoßen aber auch gem. § 307 Abs. 1, 2 Nr. 1 BGB den Betroffenen unangemessen benachteiligen.[227] Wird die Vorschrift des Art. 6 Abs. 1 lit. b) DS-GVO dagegen restriktiv ausgelegt und nimmt man an, dass der Sinn und Zweck der Vorschrift vor allem auf die primären Vertragszwecke gerichtet ist und nur die dafür erforderliche Datenverarbeitung von der Rechtsgrundlage gerechtfertigt wird, stellen die relevanten Stellen der AGB einwilligungsbedürftige Einigungen dar. Die Erlaubnis für die Verarbeitungsvorgänge in den AGB können somit nur unter den Auflagen des Art. 7 DS-GVO eingeholt werden und hier ist insbesondere das Koppelungsverbot aus Art. 7 Abs. 4 DS-GVO zu beachten.[228]

Ohne explizit eine ganz restriktive Auslegung dieser Vorschrift zu folgen, dürften die geschilderten Sachverhalt im Ergebnis an der Erforderlichkeit scheitern. Eines der tragenden Argumente hierfür dürfte sein, dass die Funktionalitäten auch nutzbar sind, wenn die Daten lediglich im lokalen Fahrzeugspeicher verarbeitet werden und keine Übermittlung an den Vertragspartner erfolgt.[229] Die nur für die aktuelle Fahrsituation erforderlichen Daten könnten direkt nach Abschluss des Fahrvorgangs gelöscht werden und so der Eingriff auf ein Minimum reduziert werden, sofern man hier von einem Eingriff sprechen mag, da das Datenschutzrecht wie ob erwähnt wohl nicht anwendbar ist.

- Sonstige Verträge

Die Vertragsschlüsse mit dem Händler und dem Hersteller werden anhand der Vielfalt der Funktionen nicht die einzigen bleiben. Vielmehr können die Daten des Fahrzeuges auch durch Werkstätten verarbeitet werden um Reparaturleistungen sachgerecht erbringen zu können oder weitere Vertragsschlüsse mit Partnern um das Infotainment-System optimal zu nutzen.

Auch um Garantieleistungen des ursprünglichen Vertrags in Anspruch zu nehmen, müssen zur Abwicklung, neben den Fahrzeugdaten zur Reparatur, die Vertragsdaten zur Bearbeitung des Garantiefalls verarbeitet werden. Das ist notwendig um den Anspruch auf Garantie, der sich aus dem Vertrag ergibt, zu verifizieren. Das Auslesen der Daten erfolgt dann auf Basis des Werkvertrages mit der Werkstatt und ist somit erforderlich, um die Reparaturleistungen sachgerecht durchführen zu können. Die Zustands- bzw. Sachdaten aus dem Fahrzeugspeicher werden hier in Zusammenhang mit dem Reparaturauftrag also den Daten des Auftraggebers und den Fahrzeugdaten, insbesondere der Fahrzeugidentifikationsnummer, gebracht. Offen bleibt ob diese Daten dann wiederrum durch die Werkstatt an den Hersteller übermittelt werden. Der Anspruch aus dem Vertrag müsste hierzu wiederrum wohl aber auf die erforderlichen Daten zur Bearbeitung des Garantieanspruches und zur Begleichung der entstandenen Kosten beschränkt werden.

5.2.2.2. BERECHTIGTES INTERESSE GEMÄß ART. 6 ABS. 1 LIT. F) DS-GVO

Art. 6 Abs. 1 lit. f) DS-GVO regelt die Zulässigkeit der Verarbeitung von personenbezogenen Daten, wenn dieses zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich ist. Das berechtigte Interesse des Verantwortlichen muss dazu mit den entgegenstehenden

[226] Vgl. zu diesem Ansatz: *Engeler*, ZD 2018, 55.
[227] Vgl. dazu auch *Wendehorst/v. Westphalen*, NJW 2016, 3745
[228] Vgl. *Golland*, MMR 2018, 130.
[229] Vgl. *Wendt*, ZD-Aktuell 2018, 06034.

schutzwürdigen Belangen des Betroffenen abgewogen werden. Somit ist eine Datenverarbeitung hier nur untersagt, wenn die Belange des Betroffenen, hier des Fahrzeugführers bzw. Halters, die Interessen des jeweiligen Gegenübers (Hersteller, Verkäufer, Werkstatt, etc.) überwiegen.

Das berechtigte Interesse des Verantwortlichen ist nicht legaldefiniert. Das berechtigte Interesse müsse, unter Berücksichtigung der Umstände der Datenerhebung, vernünftigerweise für die betroffene Person abzusehen sein.[230] Ausgangspunkt jeder Beurteilung ist somit der konkrete Zweck der jeweiligen Datenverarbeitung. Liegt der Zweck der Verarbeitung außerhalb eines vorhersehbaren Bereiches, überwiegen die Rechte und Freiheiten des Betroffenen regelmäßig und eine Verarbeitung ist unzulässig.[231] Sonst sei das berechtigte Interesse aber eher weit zu verstehen und müsse vernünftigerweise auch schutzwürdig sein[232], davon umfasst ist beispielsweise auch das Interesse des Verantwortlichen an Direktwerbung.[233] Die berechtigten Interessen umfassen somit jede vernünftige Erwägung, soweit sie konkrete Zwecke verfolgen, worin grundsätzlich auch wirtschaftliche und ideelle Interessen enthalten sind.[234] Werden die Datenverarbeitungen somit auf das berechtigte Interesse gestützt, muss der Verantwortliche zur Rechtssicherheit dafür sorgen, dass die beschriebenen Interessen dem Betroffenen zugänglich sind, also einsehbar aber auch verständlich und nachvollziehbar. Die Interessen müssen dann gegen die Interessen des durch die Datenverarbeitung Betroffenen abgewogen werden. Die durch die Verarbeitung aufkommenden Risiken müssen für den Betroffenen abschätzbar und nachvollziehbar sein und sich außerdem im Rahmen der Rechtsordnung rechtfertigen lassen.

Die Bereitstellung eines vernetzten und autonomen Fahrzeuges eröffnet dem Hersteller neben den üblichen Rechten und Pflichten mehr Möglichkeiten (und Pflichten) zur Datenerhebung. So ist beispielsweise die Erhebung von Sensor- und Kameradaten erforderlich, um den Betrieb des Fahrzeugs zu gewährleisten. Bei der Nutzung von Kamerabildern können auch personenbezogene Daten Dritter verarbeitet werden, weshalb eine Rechtsgrundlage zur Datenerarbeitung erforderlich wäre. Zudem existieren neue und bessere Möglichkeiten, um die Produkte instand zu halten und zu verbessern. Die übermittelten Daten können durch den Verantwortlichen, z.B. dem Hersteller, umfangreich analysiert werden; auf diese Weise kann die Performance und das Verhalten von Fahrzeugen in bestimmten Situationen nachvollzogen werden. Die Ergebnisse können in zukünftige Produktionen oder durch Updates von aktuellen Fahrzeugsystemen einfließen und auf diese Weise die durch den Hersteller beabsichtigten Ziele unterstützen.

Das berechtigte Interesse des Herstellers besteht somit in der Analyse von Leistungsdaten der Fahrzeuge zur Verbesserung der Qualität und Sicherheit dieser autonomen und vernetzten Fahrzeuge. Dazu sind insbesondere technische bzw. Sachdaten erforderlich um den Zustand des Fahrzeuges zu analysieren (Abnutzung, Fehlerquellen und/oder -häufigkeit) und somit Verbindungen von Fehlern zu einer möglichen spezifischen Nutzung des Fahrzeugs herzustellen. Folglich ist es für den Hersteller nicht nur erforderlich die Sachdaten zu analysieren, sondern es muss auch das konkrete Fahrverhalten berücksichtigt werden, um die Verbindung herstellen zu können. Hier ist somit das Verhalten der Fahrer in den verarbeiteten Daten enthalten und erforderlich um die Rückschlüsse zu den Fehlern zu finden. Diese

[230] Vgl. Erwägungsgrund 47.
[231] Erwägungsgrund 47, S. 4.
[232] Erwägungsgrund 47; Paal/Pauly/*Frenzel*, DS-GVO Art. 6 Rn. 28.
[233] Erwägungsgrund 47 S. 7.
[234] BeckOK DatenschutzR/*Albers/Veit* DS-GVO Art. 6 Rn. 45; ähnlich Ehmann/Selmayr/*Heberlein*, Art. 6 Rn. 22 - der aber das berechtigte Interesse ablehnt nur weil es für den Verarbeiter einen reinen „Nutzen“ hat die Daten zu verarbeiten.

Verarbeitung und die damit zusammenhängende Profilbildung, soweit man das im Zusammenhang mit dem Fahrverhalten annimmt, könnten einen intensiven Eingriff in die Rechte des Betroffenen darstellen.

Fraglich ist aber, ob die Daten auch personenbezogen verarbeitet werden müssen. Um die Eingriffsintensität zu verringern, können die Verantwortlichen die erhobenen Daten auch weiter pseudonymisieren, indem die Verbindungen zu den Klardaten ganz aus den Datensätzen gelöscht werden, oder sogar anonymisieren, indem generische Verhaltensgruppen erstellt werden und die Fahrdaten sowie die entsprechenden technischen Daten jeweils zugeordnet werden. Auch hier ließe sich dann ein Zusammenhang zwischen Fahrweise und typischen Fehlern herstellen und der Zweck erreichen. Dieses wäre somit die angemessene Lösung um Daten zu Qualitätssicherungs- und Produktbeobachtungszwecken zu verarbeiten.

Im Ergebnis kann es somit Datenverarbeitungen geben, die für den Verantwortlichen derart relevant sind, dass es ein berechtigtes Interesse darstellt. Da aber die Interessen immer mit den Interessen des Betroffenen abgewogen werden müssen, ist es erforderlich diese genau gegeneinander abzuwägen und zu untersuchen, ob es nicht alternative Verarbeitungsmöglichkeiten gäbe, die den Eingriff verringern, so wie hier dargestellt durch Pseudonymisierung oder Anonymisierung.

5.2.2.3. EINWILLIGUNG GEMÄß ART. 6 ABS. 1 LIT. A) DS-GVO

Artikel 6 DS-GVO nennt zunächst die Einwilligung, die als Willenserklärung dem Betroffenen eine autonome Entscheidung über die Verwendung seiner Daten ermöglicht.[235] In Art. 4 Nr. 11 DS-GVO wird die Einwilligung als jede „von der betroffenen Person freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist“ definiert. Die Einwilligung kann gemäß dem Wortlaut dabei für einen oder mehrere bestimmte Zwecke erteilt werden.

Eine Einwilligung soll auf der freien Entscheidung des Betroffenen beruhen und daher „freiwillig“ erfolgen, weshalb kein Zwang bestehen darf und damit die Möglichkeit vorhanden sein muss, eine echte Wahl treffen zu können.[236] Muss der Betroffene in einer weitergehende Erhebung oder Verarbeitung der Daten, also in mehr Daten oder Verarbeitungsvorgänge als erforderlich, einwilligen um eine bestimmte Leistung in Anspruch nehmen zu können, liegt das Erfordernis der Freiwilligkeit mithin nicht vor (sog. Koppelungsverbot).[237] Dies wird im nicht-öffentlichen Bereich vor allem bei einer marktbeherrschenden Stellung eines Unternehmens diskutiert, da hier auch alternative Anwendungen fehlen. Die Einwilligung muss sich darüber hinaus stets auf einen bestimmten, d.h. konkreten Fall und Zweck beziehen und darf daher keinen pauschalen Charakter haben.[238] Überdies muss die Einwilligung in Kenntnis der Sachlage des Betroffenen, d.h. informiert erfolgen. Die Einwilligungserklärung muss daher verständlich formuliert und vollständig mit Blick auf den intendierten Verarbeitungsvorgang sein. [239] Um eine wirksame Einwilligung einzuholen, muss diese unmissverständlich abgegeben worden sein; auf eine Erklärung in Schriftform oder ausnahmsweise auch elektronische Form besteht der Gesetzgeber

[235] BeckOK DatenschutzR/*Albers/Veit*, DS-GVO Art. 6 Rn. 19
[236] Paal/Pauly/*Ernst*, DS-GVO Art. 4 Rn. 69.
[237] *Dammann*, ZD 2016, 307, 311; Ehmann/Selmayr/*Heckmann*/*Paschke*, DS-GVO Art. 7 Rn. 94.
[238] Paal/Pauly/*Ernst*, DS-GVO Art. 4 Rn. 78.
[239] Paal/Pauly/*Ernst*, DS-GVO Art. 4 Rn. 81.

nicht. Vielmehr lässt er nun auch „eindeutig bestätigende“ und damit auch konkludente Handlungen als Einwilligungserklärung genügen[240], wobei die Erklärung nachweisbar sein muss.[241]

Schließlich nennt Art. 7 DS-GVO darüber hinaus Bedingungen zur Wirksamkeit der Einwilligung:

> 1. Der Verantwortliche ist beweisbelastet für das Vorliegen einer wirksamen Einwilligung;
> 2. Schriftliche Einwilligungserklärungen, die jedenfalls noch andere Sachverhalte betreffen, müssen in verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache und unterscheidbar vom übrigen Inhalt verfasst sein;
> 3. Einwilligungen sind jederzeit widerruflich; darauf ist gesondert hinzuweisen.
> 4. Bei der Beurteilung der Freiwilligkeit der Einwilligung ist im größtmöglichen Umfang zu berücksichtigen, ob die Erfüllung eines Vertrags von der Einwilligung zu einer Verarbeitung von personenbezogenen Daten abhängig ist, die für die Erfüllung des Vertrags nicht erforderlich sind.

Alle Funktionalitäten, die über die primären Zwecke[242] hinausgehen, könnten damit einwilligungspflichtig sein. Ausgenommen hiervon sind natürlich die Verarbeitungsprozesse, die bereits durch eine der Rechtsgrundlagen zuvor umfasst sind.[243] Neben den oben genannten Kriterien muss jeder einzelne Betroffene explizit in die entsprechende Datenverarbeitung einwilligen. Im Kontext des vernetzten und autonomen Fahrens kann die Einwilligung auf unterschiedliche Art und Weise eingeholt werden. Der Nachteil für den Betroffenen dabei ist, dass dieser sich wohl grundsätzlich gegenüber dem Verantwortlichen grundsätzlichen identifizieren muss.[244] Diese Identifikation wird grundsätzlich durch die Speicherung der IP-Adresse ergänzt, sodass fraglich ist ob z.B. Fake-Profile oder ähnliche Bemühungen zur Verschleierung der wahren Identität zielführend sind. Zumindest bei Rechtsansprüchen, welche im Rahmen der Einwilligung der Nachweis der jeweiligen Einwilligung sein könnte, könnte anhand der IP-Adresse ein konkreter Personenbezug hergestellt werden.[245]

Die Einwilligung kann über den Vertrag bei Kauf des Fahrzeuges in Schriftform eingeholt werden. Der Autohändler würde dann als Vertreter bzw. Vermittler des Herstellers bzw. eigentlichen Vertragspartners auftreten. Schon die Komplexität der Beteiligten lässt diese Alternative aber unpraktikabel erscheinen. Zweckmäßiger erscheint es, die Einwilligung über das Multimedia-Interface direkt im Fahrzeug einzuholen. Hierbei ist jedoch zu beachten, dass der Platz begrenzt ist und die Informationen, die dem Betroffenen für eine informierte Einwilligung zur Verfügung gestellt werden müssen, umfangreich sind.

[240] Vgl. Erwägungsgrund 32 S. 2 DS-GVO "[…] die betroffene Person in dem jeweiligen Kontext eindeutig ihr Einverständnis […] signalisiert.".
[241] So in Erwägungsgrund 42 S. 1 DS-GVO.
[242] S. Kap. 5.3.2.
[243] Vgl. Ausführlich zu dieser Thematik und Kritik an Einwilligungslösungen: *Engeler*, ZD 2018, 55.
[244] In Ausnahmefällen könnte auch die Anmeldung und Einwilligung unter einer Fake-Mail-Adresse oder einem sonstigen Pseudonym erfolgen.
[245] Vgl. Kap. 4.

Bei der Umsetzung werden zurzeit verschiedene Modelle diskutiert[246]: die gestufte Einwilligung[247], mittels Ampelsystem[248], standardisierte Symbole[249] oder durch eine erleichterte Lesbarkeit mittels einseitiger Erklärungen (sog. One-Pager)[250].

Inwiefern diese Ansätze zweckmäßig sind, wird sich in Zukunft zeigen. Erforderlich ist jedoch die Information der Betroffenen nach den Voraussetzungen der Art. 12 ff. DS-GVO. Ob diese durch alle Ansätze gewährt werden können ist zweifelhaft, da insbesondere einseitige Erklärungen auf wesentliche Bestimmungen verzichten müssten oder Piktogramme nicht ausreichend Aussagekraft haben.[251] Der Verantwortliche wird ein Interesse daran haben müssen, die Einwilligung bestmöglich einzuholen, Mängel im Verfahren werden ihm angelastet und er ist zudem in der Beweispflicht.[252]

5.2.2.4. ERFÜLLUNG VON RECHTLICHEN VERPFLICHTUNGEN GEM. ART. 6 ABS. 1 LIT. C) DS-GVO

Eine Datenverarbeitung kann außerdem gerechtfertigt sein, wenn sie dazu dient, eine rechtliche Verpflichtung zu erfüllen. Um die Verarbeitung gem. Art. 6 Abs. 1 lit. c) DS-GVO zu legitimieren, muss die rechtliche Verpflichtung auf eine materiell-rechtlichen Grundlage beruhen.[253] Damit wird die Datenverarbeitung zu einer Verpflichtung kraft objektiven Rechts.[254] So wird den nationalgesetzlich normierten Auskunfts- und Informationsansprüchen des einzelnen Mitgliedstaates und seiner Einrichtungen Rechnung getragen. Die Rechtsgrundlage aus Art. 6 Abs. 1 lit. c) DS-GVO stellt daher indirekt eine Öffnungsklausel dar.[255] Die Union gem. Art. 6 Abs. 3 lit. a) DS-GVO und die Mitgliedsstaaten gem. Art. 6 Abs. 3 lit. b) DS-GVO[256] können entsprechende weiterführende Rechtsgrundlagen schaffen.[257] Das „Ob“ der Verarbeitung bestimmt sich dann nach der jeweiligen spezifizierten Rechtsgrundlage, während das „Wie“ der Verarbeitung weiterhin nach der DS-GVO im Rahmen der Öffnungsklausel[258] von Art. 6 Abs. 2 DS-GVO ausgestaltet werden muss. Weitere materiell-rechtliche Vorgaben zur Gestaltung der Rechtsgrundlagen finden sich zudem in Art. 6 Abs. 3 S. 2 DS-GVO.

Mit der seit April 2018 gültigen E-Call-Verordnung (VO (EU) 2015/758) ist der Hersteller zudem verpflichtet, Fahrzeuge, die nach diesem Datum hergestellt werden, mit entsprechender Netzwerktechnik

[246] S. auch Stiftung Datenschutz, Neue Wege bei der Einwilligung im Datenschutz – technische, rechtliche und ökonomische Herausforderungen (Studie), 2017.
[247] Vgl. Art.-29-WP, Guidelines on Consent under Regulation 2016/679 (WP 259).
[248] Vgl. *Radlanski*, Das Konzept der Einwilligung in der datenschutzrechtlichen Realität, 198.
[249] Vgl. u.a. Art. 12 Abs. 7 DS-GVO; Kühling/Buchner/*Bäcker*, Art. 12 Rn. 20.
[250] Vgl. BMJV, „One-Pager“ – Muster für transparente Datenschutzhinweise, https://www.bmjv.de/DE/Themen/FokusThemen/OnePager/OnePager_node.html (zuletzt aufgerufen 20.08.2018).
[251] Kritisch: *Veil*, NVwZ 2018, 686, 688.
[252] Ehmann/Selmayr/*Heckmann*/*Paschke*, Art. 7 Rn. 72.
[253] Paal/Pauly/*Frenzel*, DS-GVO Art. 6 Rn. 18
[254] BeckOK DatenschutzR/*Albers*/*Veit*, DS-GVO Art. 6 Rn. 34.
[255] Siehe ErwG 45: „Erfolgt die Verarbeitung durch den Verantwortlichen aufgrund einer ihm obliegenden rechtlichen Verpflichtung oder ist die Verarbeitung zur Wahrnehmung einer Aufgabe im öffentlichen Interesse oder in Ausübung öffentlicher Gewalt erforderlich, muss hierfür eine Grundlage im Unionsrecht oder im Recht eines Mitgliedstaats bestehen.“
[256] S. bereits Kapitel 5.2: In Deutschland können die Rechtsgrundlagen durch Bund, Länder und Kommunen geschaffen werden.
[257] So auch Paal/Pauly/*Frenzel*, DS-GVO Art. 6 Rn. 36.
[258] „Die Mitgliedsstaaten können spezifischere Bestimmungen zur Anpassung der Anwendung dieser Verordnung [...] beibehalten oder einführen...“

auszurüsten und die dort genannten Daten zu übermitteln. Das e-Call System soll im Falle eines Unfalles automatisch Kontakt zu den 112-Notruf-Behörden aufnehmen und den Unfall melden. Gleichzeitig muss ein Mindestdatensatz an die Behörden übertragen werden, der aus Angaben zur Unfallzeit, zu den aktuellen Koordinaten, der Fahrtrichtung, Fahrzeug-ID und Service Provider ID besteht. Außerdem können weitere Daten aus dem On-Board-Speicher übertragen werden, zu denen die Anzahl der Insassen gehören kann oder auch weitere für den Unfall relevante Daten wie Informationen über angelegte Sicherheitsgurte oder ob sich das Fahrzeug überschlagen hat.

Anfang 2017 wurde außerdem das StVG novelliert.[259] Mit dieser Anpassung soll das automatisierte Fahren ermöglicht und gefördert werden. Durch diese Vorschriften ist das hoch- und vollautomatisierte Fahren rechtmäßig, solange der Fahrzeugführer in der Lage ist, die Kontrolle zu übernehmen.[260] In § 63 a StVG werden Vorgaben zum Datenschutz im vernetzten und automatisierten Auto gemacht und so bestimmte Datenverarbeitungsprozesse gesetzlich vorgeschrieben. Danach müssen die durch das GPS ermittelten Positions- und Zeitangaben gespeichert werden. Davon umfasst soll auch der Zeitpunkt sein, an dem der Fahrer die Kontrolle über das Fahrzeug übernommen oder an das System wieder abgegeben hat. Zusätzlich soll dokumentiert werden, wann das Fahrzeug den Fahrer dazu aufgefordert hat, wieder die Kontrolle zu übernehmen. Hierdurch sollen Unfälle und andere Schadensereignisse sowie Fehler nachgewiesen werden. Diese Beweise können dann auch in Gerichtsverfahren verwandt werden.[261] Hierdurch soll die Beweisbarkeit von Ereignissen erleichtert werden, also Unfallhergänge oder andere Fehlfunktionen nachvollzogen werden können.[262] Vorgaben über Speicherart oder -ort werden nicht gemacht, könnten aber durch eine Rechtsverordnung präzisiert werden.[263] Um diese Vorgabe umzusetzen wird eine Art Blackbox diskutiert, ähnlich dem System im Flugzeug. Der dann sog. „Event Data Recorder“ sei im vernetzten und automatisierten Fahrzeug zu installieren und soll nach einem Unfall durch eine zuständige Stelle geborgen und ausgelesen werden. Alternativ dazu wäre eine Speicherung in einem System des Herstellers möglich. Kommuniziert das Fahrzeug regelmäßig mit den Servern des Herstellers und überträgt Daten, wäre eine Speicherung der in § 63 a StVG genannten Daten auch dort möglich.[264] In § 63a Abs. 3 StVG ist zudem geregelt, dass die Daten an Dritte übermittelt werden müssen, wenn Rechtsansprüche bestehen. Unklar ist wer der Inhaber des Anspruches und damit Empfänger dieser Daten dann sein soll. In Abs. 2, wonach Behörden einen Anspruch auf die Daten haben, wird ein konkreter Empfänger adressiert. Außerdem ist nach Abs. 3 der Fahrzeughalter verantwortlich, dass die Daten an den Berechtigten übermittelt werden. Allerdings sollen nur die Daten übermittelt werden, die für die Zwecke des Anspruchs erforderlich sind.[265]

5.3. KAMERAAUFNAHMEN UND VIDEOÜBERWACHUNG

Die Nutzung von Kameras in Fahrzeugen ist - aus datenschutzrechtlicher Sicht - nicht erst im Bereich des vernetzten und autonomen Fahrens relevant, sondern wurde auch mit Blick auf die Verfügbarkeit sog. "Dashcams" vielfach diskutiert. Diese Ausführungen sind jedoch möglicherweise auch auf das ver-

[259] BT-Drs. 18/11776.
[260] S. Definition und Ausführungen in § 1 a StVG.
[261] Vgl. RAW 2014, 157; *Schonschek*, Datenschutz-Praxis 08/2015, S. 12.
[262] So auch Schlanstein, NZV 2016, 201, 202.
[263] S. § 63 b StVG.
[264] Vgl. Ausführlich und kritisch: *Wendt*, ZD-Aktuell 2018, 06034.
[265] § 63 Abs. 2 Satz 3, § 63 Abs. 2 Nr. 2 StVG.

netzte und autonome Fahren übertragbar. Dashcams sind kleine Kameras, die im Bereich der Windschutzscheibe angebracht sind und das Verkehrsgeschehen filmen; die Aufnahmen sollen dabei der Beweissicherung dienen und dem Fahrer eine bessere Rechtsverfolgung ermöglichen.[266] Aus datenschutzrechtlicher Sicht ist die Nutzung von Dashcams kritisch zu betrachten: Die Aufzeichnung des öffentlichen Raumes durch Dashcams wurde weithin als Verstoß gegen die Verbotsnorm des § 6b BDSG (alt) angesehen.[267] Die Auffassung, dass datenschutzrechtliche Interessen nicht zu einer kategorischen Vorenthaltung sachgerechter technischer Hilfsmittel zur effektiven Rechtsverfolgung gegenüber dem Bürger nicht sachdienlich sei[268], überzeugt nicht.[269] Die Rechtswidrigkeit der allgemeinen, anlasslosen Aufzeichnung des Straßenverkehrs durch Dashcams wurde zwischenzeitlich auch vom BGH bestätigt.[270] Trotz der Rechtswidrigkeit der Erhebung wurden die Dashcam Aufnahmen im Zivilprozess bestätigt.[271] Auch die Verwertbarkeit als Beweismittel im Straf- und Ordnungswidrigkeitsverfahren wird durch die Rechtsprechung angenommen[272]; gleichwohl ist die Verwertbarkeit umstritten.[273]

Wenngleich im Rahmen der Dashcam Urteile zwar die datenschutzrechtliche Bewertung bei der Nutzung von Kameras im Fahrzeug geprüft wurde, können die Wertungen trotzdem nicht ohne Weiteres auf das vernetzte und autonome Fahren übertragen werden. Einerseits wurde § 6b BDSG (alt) inzwischen durch die DS-GVO sowie das BDSG (2018) abgelöst[274], andererseits ist auch der Einsatzzweck ein anderer: Die im Smart Car integrierten Kameras sind aus technischer Sicht für den Betrieb des Fahrzeuges erforderlich und dienen nicht primär der Beweissicherung.[275] Auch hat der Fahrer nicht ohne Weiteres Zugriff auf diese Daten. Somit unterscheidet sich auch der Kreis der Zugriffsberechtigten. Insofern muss die datenschutzrechtliche Zulässigkeit der Nutzung von Kameraaufnahmen im Lichte des vernetzten und autonomen Fahrens geprüft werden.

Als Rechtsgrundlage kommt hier zunächst Art. 6 Abs. 1 lit. f) DS-GVO in Betracht. Demnach ist die Verarbeitung personenbezogener Daten zulässig, wenn der Verantwortliche hieran ein berechtigtes Interesse hat und die Interessen des Betroffenen nicht überwiegen.[276] Die Verarbeitung von (auch) personenbezogenen Daten, die über die Kamerasysteme in einem Smart Car erfasst werden, ist vorliegend für den Betrieb der Fahrzeuge erforderlich. Die Hersteller haben insofern ein gewichtiges Interesse an der Nutzung dieser Daten. Demgegenüber sind jedoch mit Blick auf den Umstand, dass die Kameras den öffentlichen Verkehrsbereich erfassen, massenhafte Eingriffe in die Persönlichkeitsrechte betroffener Passanten die Folge. Dem ist jedoch entgegen zu halten, dass eine Videoüberwachung auch in öffentlichen Verkehrsmitteln stattfindet, was ebenfalls einen solchen massenhaften Eingriff zur Folge

[266] Vgl. etwa *Heermann*, Erstmals Dash-Cam-Aufzeichnung als Beweismittel im Strafverfahren zugelassen, ZD-Aktuell 2015, 07425.
[267] *Niehaus*, Verwertbarkeit von Dashcam-Aufzeichnungen im Straf- und Ordnungswidrigkeitenverfahren, NZV 2016, 551, m.w.N.
[268] Anders etwa das AG Nienburg, ZD 2015, 341.
[269] *Niehaus*, Verwertbarkeit von Dashcam-Aufzeichnungen im Straf- und Ordnungswidrigkeitenverfahren, NZV 2016, 551.
[270] BGH, Urteil vom 15.05.2018 - VI ZR 233/17.
[271] A.a.O.
[272] AG Nienburg, DAR 2015, 280; OLG Stuttgart, NJW 2016, 2280.
[273] *Niehaus*, Verwertbarkeit von Dashcam-Aufzeichnungen im Straf- und Ordnungswidrigkeitenverfahren, NZV 2016, 551, 556.
[274] Die Videoüberwachung ist hier in § 4 BDSG (2018) geregelt.
[275] Gleichwohl können auch Daten, durch den Autohersteller und nicht den Fahrer erhoben wurden, einem Gericht zugänglich gemacht werden, vgl. etwa https://netzpolitik.org/2016/bmw-speichert-keine-standortdaten-gibt-aber-bewegungsprofil-an-gericht/
[276] Vgl. Kapitel 5.2.2.2.

hat und grundsätzlich zulässig ist. Auch nimmt die DS-GVO berechtigte Interessen für die Verarbeitung von personenbezogenen Daten an, die für die Gewährleistung der Netz- und Informationssicherheit unbedingt notwendig und verhältnismäßig sind.[277] Diese Wertung ließe sich auch auf das vernetzte und autonome Fahren übertragen: Die Nutzung von Kamerasystemen und die dabei anfallenden personenbezogenen Daten dienen der Vermeidung von Unfällen, was zwar nicht unmittelbar für die IT-Sicherheit relevant ist, vielmehr aber für die körperliche Unversehrtheit der Betroffenen. Wenn bereits die IT-Sicherheit als berechtigtes Interesse gilt, dann muss dies umso mehr für die körperliche Unversehrtheit von Verkehrsteilnehmern gelten. Ferner sieht Art. 35 Abs. 3 lit. c) DS-GVO für den Fall, dass eine systematische umfangreiche Überwachung öffentlicher Bereiche erfolgt, eine Datenschutz-Folgenabschätzung vor. Dies gilt insbesondere mittels optoelektronischer Vorrichtungen.[278] Ein pauschales Verbot für die Nutzung von Kamerasystemen im öffentlichen Bereich kann daher nicht angenommen werden. Vielmehr kommt es auf eine differenzierte Ausgestaltung bei der Umsetzung an.[279] Eine Interessenabwägung würde hier also im Ergebnis zugunsten der Autohersteller ausfallen, die eine Verarbeitung grundsätzlich auf Art. 6 Abs. 1 lit. f) DS-GVO stützen könnten.

Allerdings erfordert der Grundsatz der Verhältnismäßigkeit und der Umstand, dass eine Datenschutz-Folgenabschätzung erforderlich ist[280], dass die negativen Folgen aus der Datenverarbeitung so weit wie möglich abgemildert werden müssten. Denkbar ist hier insbesondere eine Beschränkung des Zugriffs auf die Kameraaufnahmen: Diese sollten nicht nur nach Ablauf einer bestimmten Dauer überschrieben werden, ein Zugriff sollte auch nur im Einzelfall möglich sein. Hier wäre zunächst zu überlegen, zu welchen Zwecken ein Zugriff zulässig sein sollte. Mit Blick auf die zuvor genannten Sicherheitsinteressen scheiden einfache Tatbestände wie etwa Ordnungswidrigkeiten oder andere Verkehrsverstöße aus, da es hier bereits an einem berechtigten Interesse mangelt. Bei einer Nutzung ausschließlich zur Aufklärung von Unfallursachen ist ein kurzes Zeitfenster für eine Zwischenspeicherung ausreichend. Aktuelle Ansätze verwenden ein Zeitfenster von maximal 20 Sekunden, wobei im Falle eines Unfalls die Dauer der Aufnahme erhöht werden kann.[281] Die Aufnahmen werden dann solange überschrieben, bis durch die im Fahrzeug verbauten Sensoren ein Unfall erkannt wird. Nur dann erfolgt eine länger währende Speicherung der Daten. Eine ähnliche Wertung gilt auch beim "event data recording"[282], wobei § 63a Abs. 4 StVG eine Mindestspeicherdauer von 6 Monaten und eine Maximalspeicherdauer von 3 Jahren vorsieht. Gleichwohl ist anzumerken, dass eine so lange Speicherung für Kameraaufnahmen nicht erforderlich sein dürfte, da diese, im Gegensatz zu sonstigen Fahrzeugdaten, jedenfalls nicht für statistische Berechnungen oder sonstige Erhebungen geeignet sein dürften. Darüber hinaus ergibt sich hier durch die Tatsache, dass nicht nur Fahrzeugdaten, sondern auch die Persönlichkeitsrechte Dritter betroffen sind, bereits eine andere Wertung.

Um Missbrauch zu vermeiden, könnte hierbei auch eine "trusted third party" eingebunden werden, die den Zugriff auf die Daten erst genehmigen muss, bevor der Autohersteller Zugriff erlangt. Dies könnte beispielsweise durch eine Verschlüsselung der Daten geschehen, wenn der Entschlüsselungsschlüssel dort hinterlegt wäre. Letztlich ist die Eingriffsintensität weitaus höher zu beurteilen, wenn tatsächlich Menschen Zugriff auf die Daten haben, als in einer Konstellation, wo die Daten zwar autonom vom

[277] Erwägungsgrund 49.
[278] Erwägungsgrund 91, Satz 3.
[279] Paal/Pauly/*Frenzel*, DS-GVO Art. 6 Rn. 31.
[280] S. auch Kapitel 4.3.9.
[281] *Mienert/Gipp*: Dashcam, Blockchain und der Beweis im Prozess, ZD 2017, 514, 518.
[282] Vgl. Kapitel 5.2.2.4.

Fahrzeug erhoben und dort gespeichert werden, einem menschlichen Zugriff ohne weitere Zwischenschritte jedoch entzogen sind.

Vertreten wird auch, dass ein manipulationssicherer Zeitstempel zur Erhöhung der Beweiskraft von Dashcam-Aufnahmen erforderlich ist.[283] Das Manipulationsrisiko dürfte zwar deutlich geringer ausfallen, wenn Aufnahmen nicht durch eine Dashcam des Fahrers, sondern durch die im Fahrzeug verbauten Systeme erstellt werden, da diese Aufnahmen grundsätzlich nur dem Hersteller zur Verfügung stehen. Gleichwohl wäre die Implementierung einer entsprechenden Technologie auch nicht schädlich.

Eine weitere Folge aus der Anwendung von Art. 6 Abs. 1 lit. f) DS-GVO als Rechtsgrundlage wäre, dass Betroffene ein Widerspruchsrecht geltend machen könnten, Art. 21 DS-GVO. Die Verarbeitung wäre dann einzustellen, sofern der Verantwortliche keine zwingenden schutzwürdigen Gründe für die Verarbeitung nachweisen kann oder sie der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen dienen.[284] Gerade letzteres dürfte bei einer Verwertung nur nach Verkehrsunfällen jedoch in der Regel einschlägig sein.

Nicht davon erfasst ist aber das Zeitfenster von 20 bis 30 Sekunden, in dem die Aufnahmen jeweils zwischengespeichert und dann überschrieben werden. Allerdings dürfte sich hier das Widerspruchsrecht in der Praxis nicht auswirken: Bevor Betroffene die Möglichkeit hätten, einer konkreten Verarbeitung zu widersprechen, wären die Daten bereits wieder gelöscht.

Fraglich ist allerdings, welcher Zeitpunkt für den Widerspruch gem. Art. 21 DS-GVO ausschlaggebend ist. Mit dem Wissen, dass jedes vernetzte und autonome Fahrzeug mit Kamerasystemen ausgestattet ist und eine Person im Sichtbereich der Kameras aufnehmen wird, könnten Betroffene auch ein Interesse daran haben, bereits vor einer tatsächlichen Erhebung der Verarbeitung zu widersprechen, um diese von vornherein zu unterbinden. Noch deutlicher wird diese Problematik nach einem bereits erfolgten Widerspruch: Würden Betroffene immer wieder neu widersprechen müssen, wenn Sie sich in den Sichtbereich eines vernetzten und autonomen Fahrzeugs befinden würden, würde das Widerspruchsrecht effektiv unterlaufen.

Ein weiteres Problem hinsichtlich der Betroffenenrechte ergibt sich aus den Informationspflichten. Zwar werden Dashcam-Aufnahmen grundsätzlich als personenbezogene Daten betrachtet, sodass sich entsprechend eine datenschutzrechtliche Relevanz ergibt. Allerdings haben Autohersteller in der Regel wohl keine Möglichkeit, die Betroffenen ohne erheblichen Aufwand zu identifizieren, um sie über ihre Betroffenenrechte zu informieren. Im Falle einer solchen "faktischen Pseudonymisierung" würde jedoch die Ausnahmeregelung des Art. 11 DS-GVO greifen.[285] Da eine Identifikation von Passanten nicht für den Betrieb eines vernetzten und autonomen Fahrzeuges erforderlich ist, sind die Autohersteller nicht verpflichtet, zur bloßen Einhaltung der DS-GVO zusätzliche Informationen einzuholen oder zu verarbeiten, um die betroffenen Personen zu identifizieren.

Im Lichte dieser Probleme wird die DS-GVO mitunter dafür kritisiert, keine Vorschriften zur Videoüberwachung zu beinhalten.[286] Der deutsche Gesetzgeber hat diese Problematik ebenfalls ergänzt und im reformierten Bundesdatenschutzgesetz eine entsprechende Rechtsgrundlage geschaffen. Demnach ist die Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen nur unter den

[283] *Mienert/Gipp*: Dashcam, Blockchain und der Beweis im Prozess, ZD 2017, 514, 517.
[284] Art. 21 Abs. 1 S. 2 DS-GVO.
[285] BeckOK DatenschutzR/*Wolff*, DS-GVO Art. 11 Rn. 11.
[286] *Bretthauer/Krempel/Birnstill*, Intelligente Videoüberwachung in Kranken- und Pflegeeinrichtungen von morgen, CR 2015, 239, 242.

Voraussetzungen des § 4 BDSG (2018) zulässig. In § 4 Abs. 2 BDSG (2018) finden sich auch Ausführungen zu den Informationspflichten, wonach der Umstand der Beobachtung und der Name und die Kontaktdaten des Verantwortlichen sind durch geeignete Maßnahmen zum frühestmöglichen Zeitpunkt erkennbar zu machen sind. Diese Informationspflichten sind, verglichen mit Art. 13 DS-GVO, weniger weitgehend und würden somit den o.g. Schwierigkeiten Rechnung tragen. Allerdings lassen sich konventionelle Mittel, wie etwa Informationsschilder, bei vernetzten und autonomen Fahrzeugen, nicht ohne weiteres nutzen, da sich das Sichtfeld der Kameras laufend ändert. Allenfalls denkbar wäre, entsprechende Hinweise an der erforderlichen Infrastruktur anzubringen und für Betroffene dort Informationen zu allen Autoherstellern bereit zu halten.

Dabei ist allerdings festzustellen, dass die DS-GVO keine Öffnungsklausel für Art. 6 Abs. 1 lit. f) DS-GVO vorsieht, dies ist allenfalls für Verarbeitungen unter den lit. c) und e) möglich, vgl. Art. 6 Abs. 2 DS-GVO.[287] Die Regelung des § 4 BDSG (2018) gilt jedoch nicht nur zur Erfüllung einer rechtlichen Verpflichtung oder für die Wahrnehmung einer Aufgabe im öffentlichen Interesse oder in Ausübung öffentlicher Gewalt, die dem Verantwortlichen übertragen wurde, und ist daher europarechtswidrig.

Bei der Anwendung von § 4 BDSG (2018) ist somit Art. 6 Abs. 1 lit. f) DS-GVO im Zuge einer europarechtskonformen Auslegung mit einzubeziehen.[288] Die zuvor aufgezeigten Problemstellungen werden somit nicht gelöst.

Insgesamt wären daher Anpassungen durch den Gesetzgeber wünschenswert, um die Nutzung von Kameras im Kontext des vernetzten und autonomen Fahrens konkret auszugestalten. So sieht beispielsweise § 4 Abs. 1 S. 2 Nr. 2 BDSG (2018) vor, dass der Schutz von Leben, Gesundheit oder Freiheit von Personen in Fahrzeugen und öffentlich zugänglichen großflächigen Einrichtungen des öffentlichen Schienen-, Schiffs- und Busverkehrs als ein besonders wichtiges Interesse gelten. Diese Wertung ist grundsätzlich nicht zu beanstanden und könnte auch auf das vernetzte und autonome Fahren übertragen werden. Die Bereitstellung von für alle Verkehrsteilnehmer sicheren Technologien ist letztlich im Interesse aller und könnte, als öffentliches Interesse ausgestaltet werden, das auch an die Autohersteller als Beliehene weitergereicht werden kann. Ebenso könnten Autohersteller rechtlich zur Implementierung entsprechender Technologien verpflichtet werden. Der nationale Gesetzgeber könnte dann von seinem Gestaltungsspielraum Gebrauch machen und verhältnismäßige sowie rechtssichere Regeln aufstellen. Zu beachten ist jedoch, dass autonome und vernetzte Fahrzeuge nicht nur in Deutschland, sondern auch länderübergreifend verkehren können sollten. Eine entsprechende Implementierung sollte daher auf europäischer Ebene in Form einer Verordnung erfolgen, um einen größtmöglichen Grad an Harmonisierung zu erreichen.[289]

5.4. AUTOMATISIERTE EINZELENTSCHEIDUNG UND KÜNSTLICHE INTELLIGENZ

Im Kern des autonomen und vernetzten Fahrens steht die Tatsache, dass das Auto selbstständige Entscheidungen treffen kann, um letztlich autonom – also ohne Mitwirkung des Fahrers – am Straßenverkehr teilnehmen zu können. Dies könnte auch im Lichte der Datenschutz-Grundverordnung relevant sein, wonach automatisierte Einzelentscheidungen rechtlichen Einschränkungen unterliegen: Gem. Art.

[287] *Lachenmann*: Neue Anforderungen an die Videoüberwachung, ZD 2017, 407, 410.
[288] A.a.O.
[289] Die Verordnung gilt unmittelbar, vgl. Art. 288 AEUV.

22 DS-GVO hat die betroffene Person das Recht, nicht einer ausschließlich auf einer automatisierten Verarbeitung[290] – einschließlich Profiling – beruhenden Entscheidung unterworfen zu werden, die ihr gegenüber rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt. Strittig ist die Frage, ob es sich um ein Verbot handelt, das nicht von einer Geltendmachung im Einzelfall abhängt[291], oder ob sich lediglich ein Unterlassungsanspruch ableiten lässt.[292]

5.4.1. ANWENDUNGSBEREICH

Zunächst ist zu klären, welche Konstellationen in den Anwendungsbereich des Art. 22 DS-GVO fallen. Zu beachten ist, dass sich die automatisierte Entscheidung im Einzelfall stets auf identifizierbare Personen beziehen muss. Beim autonomen Fahren werden jedoch überwiegend Sachdaten verarbeitet, die von den verschiedenen Sensorsystemen des Fahrzeuges erfasst werden. Gleichwohl können diese Sachdaten, wie in Kapitel 4 beschrieben, auch mit einer natürlichen Person verknüpfen lassen, sodass ein Personenbezug dann vorhanden ist, überwiegend bezüglich des Halters und des Fahrers. Insbesondere der Fahrer sowie andere Nutzer sind zudem unmittelbar von den Entscheidungen des Fahrzeuges betroffen. Ebenfalls betroffen sein können Dritte, beispielsweise Passanten, die durch die Sensor- und Kamerasysteme erfasst werden und deren Sicherheit unmittelbar von den autonomen Entscheidungen des Fahrzeuges abhängig sind. Hinsichtlich Profiling erscheint auch das Infotainment-System als relevant.

5.4.1.1. ENTSCHEIDUNG I.S.D. ART. 22 DS-GVO

Regelungsgegenstand des Art. 22 DS-GVO sind ausschließlich auf automatisierter Verarbeitung beruhende Entscheidungen. Es muss demnach ein gestaltender Akt mit in gewisser Weise abschließender Wirkung vorliegen, die sich rechtlich einer natürlichen oder juristischen Person zurechnen lässt.[293] Strittig ist, ob eine unmittelbar regelnde Wirkung erforderlich ist[294], oder ob vielmehr auch Maßnahmen, die lediglich auf einen tatsächlichen, nicht auf einen rechtlichen Erfolg gerichtet sind dem Anwendungsbereich des Art. 22 Abs. 1 DS-GVO unterfallen können.[295] Nicht jedoch erfasst sind Fälle, die einen lediglich abstrakten Regelungscharakter haben (z.B. Allgemeinverfügungen), da diesen der Bezug zum Einzelfall fehlt.[296] Anders kann sich dies jedoch auswirken, wenn ein Verkehrszeichen als Allgemeinverfügung ein autonomes und vernetztes Fahrzeug adressiert[297] und dieses dann eine automatisierte Entscheidung trifft, die sich auf den Halter oder die Insassen auswirkt. Auch fehlt es an einer Entscheidung, wenn der Betroffene jederzeit einschreiten und die Entscheidung annullieren kann, etwa bei Smart-Home Anwendungen, da der Betroffene hier der Entscheidung nicht unterworfen ist.[298]

---

[290] Der hier möglicherweise entgegenstehende Grad der Entscheidungsfreiheit eines dazwischentretenden Menschen ist strittig, im Anwendungsbereich des vernetzten und autonomen Fahrens jedoch auch nicht weiter relevant.
[291] Gola/*Schulz*, Art. 22 Rn. 5; Paal/Pauly/*Martini*, DS-GVO Art. 22 Rn. 1.
[292] EuArbR/*Franzen*, DS-GVO Art. 22 Rn. 3.
[293] BeckOK DatenschutzR/*von Lewinski*, DS-GVO Art. 22 Rn. 14.
[294] *Abel:* Automatisierte Entscheidungen im Einzelfall gem. Art. 22 DS-GVO, ZD 2018, 304, 305
[295] Paal/Pauly/*Martini*, DS-GVO Art. 22 Rn. 15a; so auch BeckOK DatenschutzR/*von Lewinski*, DS-GVO Art. 22 Rn. 37.
[296] BeckOK DatenschutzR/*von Lewinski*, DS-GVO Art. 22 Rn. 15.
[297] Mit Blick auf die verschiedenen Automatisierungsgrade und der Anforderung, nur noch im Notfall bzw. nach Aufforderung einzugreifen, dürfte es dem Fahrer im Ergebnis nicht mehr zumutbar sein, Verkehrszeichen selber im Blick haben zu müssen.
[298] BeckOK DatenschutzR/*von Lewinski*, DS-GVO Art. 22 Rn. 20.

Für das autonome und vernetzte Fahren können sich hier verschiedene Konstellationen ergeben. Zunächst ist ein autonomes Fahren ohne Algorithmen, die Entscheidungen etwa über die Fahrtroute oder bezüglich des Fahrverhaltens (Geschwindigkeit, Spurwechsel, usw.) treffen, undenkbar. Wenngleich diese Handlungen in der Regel noch keinen rechtlichen Charakter haben, stellen sie jedenfalls eine tatsächliche Maßnahme dar. Insofern sind diese konkreten Entscheidungen in aller Regel auch als eine Entscheidung im Sinne des Art. 22 DS-GVO zu betrachten.

Für bloße Komfort-Entscheidungen, etwa das Einstellen der Temperatur oder der Musikauswahl, bei der der Betroffene jederzeit einschreiten kann, mangelt es an einem unterworfen sein, sodass keine Entscheidung vorliegt. Schwieriger gestaltet sich wiederum die Beurteilung, wenn der Fahrer selbst noch ins Geschehen eingreifen kann, gleichzeitig aber auch die Kontrolle komplett dem Fahrzeug überlassen kann. In aller Regel dürfte ein Fahrer seine volle Aufmerksamkeit hier nicht mehr dem Straßenverkehr widmen.[299] Dies insbesondere, wenn sich der Fahrer auf die volle Selbstständigkeit des Fahrzeuges in der jeweiligen Situation verlassen kann. Dies dürfte jedenfalls ab einem Automatisierungsgrad der Stufe 3 (hochautomatisiert) der Fall sein.[300] Diese Problematik wurde auch vom Gesetzgeber erkannt und im Zuge der Reform des StVG[301] wie folgt geregelt: Gem. des im Lichte autonomen Fahrens neu geregelten § 1b StVG ist der Fahrzeugführer zur unverzüglichen Übernahme der Fahrzeugsteuerung verpflichtet, wenn er durch das System zur Übernahme der Fahrzeugsteuerung aufgefordert wird. Die Pflicht des Fahrzeugführers ist hier zwar auf Sachverhalte beschränkt, in denen er/sie vom Fahrzeug zur Übernahme der Kontrolle aufgefordert wird. Gleichwohl kann bereits die Entscheidung, ob und wann der Fahrzeugführer eine entsprechende Aufforderung erhält, eine tatsächliche Handlung mit erheblicher Bedeutung sein.

Im Gegenzug sind bloße Entscheidungen über die Art und Weise, wie das System Entscheidungen fällt – etwa bei der Nutzung von selbstlernenden Algorithmen und künstlicher Intelligenz – nicht vom Anwendungsbereich erfasst, da es hier an einem Einzelfallbezug fehlt.

Ebenfalls kritisch gesehen werden kann diese Fragestellung bezüglich der fürs vernetzte Fahren erforderlichen Infrastruktur-Systeme. So gelten Verkehrszeichen in der Verwaltungspraxis als Allgemeinverfügung.[302] Dies gilt auch für Verkehrsampeln, sowie (analog) bei Halteverboten oder etwa einer Fahrbahnmarkierung.[303] Auch hier würde also der für Art. 22 DS-GVO geforderte Allgemeinbezug fehlen. Aus datenschutzrechtlicher Sicht stellt sich allerdings sehr wohl die Frage, ob ein Einzelfallbezug bei vernetzten Systemen tatsächlich ausgeschlossen werden kann. Insbesondere Verkehrsleitsysteme benötigen Informationen über den Verkehrsfluss – also auch, ob ein Fahrzeug im Rückstau einer Verkehrsampel steht oder nicht. Wenngleich die Ampel als Verkehrszeichen weiterhin einen allgemeingültigen Charakter hat, ließe sich gleichermaßen argumentieren, dass eine bestimmte Gruppe an Fahr-

[299] Vgl. etwa auch den Unfall des Uber-Testfahrzeuges, wonach die Testfahrerin mehrfach den Blick von der Straße abgewendet hatte, https://www.ntsb.gov/investigations/AccidentReports/Reports/HWY18MH010-prelim.pdf (S. 3).
[300] Vgl. Kapitel 3.
[301] Vgl. Entwurf der Bundesregierung zur Änderung des Straßenverkehrsgesetzes, Drucksache 18/11300, sowie die durch den Verkehrsausschuss geänderte Fassung. Drucksache 18/11776.
[302] BVerwGE 27, 181 (182) = NJW 1967, 1627; E 59, 221 (224 f.) = NJW 1980, 1640; E 92, 32 (34) = NJW 1993, 1729; BVerwG NJW 1995, 1977; NJW 2004, 698; VGH BW NVwZ-RR 1998, 682; HessVGH NJW 1999, 1651 und 2057; OVG NW NJW 1996, 3024; OVG RP NVwZ 1985, 666 (667); OLG Koblenz NJW 1995, 2302.
[303] Schoch/Schneider/*Bier/Schoch*, VwGO § 80 Rn. 150.

zeugen – bei Identifizierbarkeit also mit Ihrem Halter bzw. Fahrer – durch das Verkehrsleitsystem adressiert wird. Ein Einzelfallbezug könnte dann sehr wohl gegeben sein. Entsprechend würde auch hier eine Entscheidung vorliegen.

5.4.1.2. AUTOMATISIERTE VERARBEITUNG

Die Entscheidung müsste sodann ausschließlich mit automatisierter Verarbeitung erreicht werden. Dies ist etwa der Fall, wenn ein computertechnisches System eine Entscheidung ohne jegliche menschliche Einflussnahme trifft[304], oder ein im Prozess involvierter Mensch keinen hinreichenden Einfluss auf die Entscheidung hat.[305] Nicht jedoch erfasst sein sollen Fälle, in denen eine Verarbeitung lediglich eine Entscheidung vorbereitet, oder wo die Verarbeitung unterstützend hinzugezogen wird.[306] Dies insbesondere, weil Art. 22 DS-GVO die Gefahr von nicht überprüften automatisierten Verarbeitungen für den Persönlichkeitsschutz begrenzen will.[307] Ein menschliches Dazwischentreten ist allenfalls bei selbstlernenden Systemen wenigstens in der Trainingsphase als systemimmanenter Prozess anzunehmen.[308] Hier ist jedoch auf die Zielsetzung abzustellen, nämlich die Optimierung des Systems; ein Schutz der Persönlichkeitsrechte des Betroffenen soll hierdurch gerade nicht bezweckt werden.[309] Insofern ist auch bei selbstlernenden Systemen eine automatisierte Verarbeitung in aller Regel anzunehmen.

Eine automatisierte Verarbeitung ist im Kontext von autonomen und vernetzten Fahren in der Regel anzunehmen. Die Loslösung menschlicher Entscheidungsspielräume ist der Nutzung autonomer und vernetzter Systeme gerade inhärent. Wenngleich es Konstellationen geben wird, in denen nach wie vor Menschen Entscheidungen treffen – etwa bei einem Werkstattbesuch – werden doch die allermeisten der o.g. Entscheidungen durch Algorithmen ermittelt und soweit ohne menschliches Einschreiten getroffen, sodass sich hieraus keine nennenswerte Einschränkung des Anwendungsbereichs ergibt.

5.4.1.3. ERHEBLICHKEIT DER ENTSCHEIDUNG

Die Entscheidung müsste zudem erheblich i.S.d. Art. 22 DS-GVO sein, d.h. entweder rechtliche Wirkung entfalten oder den Betroffenen in ähnlicher Weise erheblich beeinträchtigen. Eine rechtliche Wirkung entfaltet eine Maßnahme dann, wenn sie den rechtlichen Status des Betroffenen in irgendeiner Weise verändert.[310] Eine rechtliche Wirkung kann sich nach öffentlichem Recht etwa aus einem Verwaltungsakt ergeben.[311] Dies dürfte insbesondere auch für die o.g. Ausführungen zu möglichen Allgemeinverfügungen durch die Infrastruktur für eine autonome und vernetzte Verkehrsführung zutreffen. Denkbar ist eine solche rechtliche Wirkung ebenfalls, wenn es durch den Verstoß gegen Verkehrsregeln zu einer Ordnungswidrigkeit oder Straftat kam, für die der Fahrzeughalter oder -fahrer haften muss. Entsprechende Konstellationen sind hier insbesondere denkbar, wenn noch keine vollständige Automatisierung vorliegt (etwa lediglich eine Hochautomatisierung der Stufe 3[312]).

[304] Paal/Pauly/*Martini*, DS-GVO Art. 22 Rn. 16.
[305] Gola/*Schulz*, Art. 22 Rn. 14.
[306] Franzen/Gallner/*Oetker/Franzen* DS-GVO Art. 22 Rn. 1.
[307] Paal/Pauly/*Martini*, DS-GVO Art. 22 Rn. 20.
[308] BeckOK DatenschutzR/*von Lewinski*, DS-GVO Art. 22 Rn. 23.2.
[309] A.a.O.
[310] Paal/Pauly/*Martini*, DS-GVO Art. 22 Rn. 26.
[311] Gola/*Schulz*, Art. 22 Rn. 23.
[312] Vgl. Kapitel 3.

Liegt keine rechtliche Entscheidung vor, wäre der Anwendungsbereich des Art. 22 DS-GVO nur eröffnet, wenn eine anderweitige erhebliche Beeinträchtigung gegeben wäre. Als Beeinträchtigung kann grundsätzlich jede Entscheidung betrachtet werden, die eine negativ fühlbare Konsequenz nach sich zieht.[313] Gleichwohl bleibt unklar, ob die rechtlichen Folgen tatsächlich negativ, oder auch positiv sein können.[314] Bezüglich der Erheblichkeit kommt es hingegen auf objektive Faktoren im Einzelfall an.[315] Denkbar wären hier etwa Entscheidungen, die eine beträchtlich erhöhte Fahrtzeit nach sich ziehen, z.B. die falsche Berechnung einer Route. Dabei wäre jedoch zu bedenken, dass es an einem unterworfen sein fehlt, wenn der Betroffene jederzeit eingreifen könnte.[316] Im Übrigen ist zu beachten, dass Art. 22 DS-GVO nur Datenverarbeitungen erfassen soll, jedoch nicht den Charakter eines Anti-Diskriminierungsgesetzes o.ä. einnimmt.[317] Entsprechend muss die Entscheidung auch für das Persönlichkeitsrecht erheblich sein.[318] Dies dürfte sich jedenfalls nicht für alle Entscheidungen, die im Rahmen des autonomen und vernetzten Fahrens durch automatisierte Datenverarbeitung erreicht werden und die keine rechtliche Beeinträchtigung darstellen, annehmen lassen.

5.4.1.4. PROFILING

Art. 22 DS-GVO erfasst auch den Spezialfall des Profiling. Gem. Art. 4 Nr. 4 DS-GVO bezeichnet Profiling jede Art der automatisierten Verarbeitung personenbezogener Daten, die darin besteht, dass diese personenbezogenen Daten verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten, insbesondere um Aspekte bezüglich Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel dieser natürlichen Person zu analysieren oder vorherzusagen. Die Bewertung soll dabei jedoch eine gewisse Komplexität implizieren, da die Erfassung trivialer Entscheidungen wenig sachgerecht scheint.[319] Personalisierte Werbung und sonstige vergleichbare Individualisierungen, sind demnach nicht von Art. 22 Abs. 1 DS-GVO erfasst.[320] Beim vernetzten und autonomen Fahren ist zu hinterfragen, für welche Anwendungsfälle Profiling vorliegend in Betracht kommt.

Ein relativ offensichtlicher Anwendungsbereich, gerade bezüglich der Individualisierung auf Basis der Gewohnheiten und Wünsche des Nutzers, wäre das Infotainment System. Hier werden jedoch in aller Regel keine komplexen Auswertungen erfolgen, die über die zuvor genannten Personalisierungen hinausgehen. Eine Anwendbarkeit von Art. 22 DS-GVO dürfte hier somit in aller Regel nicht in Betracht kommen.

Eine größere Komplexität der Auswertung könnte sich aber bei der Auswertung von Standortdaten ergeben; insbesondere soll die Analyse von Ortswechseln explizit als Profiling erfasst werden.[321] Erfolgt hier eine entsprechende Auswertung, beispielsweise zum Tracking oder zur Optimierung von Fahrtrouten, dürfte Profiling vorliegen. Insbesondere ist die Errechnung von Wahrscheinlichkeitswerten, was diesbezüglich denkbar erscheint, vom Anwendungsbereich der Norm erfasst.[322] Eine ähnliche Wertung

[313] BeckOK DatenschutzR/*von Lewinski*, DS-GVO Art. 22 Rn. 38.
[314] Ehmann/Selmayr/*Hladjik*, Art. 22 Rn. 9.
[315] Paal/Pauly/*Martini*, DS-GVO Art. 22 Rn. 27.
[316] S.o. zur Frage, ob eine Entscheidung i.S.d. Art. 22 DS-GVO vorliegt.
[317] BeckOK DatenschutzR/*von Lewinski*, DS-GVO Art. 22 Rn. 38.
[318] Paal/Pauly/*Martini,* DS-GVO Art. 22 Rn. 27.
[319] BeckOK DatenschutzR/*von Lewinski*, DS-GVO Art. 22 Rn. 12.
[320] Paal/Pauly/*Martini*, DS-GVO Art. 22 Rn. 23.
[321] Vgl. Art. 4 Nr. 4 DS-GVO.
[322] Ehmann/Selmayr/*Hladjik*, Art. 22 Rn. 7.

dürfte sich ergeben, wenn die Fahrweise des Fahrers analysiert wird, z.B. zur Nutzung von Telematik-Tarifen bei den KFZ-Versicherungen.[323] Eine entsprechende Nutzung ist jedoch - in beiden Fällen - kein integraler Bestandteil des vernetzten und autonomen Fahrens. Insofern lässt sich das Vorliegen von Profiling nicht ohne weiteres pauschal annehmen.

5.4.2. AUSNAHMEREGELN

Nach Art. 22 Abs. 1 DS-GVO hat der Betroffene das Recht, nicht einer ausschließlich auf einer automatisierten Verarbeitung – einschließlich Profiling – beruhenden Entscheidung unterworfen zu werden, die ihr gegenüber rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt. Dies gilt gem. Abs. 2 nicht,

- wenn die Entscheidung für den Abschluss oder die Erfüllung eines Vertrags zwischen der betroffenen Person und dem Verantwortlichen erforderlich ist,
- aufgrund von Rechtsvorschriften der Union oder der Mitgliedstaaten, denen der Verantwortliche unterliegt, zulässig ist und diese Rechtsvorschriften angemessene Maßnahmen zur Wahrung der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person enthalten oder
- mit ausdrücklicher Einwilligung der betroffenen Person erfolgt.

In den Fällen, in denen die Entscheidung zur Durchführung eines Vertrages erforderlich ist oder auf der Einwilligung des Betroffenen beruht (vgl. Art. 6 Abs. 1 lit. a) bzw. b) DS-GVO) müssen angemessene Maßnahmen implementiert werden, um die Rechte und Freiheiten sowie die berechtigten Interessen der betroffenen Person zu wahren, wozu mindestens das Recht auf Erwirkung des Eingreifens einer Person seitens des Verantwortlichen, auf Darlegung des eigenen Standpunkts und auf Anfechtung der Entscheidung gehört.[324]

Dies dürfte sich in der Praxis als durchaus schwierig erweisen. Autonomes Fahren ist nicht möglich, wenn durch den Verantwortlichen eine menschliche Interventionsmöglichkeit sichergestellt sein muss. Allenfalls könnte hier über eine Interventionsmöglichkeit des Betroffenen selbst nachgedacht werden; wie oben ausgeführt, wäre in solchen Konstellationen der Anwendungsbereich des Art. 22 DS-GVO jedoch gar nicht eröffnet, da es an einem Unterworfensein fehlen würde. In der Praxis scheint daher eine Rechtsvorschrift der Union oder der Mitgliedstaaten erforderlich, die den Risiken entsprechend Gebühr trägt.[325]

5.4.3. ERKLÄRBARKEIT VON ENTSCHEIDUNGEN

Eine Problematik, die nicht nur dem autonomen und vernetzten Fahren immanent ist, sondern vielmehr jeglichen Anwendungsbereichen von künstlicher Intelligenz, ist die Frage der Erklärbarkeit von Entscheidungen. Wie bereits dargelegt, lassen sich Algorithmen bei der Nutzung autonomer Fahrzeuge und einer vernetzten Verkehrsinfrastruktur nicht hinwegdenken. Wie zuvor dargelegt, können solche automatisierten Entscheidungen auch grundsätzlich dem Art. 22 DS-GVO unterliegen. Neben den zuvor genannten Maßnahmen sieht die DS-GVO vor, dass Betroffene auch gewisse Rechte bezüglich einer

[323] Vgl. auch Kapitel 5.5; im Detail siehe außerdem die Vertiefungsstudie "Profiling und automatisierte Einzelentscheidungen im Versicherungsbereich".
[324] Vgl. Art. 22 Abs. 3 DS-GVO.
[325] Zu den Rechtsgrundlagen vgl. auch Kapitel 5.2.

automatisierten Entscheidung im Einzelfall gegenüber dem Verantwortlichen haben. So ist der Verantwortliche gem. der Art. 13 Abs. lit. f), 14 Abs. 2 lit. g) und 15 Abs. 1 lit. h DS-GVO verpflichtet, dem Betroffenen zu informieren über

- das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling gemäß Artikel 22 Absätze 1 und 4,
- aussagekräftige Informationen über die involvierte Logik sowie
- die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person.

Gem. Art. 12 Abs. 1 DS-GVO sind diese Informationen dem Betroffenen in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu übermitteln.[326] Angemerkt wird allerdings, dass diese Regelungen nicht hinreichend klar sind.[327] Dem ist zuzustimmen: Während eine Information über das Bestehen einer automatisierten Entscheidungsfindung im Einzelfall unproblematisch sein dürfte, bleibt unklar, was mit aussagekräftigten Informationen über die involvierte Logik gemeint ist. Zudem lässt Art. 12 Abs. 1 DS-GVO Interpretationsspielraum bezüglich des Verständnishorizontes bei der Frage, wann eine Information hinreichend verständlich ist.

5.4.3.1. AUSSAGEKRÄFTIGE INFORMATIONEN ÜBER DIE INVOLVIERTE LOGIK

In der Praxis stellt sich das Bereitstellen aussagekräftiger Informationen über die involvierte Logik bei der Nutzung von künstlicher Intelligenz und selbstlernender Systeme als Herausforderung dar. Insbesondere sind entsprechende Algorithmen oftmals gleichzeitig Geschäftsgeheimnisse der Verantwortlichen. Die Offenlegung des gesamten Algorithmus würde daher mit den berechtigten Interessen der Verantwortlichen, ihre Geschäftsgeheimnisse geheim zu halten, kollidieren. In diesem Kontext hatte der BGH bereits entscheiden, dass die Schufa ihren Scoring-Algorithmus nicht offenlegen muss, da das Interesse am Schutz des Geschäftsgeheimnisses das Auskunftsrecht des Betroffenen überwiege.[328] Demnach soll lediglich dargelegt werden, welche personenbezogenen Informationen für eine Entscheidung berücksichtigt wurden. Dabei ist jedoch anzumerken, dass das Urteil vom 28. Januar 2014 ist, mithin also vor Beschluss und in Kraft treten der DS-GVO. Die Wertungen des Gerichts bezogen sich somit auf die alte Rechtslage. Allerdings scheint es naheliegend, diese Wertungen auch zukünftig aufrecht zu erhalten, da der Schutz von Algorithmen insbesondere in einer digitalisierten Welt auch weiterhin ein wichtiger Wirtschaftsfaktor ist. Die DS-GVO solle daher nicht dahingehend ausgelegt werden, dass nunmehr eine Pflicht zur Offenlegung von Geschäftsgeheimnissen bestünde.[329] Diese Wertung lässt sich auch der DS-GVO entnehmen: Erwägungsgrund 63 DS-GVO führt insoweit aus, dass das Auskunftsrecht des Betroffenen nicht die Rechte und Freiheiten anderer Personen, etwa Geschäftsgeheimnisse oder Rechte des geistigen Eigentums und insbesondere das Urheberrecht an Software, negativ beeinträchtigen soll. Vor diesem Hintergrund sollte eine Information über die Grundannahmen der Algorithmus-Logik als ausreichend erachtet werden.[330] Dies könnte sich aus den zugrundeliegenden,

[326] Paal/Pauly/*Martini*, DS-GVO Art. 22 Rn. 41a.
[327] *Bräutigam/Schmidt-Wudy*, Das geplante Auskunfts- und Herausgaberecht des Betroffenen nach Art. 15 der EU-Datenschutzgrundverordnung, CR 2015, 56, 62.
[328] BGH VI ZR 156/13.
[329] *Roßnagel/Nebel/Richter*, Was bleibt vom Europäischen Datenschutzrecht? Überlegungen zum Ratsentwurf der DS-GVO ZD 2015, 455, 458.
[330] Paal/Pauly/*Paal/Hennemann*, DS-GVO Art. 13 Rn. 31.

geeigneten mathematischen oder statistischen Verfahren ergeben.[331] Gleichwohl muss abgewartet werden, inwiefern die vom BGH aufgestellte Wertung zum Schufa-Urteil tatsächlich aufrechterhalten werden kann.[332] Eine eindeutige Beantwortung dieser Frage scheint damit zum jetzigen Zeitpunkt nicht abschließend möglich.

Aus technischer Sicht wird die Realisierung des Auskunftsrechts durch Phänomene wie die sog. „black box" erschwert: Selbstlernende Algorithmen verbessern sich fortlaufend selbst, und – Stand heute - es ist oftmals nicht möglich, Entscheidungsprozesse rückwirkend nachzuvollziehen. Auch müssten womöglich die Informationen, die dem Betroffenen zur Verfügung gestellt werden, laufend angepasst werden, wenn eine automatische Anpassung durch den Algorithmus selbst erfolgt. Diese Problematik spräche ebenfalls dafür, lediglich die Grundannahmen der Algorithmus-Logik zu erklären. Bei selbstlernenden Algorithmen stellt sich jedoch durchaus die Frage, wie groß sich eine Abweichung vom vorgegebenen Regelwerk (bezüglich der Frage, wie der Algorithmus lernen soll) ergeben kann. Jedenfalls wenn die Grundannahmen der Logik, auf dessen Basis der Algorithmus lernt, nicht ausreichen, um die Entscheidungsfindung im Anschluss verstehen zu könnten, dürften die Anforderungen an den Grundsatz der Transparenz damit nicht erfüllt sein.[333] Hier dürfte insbesondere eine weitere Zusammenarbeit von Experten im Datenschutzrecht mit Informatikern erforderlich sein, um sicherzustellen, dass einerseits technisch realisierbare Lösungen berücksichtigt werden, während andererseits ein hinreichender Schutz der Betroffenen gewährleistet ist.

5.4.3.2. VERSTÄNDLICHKEIT DER INFORMATIONEN

Eine weitere Problematik ergibt sich aus der Frage, wie – mitunter sehr komplexe – Informationen verständlich dargelegt werden können. So ist etwa unklar, wer das maßgebliche Beurteilungssubjekt ist: Die betroffene Person, der Verantwortliche oder ein verständiger Dritter?[334] Dabei muss insbesondere berücksichtigt werden, dass aussagekräftige Informationen bei einem komplexen Algorithmus auch komplexe Informationen erforderlich machen könnten. Naturgemäß hat der Verantwortliche den besten Überblick über die eingesetzte Technologie. Gleichzeitig führt dieser Wissensvorsprung in der Praxis dazu, dass etwa der Betroffene kaum in der Lage sein wird, derart komplexe, technische Informationen zu verstehen. Detaillierte Informationen erhöhen insofern nicht zwingend die Transparenz für den Betroffenen. Dies ergibt sich auch bereits aus Erwägungsgrund 58 sowie Art. 12 Abs. 1 DS-GVO, wonach eine einfache und verständliche Sprache genutzt werden soll. Dies dürfte kaum möglich sein, wenn ein komplexer Algorithmus im Detail – also aus Sicht des Verantwortlichen - erklärt werden soll.

Wird hingegen richtigerweise auf den Betroffenen als Empfänger abgestellt, bleibt allein die zuvor aufgeworfene die Frage, ob die Informationen für den individuell Betroffenen verständlich sein müssen, oder ob hier ein verständiger und objektiver Dritter als Referenz herangezogen werden kann. Dagegen spricht, dass dann nicht gewährleistet werden kann, dass dem individuell Betroffenen tatsächlich die in der DS-GVO festgelegten Informationen nicht zur Verfügung stünden. Gleichzeitig zeigen sich in der Gesellschaft große Unterschiede bezüglich des Verständnisses von ICT-Systemen. Den Verantwortlichen abzuverlangen dafür Sorge zu tragen, dass *jeder* diese Informationen versteht, würde mit Blick auf die große Individualität in der Praxis dazu führen, dass große Rechtsunsicherheit entstünde. Auf den durchschnittlichen Nutzer abzustellen scheint daher insgesamt die sachgerechteste Lösung.[335]

---

[331] Plath/*Kamlah*, Art. 22 Rn. 16.
[332] BeckOK DatenschutzR/*Schmidt-Wudy*, DS-GVO Art. 15 Rn. 78.3
[333] Vgl. auch Erwägungsgrund 60.
[334] BeckOK DatenschutzR/*Schmidt-Wudy*, DS-GVO Art. 15 Rn. 78.
[335] A.a.O., Rn. 78.2.

Mit Blick auf das autonome und vernetzte Fahren ergeben sich hier keine spezifischen Herausforderungen, die über die aufgezeigten Probleme bei der Nutzung von KI im Allgemeinen hinausgehen. Wie sich die praktische Umsetzung der DS-GVO in diesem Feld entwickeln wird, wird jedenfalls weiter beobachten zu sein.

5.5. FUNCTION CREEP

Eine weitere Problematik, die im Kontext des vernetzten und smarten Fahrens mit Blick auf die Vielzahl der verfügbaren Informationen relevant ist, ist das Phänomen des "function creep", also die schleichende Ausweitung der Zweckbestimmung. Die europäische Kommission beschreibt "function creep" als den Umstand, dass Prozesse und Technologien, die für einen bestimmten Zweck implementiert wurden, auf andere Zwecke angewendet werden, die bei der ursprünglichen Implementierung nicht diskutiert wurden, und für die es insofern keine sichere Zustimmung aller Beteiligten gibt.[336] Im Kontext des Datenschutzrechts heißt das also, dass personenbezogene Daten, die für einen festgelegten, legitimen Zweck verarbeitet werden, um eine spezielle Funktion zu erfüllen, nunmehr für andere Zwecke als ursprünglich angedacht verarbeitet werden. Dies kann sich etwa durch sich weiterentwickelnde technische Möglichkeiten ergeben. Mit Blick auf den Zweck stellt sich dann die Frage, ob etwas, das zunächst als sozial, ethisch und rechtlich zulässiger Zweck erscheint, sich durch neue technische Möglichkeiten in eine Richtung entwickelt, wo dies nicht mehr ohne Weiteres angenommen werden kann. Problematisch ist dies aus datenschutzrechtlicher Sicht insbesondere mit Blick auf den Grundsatz der Zweckbindung, aber auch hinsichtlich der erforderlichen Transparenz. Insofern lässt sich vertreten, dass das Risikopotential einer Zweckänderung durchaus große Gefahren für den Schutz der Privatsphäre darstellt, sowohl bei der Nutzung durch öffentliche als auch durch private Stellen.[337]

Hinsichtlich des vernetzten und autonomen Fahrens können sich hier diverse Konstellationen ergeben, für die "function creep" in Betracht kommt. So dürften einerseits KFZ-Versicherer ein Interesse daran haben, auf Informationen aus einem Smart Car zuzugreifen, um Prämien akkurat zu berechnen - solche "Telematik-Tarife" werden bereits heute angeboten. Hierbei trifft jedoch der Fahrer selbst eine freiwillige Entscheidung, ob er seine Fahrtdaten offenlegen will.[338] Denkbar ist allerdings durchaus, dass sich solche Tarife als Standard etablieren.[339] Gerade mit dem Vorhandensein umfangreicher Sensorsysteme und -daten scheint dies umso naheliegender zu sein, ebenso eine dann verpflichtende Nutzung. Neben Versicherungen können sich jedoch auch andere Anwendungsfälle ergeben, z.B. zur Ahndung von Ordnungswidrigkeiten. Insgesamt dürfte sich jedenfalls eine Verschiebung der Interessenlage hinsichtlich der Nutzung personenbezogener Daten ergeben: Mit zunehmender Automatisierung, insbesondere ab einer Vollautomatisierung (Stufe 4[340]), dürften jedenfalls Versicherungen kein Interesse mehr an Zugriff auf Daten über das Verhalten des Fahrers haben, da mit zunehmender Automatisierung der Grad der

[336] European Commission Directorate-General Joint Research Centre, Biometrics at the Frontiers: Assessing the Impact on Society. For the European Parliament Committee on Citizens' Freedoms and Rights, Justice and Home Affairs (LIBE), Executive Summary, 2005, p 7.
[337] House of Commons Science and Technology Committee, Current and future uses of biometric data and technologies, Sixth Report of Session 2014–15, p.27.
[338] *Klimke*: Telematik-Tarife in der Kfz-Versicherung, r+s 2015, 217.
[339] A.a.O.
[340] Vgl. Kapitel 2.1.

Verantwortlichkeit des Fahrers sinkt und insofern auch weniger Interesse an der Nutzung personenbezogener Daten besteht. Damit sinkt auch das Risiko, das sich aus einer Zweckänderung für die Betroffenen ergeben kann.

Die rechtliche Würdigung einer Zweckänderung hängt grundsätzlich davon ab, wie diese umgesetzt wird. Zunächst hätte der Gesetzgeber die Möglichkeit tätig zu werden und entsprechende Anpassungen umzusetzen. Eine Rechtsvorschrift des Unionsrechts oder des nationalen Rechts, die dies erlaubt, müsste allerdings notwendig und verhältnismäßig sein und dem Schutz eines der Ziele, die Art. 23 Abs. 1 DS-GVO nennt, dienen.[341] Dies könnte etwa eine Kontroll-, Überwachungs- und Ordnungsfunktionen sein, die dauernd oder zeitweise mit der Ausübung öffentlicher Gewalt für die unter den Art. 23 lit. a), b), c), d), e) und g) DS-GVO genannten Zwecke verbunden sind. Die Herstellung Aufrechterhaltung einer Infrastruktur für vernetztes und autonomes Fahren - einschließlich der Einhaltung aller relevanten Regeln - kann mitunter großen Einfluss auf die wirtschaftliche Entwicklung eines Landes haben. Dies könnte entsprechend ein öffentliches Interesse i.S.d. Art. 23 Abs. 1 lit. e) DS-GVO darstellen.[342]

Darüber hinaus finden sich jedoch auch entsprechende Regelungen in der DS-GVO selber: Gem. Art. 5 Abs. 1 lit. b) DS-GVO müssen personenbezogene Daten für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden. Zu diesen nicht als unvereinbar gelten gem. Art. 5 Abs. 1 lit. b) 2. Hs. i.V.m. Art. 89 Abs. 1 DS-GVO eine Weiterverarbeitung für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke. Die DS-GVO sieht demnach vor, dass an den Primärzweck als Maßstab zur Beurteilung angeknüpft werden muss.[343] Die in Art. 5 Abs. 1 lit. b) DS-GVO genannte Liste ist jedoch nicht abschließend: Wann der Zweck einer Weiterverarbeitung mit dem Erhebungszweck vereinbar ist, wird in Art. 6 Abs. 4 DS-GVO weiter konkretisiert.[344] Beruht die Verarbeitung demnach nicht auf einer Einwilligung oder einer Rechtsvorschrift i.S.d. Art. 23 DS-GVO (s.o.), sind u.a. folgende Faktoren zu berücksichtigen:

- jede Verbindung zwischen den Zwecken, für die die personenbezogenen Daten erhoben wurden, und den Zwecken der beabsichtigten Weiterverarbeitung,
- den Zusammenhang, in dem die personenbezogenen Daten erhoben wurden, insbesondere hinsichtlich des Verhältnisses zwischen den betroffenen Personen und dem Verantwortlichen,
- die Art der personenbezogenen Daten, insbesondere ob besondere Kategorien personenbezogener Daten gemäß Artikel 9 verarbeitet werden oder ob personenbezogene Daten über strafrechtliche Verurteilungen und Straftaten gemäß Artikel 10 verarbeitet werden,
- die möglichen Folgen der beabsichtigten Weiterverarbeitung für die betroffenen Personen,
- das Vorhandensein geeigneter Garantien, wozu Verschlüsselung oder Pseudonymisierung gehören kann.

Anzumerken ist, dass auch diese Kriterien nicht abschließend sind.[345] Eine rechtssichere Beurteilung gestaltet sich insofern als schwierig und hebt das Erfordernis, eines guten Zusammenspiels zwischen

[341] BeckOK DatenschutzR/*Schantz*, DS-GVO Art. 5 Rn. 22.
[342] Gola/*Gola*, Art. 23 Rn. 2.
[343] Paal/Pauly/*Frenzel*, DS-GVO Art. 5 Rn. 30.
[344] *Dammann*, Erfolge und Defizite der EU-Datenschutzgrundverordnung - Erwarteter Fortschritt, Schwächen und überraschende Innovationen, ZD 2016, 307 (312), Schantz, Die Datenschutz-Grundverordnung – Beginn einer neuen Zeitrechnung im Datenschutzrecht, NJW 2016, 1841, 1844.
[345] Paal/Pauly/*Frenzel*, DS-GVO Art. 6 Rn. 48.

Datenschutzbeauftragten, Aufsichtsbehörden und Gerichten in den Vordergrund.[346] Im Lichte des vernetzten und autonomen Fahrens dürften sich hier - mit Blick auf die Komplexität der Systeme und dem Zusammenspiel verschiedener Stellen - durchaus praktische Schwierigkeiten ergeben.

Bezüglich der zuvor genannten Anwendungsbeispiele zeigen sich bereits spezifische Herausforderungen. So ist bei einer Vielzahl der erfassten Daten zunächst von einem primär technischen Verarbeitungszweck auszugehen. Insofern besteht keine hinreichende Verbindung zwischen diesem ursprünglichen Zweck und einer Weiterverarbeitung für Versicherungszwecke oder zur Ahndung von Ordnungswidrigkeiten. Auch der Zusammenhang, in dem die personenbezogenen Daten erhoben wurden, insbesondere hinsichtlich des Verhältnisses zwischen der betroffenen Person und dem Verantwortlichen, dürfte für diese Zwecke wenig hilfreich sein, da weder mit Versicherern noch mit Ordnungsbehörden eine direkte Datenverarbeitung erfolgt. Identisch sind hingegen die Daten, die genutzt würden, da durch das Vorhandensein einer großen Anzahl an Daten keine weiterführende Erhebung erforderlich ist. Hinsichtlich möglicher Folgen lässt sich anmerken, dass jedenfalls bei Ordnungswidrigkeiten in der Regel eine negative Konsequenz für den Betroffenen entstehen dürfte. Bei Versicherungen könnte sich der Effekt in Form von günstigeren Tarifen zwar auch positiv äußern, kann im Einzelfall jedoch ebenfalls negative Auswirkungen haben. Das Vorhandensein geeigneter Garantien wie Pseudonymisierung und Verschlüsselung könnte aus technischer Sicht - wenigstens bis zu einem gewissen Grad - realisiert werden.

In der Summe dürften diese Faktoren jedoch nicht reichen, um eine solche Zweckänderung zu legitimieren. Insbesondere sind die möglichen negativen Folgen für den Betroffenen zu nennen, für die es - der Natur der Anwendungsfälle entsprechend - keine Maßnahmen gibt, um diese Folgen abzudämpfen.

Daraus ergibt sich, dass eine Zweckänderung unter Berücksichtigung der DS-GVO allenfalls möglich ist, wenn eine Rechtsvorschrift des Unionsrechts oder des nationalen Rechts dies erlaubt. Dabei sind jedoch die in Art. 23 DS-GVO festgelegten Einschränkungen zu beachten. Vor diesem Hintergrund scheinen Zweckänderungen nicht gänzlich ausgeschlossen. Der Gesetzgeber sollte dabei jedoch stets die Auswirkungen auf Betroffene im Blick haben und für entsprechende Garantien bzw. einen entsprechenden Ausgleich sorgen, um negative Folgen so weit wie möglich zu reduzieren.

5.6. ANFORDERUNGEN AN DATENVERARBEITENDE SYSTEME IM KONTEXT VON SMART CARS

Die Grundsätze in Art. 5 DSVGO beschreiben nicht nur die rechtlichen Voraussetzungen der Datenverarbeitung, sondern unter lit. f.) mit der Integrität und Vertraulichkeit von Daten auch zur Datensicherheit. Damit wird in der DS-GVO auch ein sog. technischer Datenschutz in Form der Datensicherheit implementiert. Die Gewährleistung der Datensicherheit wird in Art. 32 DS-GVO nochmal konkretisiert und verpflichtet den Verantwortlichen zur Implementierung von geeigneten technischen und organisatorischen Maßnahmen, die das Schutzziel der Vertraulichkeit und Integrität der verarbeiteten Daten gewährleisten sollen.[347] Geschützt werden sollen damit nicht nur Angriffe auf die Datensätze sondern auch die unbeabsichtigte Veränderung oder der Verlust der Daten.[348] Die Datensicherheit ist damit immer ein

[346] Gola/*Schulz*, Art. 6 Rn. 179.
[347] BeckOK DatenschutzR/*Schantz*, DS-GVO Art. 5 Rn. 35.
[348] Paal/Pauly/*Martini*, DS-GVO Art. 32 Rn. 29.

Thema, sobald dem Verantwortlichen eine Rechtsgrundlage zur Verarbeitung der Daten zur Verfügung steht. Ein Mindestmaß an Datensicherheit ist immer erforderlich, unabhängig vom Risiko der Verarbeitung. Die Maßnahmen müssen jedoch verbessert werden, wenn das Risiko der Verarbeitung steigt um "geeignete" Maßnahmen im Sinne des Art. 32 DS-GVO darzustellen.[349] Abwägungsfaktoren in diesem Zusammenhang sind nicht nur die Risiken der Datenverarbeitung sondern auch der Stand der Technik sowie die Implementierungskosten.[350] Zur Beurteilung des Risikos der Datenverarbeitung sind nach Art. 32 Abs. 1 DS-GVO folgende Parameter zu berücksichtigen:

- die Art der Verarbeitung,
- der Umfang der Verarbeitung,
- die Umstände und die Zwecke der Verarbeitung
- sowie die unterschiedlichen Eintrittswahrscheinlichkeit und
- Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen.

Im Ergebnis bedeutet dieses, dass die getroffenen Maßnahmen nicht nur digitaler Natur sein müssen sondern auch physikalische Maßnahmen zu treffen sind. Dazu gehören neben den ordnungsgemäßen Datenverarbeitungsvorgängen und der Schaffung einer angemessenen Organisationsstruktur, die den Datenschutz hinreichend in ihre Abläufe einbezieht, auch hardwarebasierte Maßnahmen. Die DS-GVO nennt dabei in Art. 32 Abs. 1 DS-GVO beispielhaft konkrete Maßnahmen und Ziele, wie

- die Pseudonymisierung und Verschlüsselung von personenbezogenen Daten,
- die Fähigkeit, Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen,
- die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen, und
- ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

Entsprechend den Vorgaben aus Art. 5 Abs. 2 DS-GVO und Art. 24 Abs. 1 DS-GVO ist der für die Datenverarbeitung Verantwortlich verpflichtet über die Umsetzung dieser Maßnahmen einen Nachweis zu erbringen, diese müssen somit dokumentiert werden. Die getroffenen technischen und organisatorischen Maßnahmen müssen außerdem regelmäßig überprüft und aktualisiert werden.[351]

5.6.1. PRIVACY BY DESIGN UND PRIVACY BY DEFAULT

Systematisch in der DS-GVO im Rahmen der Gewährleistung der Sicherheit (Art. 32 DS-GVO) vorgeordnet, aber im weiteren Sinne auch eine Maßnahme zur Datensicherheit, sind die in Art. 25 DS-GVO geregelten Ansätze zu Privacy by Design und Privacy by Default.[352] Demnach sind bereits während der Entwicklung von Produkten, die auch personenbezogene Daten verarbeiten, geeignete technische und organisatorische Maßnahmen zu bestimmen. So soll die Einhaltung der DS-GVO, insbesondere mit

[349] Vgl. Paal/Pauly/*Martini*, DS-GVO Art. 32 Rn. 51.
[350] Vgl. Paal/Pauly/*Martini*, DS-GVO Art. 32 Rn. 26.
[351] Art. 24 Abs. 1 S. 2 DS-GVO.
[352] Paal/Pauly/*Martini*, DS-GVO Art. 25 Rn. 4.

Blick auf die Datenminimierung und die Rechte der Betroffenen, effektiv eingebunden und bedacht werden (Privacy by Design).[353] Weiterhin verlangt der Abs. 2, dass die Voreinstellungen des datenverarbeitenden Objektes so konfiguriert sind, dass nur die personenbezogenen Daten verarbeitet werden die für den jeweiligen bestimmten Verarbeitungszweck auch erforderlich sind (Privacy by Default).[354] Dabei muss insbesondere sichergestellt werden, dass personenbezogene Daten nicht bereits per Voreinstellung und ohne ein aktiv werden der betroffenen Person einer unbestimmten Zahl von natürlichen Personen zugänglich gemacht werden.

Privacy by Design bezieht sich auf den Ansatz, dass "der Datenschutz proaktiv in das Design und die Architektur eines IKT-Systems eingebettet werden muss".[355] Mit diesem Ansatz kann die Zeit erspart werden, um bereits bestehende Datenverarbeitungssysteme zu verbessern und existierende Datenschutzprobleme zu beheben, die zum Zeitpunkt der Entwicklung nicht beachtet wurden.[356] Es schützt auch die Rechte der Benutzer, stärkt ihr Vertrauen in die von ihnen verwendeten Technologien und gewährleistet die organisatorische Verantwortung.[357] Mit Privacy by Default wird ein Ansatz verfolgt, bei dem Grundeinstellungen der Technologie so konfiguriert sind, dass nur die wirklich notwendigen Daten verarbeitet werden und damit den Grundsätzen der Datenvermeidung und Datensparsamkeit ebenfalls von Anfang an genüge getan wird und der Nutzer alle weiteren Datenverarbeitungsvorgänge eigenverantwortlich konfigurieren kann.[358]

Somit sollten von Beginn an datenschutzrechtliche Belange in das Design des vernetzten und automatisierten Fahrzeuges mit einfließen und die Datenverarbeitung nur auf das notwendige Maß beschränkt werden. Das Betrifft den Umfang der erhobenen Daten sowie die Übermittlungsvorgänge und weiteren Datenverarbeitungsprozesse.[359]

Ein effektiver Schutz durch organisatorische Maßnahmen kann hier bereits durch den Teilbereich des Aufbewahrungsortes der Daten gewährleistet werden. In Betracht kommen können hierfür drei unterschiedliche Szenarien: Zum einen können die Daten im Auto gespeichert werden (sog. Event-Data-Recording), fraglich bleibt dann ob es sich noch um ein klassisches "Connected-Car" handelt[360]. Eine weitere Möglichkeit wäre es, die Daten in der Cloud der jeweiligen Fahrzeuganbieter oder Versicherungen zu speichern oder in einer durch den Betroffenen frei wählbaren Cloud. Als letzte Möglichkeit könnten die generierten Daten in die Hände eines Treuhänders gegeben werden, der diese nur unter bestimmten Voraussetzungen an Dritte herausgibt.[361] Im Ergebnis müsste bei den verschiedenen Alternativen eine Abwägung zwischen dem Datenschutz und der Zweckmäßigkeit erfolgen. Die Speicherung direkt im Fahrzeug wäre für die Betroffenen wohl am sichersten, sofern entsprechende IT-Sicherheitsmaßnahmen implementiert sind, aber erfüllt wohl nicht die Ansprüche und den Komfort eines „Connected-Car“. Zudem würde es die Automatisierung des Fahrzeuges erheblich erschweren. Dagegen kann

[353] Art. 25 Abs. 1 DS-GVO.
[354] Art. 25 Abs. 2 DS-GVO.
[355] *Cavoukian/Dixon*, PbD, 5.
[356] *Schaar,* IDIS 2010, 267.
[357] Van Rooy and Bus, 2010; Cavoukian, Taylor and Abrams, 2010.
[358] Vgl. Auer-Reinsdorff/Conrad, § 36 Rn. 164.
[359] *Forgó*, Datenschutzrechtliche Fragestellungen des autonomen Fahrens in Oppermann/Stender-Vorwachs, Autonomes Fahren, S. 169.
[360] Vergleiche Diskussion in Kap. 2.1
[361] Übersicht dazu bei *Jakobi, Gunnar und Stevens*, Privacy-By-Design für das Connected Car: Architekturen aus Verbrauchersicht, DuD 2018, 704, 706.

durch die Speicherung direkt bei den Herstellern ein hoher Komfort gewährleistet werden, aber die Daten sind dem Herrschaftsbereich des Betroffenen grundsätzlich entzogen. Eine Ausgewogene Lösung könnte daher der Treuhänder sein, da er nicht von eigenen Interessen getrieben ist und die personenbezogenen Daten selber nicht verarbeitet.[362]

Weitere Maßnahmen ließen sich in der Übermittlung der Daten treffen. So könnten die Daten vor der Übermittlung an den Hersteller oder den sonstigen Dritten möglichst anonymisiert werden, wobei die Anonymisierung im Fahrzeug direkt stattfinden kann oder beim Treuhänder, der dann die Daten zudem aggregiert, sodass eine tatsächliche und effektive Anonymisierung stattfindet.

Eine weitere erforderliche Maßnahme wäre es, dem Betroffenen jederzeit die Möglichkeit zu geben, die gesendeten Daten nachzuvollziehen und die Empfänger anzuzeigen. Dieses wäre durch ein Multimedia Interface direkt im Fahrzeug oder durch eine angebundene Applikation möglich. Dem Nutzer könnte dadurch die Möglichkeit zur Verwaltung seiner Einwilligungen gegeben werden und die Zwecke und Möglichkeiten transparent dargestellt werden. Auch die jederzeitige Widerrufbarkeit der Einwilligung könnte so einfach gewährleistet werden.

Wie auch schon im Kapitel 4.3.6 festgestellt, stellt die Infrastruktur für den Betrieb des automatisierten und vernetzen Fahrens eine kritische Infrastruktur im Sinne der Richtlinie 2008/114/EG dar. Des Weiteren wird der Betrieb einer solchen Infrastruktur gem. Art. 4 Abs. 4 auch durch die Richtlinie (EU) 2016/1148[363] erfasst. Die Betreiber solcher Infrastrukturen werden der besonderen Aufsicht u.a. des BSI unterworfen und müssen bestimmte Bedingungen erfüllen, z.B. dass die eingesetzte Technik dem aktuellen Stand der Technik entsprechend muss. Weitere Resolutionen der EU gibt es allgemein für den Bereich des „Autonomen Fahren im europäischen Verkehrswesen“, aber auch konkrete Vorschläge zur Daten- und Infrastruktursicherheit.[364] Die Kommission kam hierbei jedenfalls zu dem Schluss, dass eine gewisse Harmonisierung der physischen Infrastruktur erforderlich sein wird um sicherzustellen, dass automatisierte Fahrzeuge sicher im gemischten Verkehr betrieben werden.[365] Die Hersteller der Fahrzeuge werden durch diese Vorgaben genauso adressiert, wie die Betreiber der Infrastruktur, unabhängig davon ob es sich um einen öffentlichen Betreiber handelt oder dieser, zumindest teilweise, privat agiert.

Im Ergebnis ist die Datensicherheit im automatisierten und vernetzen Auto eine mehrschichtige Angelegenheit, die durch die verschiedenen Akteure, den Betroffenen einbezogen, verwirklicht werden muss. Der Datenschutz wirkt sich somit bereits auf das Design des Fahrzeuges, der Softwareplattform, die Speicherorte aber auch der Infrastruktur aus. Hierbei sollte es eine enge Abstimmung zwischen den Hersteller, den öffentlichen Einrichtungen aber auch Verbraucherschützern geben, um die berechtigten Interessen aller Parteien in einen Ausgleich zu bringen.

---

[362] Zu dem Ergebnis kommen auch *Jakobi, Gunnar und Stevens*, Privacy-By-Design für das Connected Car: Architekturen aus Verbrauchersicht, DuD 2018, 704, Tabelle 1 auf S. 705.

[363] Richtlinie (EU) 2016/1184 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union.

[364] 2018/0129(COD) Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates zur Änderung der Richtlinie 2008/96/EG über ein Sicherheitsmanagement für die Straßenverkehrsinfrastruktur; COM(2018) 286 final: Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die Typgenehmigung von Kraftfahrzeugen und Kraftfahrzeuganhängern sowie von Systemen, Bauteilen und selbstständigen technischen Einheiten für diese Fahrzeuge im Hinblick auf ihre allgemeine Sicherheit und den Schutz der Fahrzeuginsassen und von ungeschützten Verkehrsteilnehmern, zur Änderung der Verordnung (EU) 2018/... und zur Aufhebung der Verordnungen (EG) Nr. 78/2009, (EG) Nr. 79/2009 und (EG) Nr. 661/2009.

[365] A.a.O..

ABKÜRZUNGSVERZEICHNIS

A.a.O.	am angegebenen Ort
Abs.	Absatz
ABS	Anti-Blockier-System
ACC	Adaptive Cruise Control
ACEA	European Automobile Manufacturers´ Association
ADAC	Allgemeine Deutsche Automobil-Club
aE.	am Ende
AEUV	Vertrag über die Arbeitsweise der Europäischen Union
AGB	Allgemeine Geschäftsbedingungen
Art.	Artikel
Az.	Aktenzeichen
BDSG	Bundesdatenschutzgesetz
BGB	Bürgerliches Gesetzbuch
BGH	Bundesgerichtshof
BMJV	Bundesministerium der Justiz und für Verbraucherschutz
BMVI	Bundesministerium für Verkehr und digitale Infrastruktur
BT- Drs	Bundestagsdrucksache
BVerwG	Bundesverwaltungsgericht
BVerwGE	Bundesverwaltungsgericht Entscheidungen
BW	Baden-Württemberg
bzw.	beziehungsweise
CR	Computer und Recht
DatenschutzR	Datenschutzrecht
d.h.	das heißt
DOD	Department of Defense
DS-GVO	Datenschutz Grundverordnung
DSK	Datenschutzkonferenz
DS-RL	Datenschutz Richtlinie
DuD	Datenschutz und Datensicherung
EC	European Commission
EG	Europäische Gemeinschaft(en)
et al.	und andere
etc.	et cetera
ErwG	Erwägungsgrund
EU	Europäische Union
EuArbR	Europäisches Arbeitsrecht
EuGH	Gerichtshof der Europäischen Gemeinschaft / Europäischer Gerichtshof
EuZW	Europäische Zeitschrift für Wirtschaftsrecht
EWR	Europäischer Wirtschaftsraum
FernStG	Fernstraßengesetz
f.	folgende
ff.	die folgenden
FIN	Fahrzeugidentifikationsnummer
FZV	Fahrzeug-Zulassungsverordnung
GDPR	General Data Protection Regulation
gem.	gemäß
ggf.	gegebenenfalls

GPS	Global Positioning System
GSM	Global System for Mobile Communications
HessVGH	Hessischer Verwaltungsgerichtshof
HNU	Hochschule Neu-Ulm
Hs.	Halbsatz
ID	Identifikation
IKT	Informations- und Kommunikationstechnik
IMEI	International Mobile Station Equipment Identity
IMSI	International Mobile Subscriber Identity
insb.	insbesondere
IP	Internet Protocol
i.S.d.	im Sinne der/des
ISO	International Organization for Standardization
IT	Informationstechnik
i.V.m.	in Verbindung mit
JI-RL	Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates
Kap.	Kapitel
KBA	Kraftfahrt-BundesAmt
Kfz	Kraftfahrzeug
LDSG	Landesdatenschutzgesetz
lit.	littera
MMR	MultiMedia und Recht
m.w.N.	mit weiteren Nachweisen
Nds. LDSG	Niedersächsisches Landesdatenschutzgesetz
NJW	Neue Juristische Wochenschrift
Nr.	Nummer
NVwZ	Neue Zeitschrift für Verwaltungsrecht
NZKart	Neue Zeitschrift für Kartellrecht
NZV	Neue Zeitschrift für Verkehrsrecht
o.ä.	oder ähnlich
o.g.	oben genannten
OLG	Oberlandesgericht
OVG	Oberverwaltungsgericht
RFC	Request for Comments
p.	page
PbD	Privacy by design
S.	Satz / Seite
SAE	Society of Automotive Engineers
SIM	Subscriber identity module
sog.	so genannt
StrWG	Straßen- und Wegegesetz

StPO	Strafprozessordnung
StVG	Straßenverkehrsgesetz
s.o.	sieh(e) oben
s.u.	sieh(e) unten
SVR	Straßenverkehrsrecht
TK	Telekommunikation
TKG	Telekommunikationsgesetz
u.a	unter anderem
UDID	Unique Device Identification
UMTS	Universal Mobile Telecommunication System
UrhG	Urhebergesetz
VDA	Verband der Automobilindustrie
vgl.	vergleiche
VIN	Vehicle Information Number
VO	Rechtsverordnung,Verordnung (EG)
VW	Volkswagen
VwGO	Verwaltungsgerichtsordnung
WP	Working Party
WLAN	Wireless Local Area Network
z.B	zum Beispiel
ZD	Zeitschrift für Datenschutz

LITERATURVERZEICHNIS

3GPP, TS 22.016	International Mobile station Equipment Identities (IMEI), (V9.0, 2009), (http://www.qtc.jp/3GPP/Specs/22016-900.pdf, zuletzt aufgerufen am 11.09.2018)
92. Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder	Das Standard-Datenschutzmodell, Eine Methode zur Datenschutzberatung und -prüfung auf der Basis einheitlicher Gewährleistungsziele, November 2016 (https://www.huntonprivacyblog.com/wp-content/uploads/sites/28/2017/04/SDM-Methode_V_1_0.pdf, zuletzt aufgerufen am 11.09.2018)
Abel, Ralf B.	Automatisierte Entscheidungen im Einzelfall gem. Art. 22 DS-GVO, in: ZD 2018, 304-307
Allgemeiner Deutscher Automobil-Club (ADAC)	Studie, „Welche Daten erzeugt ein modernes Auto?“, Mai 2016 (https://www.adac.de/infotestrat/technik-und-zubehoer/fahrerassistenzsysteme/daten_im_auto/default.aspx, zuletzt aufgerufen am 06.09.2018)
Ambrock, Jens/ Karg, Moritz	Ausnahmetatbestände der DS-GVO als Rettungsanker des internationalen Datenverkehrs? Analyse der Neuerungen zur Angemessenheit des Datenschutzniveaus, in: ZD 2017, 154-161
Artikel-29-Datenschutzgruppe (Article 29 Data Protection Working Party)	Guidelines on consent under Regulation 2016/679, 17/EN, WP 259, rev. 01 (https://www.datenschutz-praxis.de/wp-content/uploads/2018/06/20180416_Article29WPGuidelineson-Consent_publishpdf.pdf, zuletzt aufgerufen am 11.09.2018) Opinion 13/2011 on Geolocation services on smart mobile devices, 881/11/EN, WP 185 (http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp185_en.pdf, zuletzt aufgerufen am 11.09.2018) Stellungnahme 1/2010 zu den Begriffen „für die Verarbeitung Verantwortlicher“ und „Auftragsbearbeiter“, 00264/10/DE, WP 169 (http://www.privacy-regulation.eu/privazyplan/article29/files/wp169%20DE%20Verantwortlicher%20vs.%20Auftragsverarbeiter%202010%2002%2016.pdf, zuletzt aufgerufen am 11.09.2018)
Auer-Reinsdorff (Hrsg.), Astrid/ Conrad (Hrsg.), Isabell	Handbuch IT- und Datenschutzrecht, 2. Auflage, München 2016

Bräutigam, Peter/ Schmidt-Wudy, Florian	Das geplante Auskunfts- und Herausgaberecht des Betroffenen nach Art. 15 der EU-Datenschutzgrundverordnung, Ein Diskussionsbeitrag zum anstehenden Trilog der EU-Gesetzgebungsorgane, in: CR 2015, 56-63
Bretthauer, Sebastian/ Krempel, Erik/ Birnstill, Pascal	Intelligente Videoüberwachung in Kranken- und Pflegeeinrichtungen von morgen, Eine Analyse der Bedingungen nach den Entwürfen der EU-Kommission und des EU-Parlaments für eine DS-GVO, in: CR 2015, 239-245
Bundesministerium für Justiz und für Verbraucherschutz	„One-Pager“ - Muster für transparente Datenschutzhinweise (https://www.bmjv.de/DE/Themen/FokusThemen/OnePager/OnePager_node.html, zuletzt aufgerufen am 11.09.2018)
Bundesministerium für Verkehr und digitale Infrastruktur	Automatisiertes und vernetztes Fahren (https://www.bmvi.de/DE/Themen/Digitales/Automatisiertes-und-vernetztes-Fahren/automatisiertes-und-vernetztes-fahren.html, zuletzt aufgerufen am 11.09.2018)
Cavoucian, Ann Dixon, Mark	Privacy and Security by Design: An Enterprise Architecture Approach, 2013 (https://www.ipc.on.ca/wp-content/uploads/Resources/pbd-privacy-and-security-by-design-oracle.pdf, zuletzt aufgerufen am 11.09.2018)
Cavoukian, Ann Scott, Taylor Abrams, Martin E.	Privacy by Design: essential for organizational accountability and strong business pracises (https://link.springer.com/content/pdf/10.1007%2Fs12394-010-0053-z.pdf, zuletzt aufgerufen am 11.09.2018)
Dammann, Ulrich	Erfolge und Defizite der EU-Datenschutzgrundverordnung, Erwarteter Fortschritt, Schwächen und überraschende Innovationen, in: ZD 2016, 207-314
Datenschutz-Folgenabschätzung (DSFA)	Liste der Verarbeitungstätigkeiten, für die eine DSFA durchzuführen ist (https://www.ldi.nrw.de/mainmenu_Aktuelles/submenu_EU-Datenschutzreform/Inhalt/EU-Datenschutzreform/DSFA-Muss-Liste-1_0.pdf, zuletzt aufgerufen am 11.09.2018)
Datenschutzkonferenz (DSK)	Kurzpapier Nr. 13 Auftragsverarbeitung, Art. 28 DS-GVO (https://www.lfd.niedersachsen.de/download/126580/DSK-Kurzpapier_Nr._13_-_Auftragsverarbeitung.pdf, zuletzt aufgerufen am 11.09.2018)

Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit	Liste von Verarbeitungsvorgängen nach Art. 35 Abs. 4 DSGVO (https://datenschutz-hamburg.de/assets/pdf/Liste%20Art%2035-4%20DSGVO%20HmbBfDI-%C3%B6ffentlicher%20Bereich_v1.0.pdf, zuletzt aufgerufen am 11.09.2018)
Der Landesbeauftragte für den Datenschutz Niedersachsen	Liste von Verarbeitungsvorgängen nach Art. 35 Abs. 4 DS-GVO (https://www.lfd.niedersachsen.de/download/131098/Liste_von_Verarbeitungsvorgaengen_nach_Art._35_Abs._4_DS-GVO.pdf, zuletzt aufgerufen am 11.09.2018)
Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz	Liste von Verarbeitungsvorgängen nach Art. 35 Abs. 4 DS-GVO (https://www.datenschutz.rlp.de/fileadmin/lfdi/Dokumente/Orientierungshilfen/DSFA_-_Muss-Liste_RLP_NOE.pdf, zuletzt aufgerufen am 11.09.2018)
Donath, Andreas	Volvo schaut dem Fahrer in die Augen (https://www.golem.de/news/muede-und-unaufmerksam-volvo-schaut-dem-fahrer-in-die-augen-1403-105199.html, zuletzt aufgerufen am 11.09.2018)
Drexl, Josef	Neue Regeln für die Europäische Datenwirtschaft?, Ein Plädoyer für einen wettbewerbspolitischen Ansatz - Teil 2, in: NZKart 2017, 415-421
Düsseldorfer Kreis	Orientierungshilfe zu den Datenschutzanforderungen an App-Entwickler und App-Anbieter (https://www.lda.bayern.de/media/oh_apps.pdf, zuletzt aufgerufen am 11.09.2018)
Eckhardt, Jens	DS-GVO: Anforderungen an die Auftragsverarbeitung als Instrument zur Einbindung Externer, in: CCZ 2017, 111-117
Ehmann, Eugen/ Schonschek Oliver	Prozessorientierte Datenschutz-Praxis, Aktuelle Lösungsschemata für alle Aufgaben im Datenschutz mit Erläuterungen und Mustern, 2. Auflage, München 2011
Ehmann (Hrsg.), Eugen/ Selmayr (Hrsg.), Martin	Datenschutz-Grundverordnung: DS-GVO, Kommentar, 2. Auflage, München 2018
Eßer (Hrsg.), Martin/ Kramer (Hrsg.), Philipp/ Lewinski (Hrsg.), Kai von	DSGVO/BDSG, Datenschutz-Grundverordnung/Bundesdatenschutzgesetz und Nebengesetze, 6. Auflage, Köln 2018
Engeler, Malte	Das überschätzte Kopplungsverbot, Die Bedeutung des Art. 7 Abs. 4 DS-GVO in Vertragsverhältnissen, in: ZD 2018, 55-62
European Automobile Manufactures Association (ACEA)	Principles of Data Protection in Relation to Connected Vehicles ans Services, 2015

European Commission Directorate – General Joint Research Centre	Biometrics at the Frontiers: Assessing the Impact on Society. For the European Parliament Committee on Citizens' Freedoms and Rights, Justice and Home Affairs (LIBE), Executive Summary, 2005 (http://www.statewatch.org/news/2005/mar/Report-IPTS-Biometrics-for-LIBE.pdf, zuletzt aufgerufen am 11.09.2018)
Forgó, Nikolaus/ Krügel, Tina	Der Personalbezug von Geodaten - Cui bono, wenn alles bestimmbar ist?, in: MMR 2010, 17-23.
Franzen (Hrsg.), Martin/ Gallner (Hrsg.), Inken/ Oetker (Hrsg.), Hartmut	Kommentar zum europäischen Arbeitsrecht, 2. Auflage, München 2018
Gemeinsame Erklärung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder und des Verbandes der Automobilindustrie (VDS)	Datenschutzrechtliche Aspekte bei der Nutzung vernetzter und nicht vernetzter Kraftfahrzeuge, Januar 2016
Gola (Hrsg.), Peter	Datenschutz-Grundverordnung: DS-GVO, Kommentar, 2. Auflage, München 2018
Golland, Alexander	Kopplungsverbot in der Datenschutz-Grundverordnung, Anwendungsbereich, ökonomische Auswirkungen auf Web 2.0-Dienste und Lösungsvorschlag, in: MMR 2018, 130-135
Graf, Felix	„Car 2 Car/Car 2 X“ Kommunikation - Kommunikation zwischen Fahrzeugen und deren Umgebung (https://www.uni-koblenz-landau.de/de/koblenz/fb4/ist/AGZoebel/Lehre/ss09/Seminar09/graf, zuletzt aufgerufen am 06.09.2018)
Heermann, Thorsten	AG Nienburg: Erstmals Dash-Cam-Aufzeichnung als Beweismittel im Strafverfahren zugelassen, in: ZD-Aktuell 2015, 07425.
House of Commons, Science and Technology Committee	Current and future uses of biometric data and technologies, Sixth Report of Session 2014-15, (https://publications.parliament.uk/pa/cm201415/cmselect/cmsctech/734/734.pdf, zuletzt aufgerufen am 11.09.2018)
Information Sciences Institute, University of Southern California	RFC 760, DOD Standard Internet Protocol, Januar 1980 (https://tools.ietf.org/html/rfc760, zuletzt aufgerufen am 11.09.2018)
Klimke, Dominik	Telematik-Tarife in der Kfz-Versicherung, in: RuS 2015, 217-225
Krügel, Tina	Das personenbezogene Datum nach der DS-GVO, Mehr Klarheit und Rechtssicherheit?, in: ZD 2017, 455-460

Kühling (Hrsg.), Jürgen/ Buchner (Hrsg.), Benedikt/	Datenschutz-Grundverordnung, Bundesdatenschutzgesetz: DS-GVO/BDSG, Kommentar, 2. Auflage, München 2018
Lachenmann, Matthias	Neue Anforderungen an die Videoüberwachung, Kritische Betrachtung der Neuregelungen zur Videoüberwachung in DS-GVO und BDSG neu, in: ZD 2017, 407-411
Landesbeauftragter für Datenschutz und Informationsfreiheit Baden Württemberg	Liste von Verarbeitungsvorgängen nach Art. 35 Abs. 4 DS-GVO (https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2018/05/Liste-von-Verarbeitungsvorg%C3%A4ngen-nach-Art.-35-Abs.-4-DS-GVO-LfDI-BW.pdf, zuletzt aufgerufen am 11.09.2018)
McKinsey&Company	Monetizing car data, New service business opportunities to create new customer benefits September 2016 (https://www.mckinsey.com/~/media/McKinsey/Industries/Automotive%20and%20Assembly/Our%20Insights/Monetizing%20car%20data/Monetizing-car-data.ashx, zuletzt aufgerufen am 11.09.2018)
Mienert, Heval/ Gipp, Bela	Dashcam, Blockchain und der Beweis im Prozess, Kriterien für einen Privacy by Design-Lösungsansatz bei Dashcams, in: ZD 2017, 514-519
National Transportation Safety Board	Preliminary Report Highway, HWY18MH010 (https://www.ntsb.gov/investigations/AccidentReports/Reports/HWY18MH010-prelim.pdf, zuletzt aufgenommen am 11.09.2018)
Niehaus, Holger	Verwertbarkeit von Dashcam-Aufzeichnungen im Straf- und Ordnungswidrigkeitenverfahren, Zugleich Anmerkung zu OLG Stuttgart, Beschl. v. 4.5.2016 - 4 Ss 543/15 -, NZV 2016, 588, in: NZV 2016, 551-556
Oppermann (Hrsg.), Bernd H./ Stender-Vorwachs (Hrsg.), Jutta	Autonomes Fahren, Rechtsfolgen, Rechtsprobleme, technische Grundlagen, 1. Auflage, München 2017
Paal (Hrsg.), Boris P./ Pauly (Hrsg.), Daniel A.	Datenschutz-Grundverordnung, Bundesdatenschutzgesetz: DS-GVO BDSG, 2. Auflage, München 2018
Petri, Thomas	Anmerkung zu einer Entscheidung des EuGH, Urteil vom 05.06.2018 (C-210/16) - Zur Frage der Verantwortlichkeit von Facebook und des Betreibers einer Facebook-Fanpage für die Verarbeitung personenbezogener Daten, in: EuZW 2018, 540-541

Plath (Hrsg.), Kai-Uwe	DSGVO/BDSG, Kommentar zu DSGVO, BDSG und den Datenschutzbestimmungen des TMG und TKG, 3. Auflage, Köln 2018
Radlanski, Philip	Das Konzept der Einwilligung in der datenschutzrechtlichen Realität, 1. Auflage, Tübingen 2016
Recht Automobil Wirtschaft (RAW)	„Erneuter Sieg für Audi in Le Mans“ in: RAW 2014, 157
Reuter, Markus	BMW speichert keine Standortdaten, gibt aber Bewegungsprofil an Gericht, 21.07.2016 (https://netzpolitik.org/2016/bmw-speichert-keine-standortdaten-gibt-aber-bewegungsprofil-an-gericht/, zuletzt aufgerufen am 11.09.2018)
Richter, Philipp	Datenschutz zwecklos? - Das Prinzip der Zweckbindung im Ratsentwurf der DSGVO, in: DuD 2015, 735-740
Roßnagel, Alexander/ Nebel, Maxi/ Richter, Philipp	Was bleibt vom Europäischen Datenschutzrecht?, Überlegungen zum Ratsentwurf der DS-GVO, in: ZD 2015, 455-460
Roßnagel, Alexander	Fahrzeugdaten – wer darf über sie entscheiden?, in: SVR 2014, 281.
Rummel, Christopher	Das vernetzte Auto: Datenverarbeitung in Echtzeit, in: IoT 2018 (https://www.industry-of-things.de/das-vernetzte-auto-datenverarbeitung-in-echtzeit-a-686637/, zuletzt aufgerufen am 11.09.2018)
Schaar, Peter	Privacy by Design, in: IDIS 2010, 267-274
Schantz, Peter	Die Datenschutz-Grundverordnung - Beginn einer neuen Zeitrechnung im Datenschutzrecht, in: NJW 2016, 1841-1847
Schlanstein, Peter	Nutzung von Fahrzeugdaten zur Optimierung der Verkehrsunfallaufnahme, in: NZV 2016, 201.
Schoch (Hrsg.), Friedrich/ Schneider (Hrsg.), Jens-Peter/ Bier (Hrsg.), Wolfgang	Verwaltungsgerichtsordnung: VwGO, 34. Auflage, München 2018
Society of Automotive Engineers (SAE)	Standard SAE International: Levels of Driving Automation for On-Road Vehicles J3016 (https://www.smmt.co.uk/wp-content/uploads/sites/2/automated_driving.pdf, zuletzt aufgerufen am 11.09.2018)

Stiftung Datenschutz	Neue Wege bei der Einwilligung im Datenschutz - technische, rechtliche und ökonomische Herausforderungen, 2017 (https://www.stiftungdatenschutz.org/fileadmin/Redaktion/Bilder/Abschluss_Studie_30032017/stiftungdatenschutz_broschuere_20170611_01.pdf, zuletzt aufgerufen am: 11.09.2018)
Tesla	Allgemeine Geschäftsbedingungen (AGB) (https://www.tesla.com/de_DE/order/download-order-agreement?country=DE, zuletzt aufgerufen am 11.09.2018) Rechtliche Hinweise auf Tesla-Website (https://www.tesla.com/de_DE/about/legal, zuletzt aufgerufen am 11.09.2018) TeslaMAG, Tesla Model 3 verfügt über eine auf den Innenraum gerichtete Kamera im Rückspiegel (https://tesla-mag.de/news/tesla-model3-innenraum-kamera-rueckspiegel-15557, zuletzt aufgerufen am 11.09.2018)
Unabhängiges Landeszentrum für Datenschutz (ULD)	Liste von Verarbeitungsvorgängen nach Art. 35 Abs. 4 DS-GVO (https://www.datenschutzzentrum.de/uploads/datenschutz-folgenabschaetzung/20180525_LfD-SH_DSFA_Muss-Liste_V1.0.pdf, zuletzt aufgerufen am 11.09.2018)
Van Rooy, Dirk Bus, Jaques	Trust and privacy in the future internet – a research perspective (https://link.springer.com/content/pdf/10.1007%2Fs12394-010-0058-7.pdf, zuletzt aufgerufen am 11.09.2018)
Veil, Winfried	Die Datenschutz-Grundverordnung: des Kaisers neue Kleider, Der gefährliche Irrweg des alten wie des neuen Datenschutzrechts, in: NVwZ 2018, 686-696.
Verband der Automobilindustrie (VDA)	Datenschutz-Prinzipien für vernetzte Fahrzeuge, November 2014
Verband der Automobilindustrie (VDA)	Automatisierung - Von Fahrassistenzsystemen zum vollautomatisierten Fahren, 2015
Vogt, Joerg-Oliver	Geschäftsmodelle für das vernetzte Fahrzeug - Klassifikation, Angebot und Nutzen für das mobile Arbeiten, HNU Working Paper Nr. 30, 2014
Volkswagen (VW)	SSP 543: Der Passat 2015, Fahrassistenzsysteme Selbststudienprogramm.
Weichert, Thilo	Datenschutz im Auto - Teil 1, Das Kfz als großes Smartphone mit Rädern, in: SVR 2014, 201-207
Weichert, Thilo	Der Personenbezug von Kfz-Daten, in: NVZ 2017, 507-513

Weichert, Thilo	Car-to-Car-Communication zwischen Datenbegehrlichkeit und digitaler Selbstbestimmung, in: SVR 2016, 361.
Weisser, Ralf/ Färber, Claus	Rechtliche Rahmenbedingungen bei Connected Car, Überblick über die Rechtsprobleme der automobilen Zukunft, in: MMR 2015, 506-512
Wendehorst, Christiane/ Westphalen, Friedrich v.	Das Verhältnis zwischen Datenschutz-Grundverordnung und AGB-Recht, in: NJW 2016, 3745-3750
Wendt, Kai	Autonomes Fahren und Datenschutz – eine Bestandsaufnahme, in: ZD-Aktuell 2018, 06034.
Wolff (Hrsg.), Heinrich Amadeus/ Brink (Hrsg.), Stefan	BeckOK Datenschutzrecht, 22. Edition, Stand: 01.11.2017, München 2017
Ziegenhorn, Gero/ Heckel,Katharina von	Datenverarbeitung der Private nach der europäischen Datenschutzreform, in: NVwZ 2016, 1585-1591